SECRET TEXTS AND CIPHERBALLOTS: SECRET SUFFRAGE AND REMOTE ELECTRONIC VOTING

Adrià Rodríguez-Pérez

ADVERTIMENT. L'accés als continguts d'aquesta tesi doctoral i la seva utilització ha de respectar els drets de la persona autora. Pot ser utilitzada per a consulta o estudi personal, així com en activitats o materials d'investigació i docència en els termes establerts a l'art. 32 del Text Refós de la Llei de Propietat Intel·lectual (RDL 1/1996). Per altres utilitzacions es requereix l'autorització prèvia i expressa de la persona autora. En qualsevol cas, en la utilització dels seus continguts caldrà indicar de forma clara el nom i cognoms de la persona autora i el títol de la tesi doctoral. No s'autoritza la seva reproducció o altres formes d'explotació efectuades amb finalitats de lucre ni la seva comunicació pública des d'un lloc aliè al servei TDX. Tampoc s'autoritza la presentació del seu contingut en una finestra o marc aliè a TDX (framing). Aquesta reserva de drets afecta tant als continguts de la tesi com als seus resums i índexs.

ADVERTENCIA. El acceso a los contenidos de esta tesis doctoral y su utilización debe respetar los derechos de la persona autora. Puede ser utilizada para consulta o estudio personal, así como en actividades o materiales de investigación y docencia en los términos establecidos en el art. 32 del Texto Refundido de la Ley de Propiedad Intelectual (RDL 1/1996). Para otros usos se requiere la autorización previa y expresa de la persona autora. En cualquier caso, en la utilización de sus contenidos se deberá indicar de forma clara el nombre y apellidos de la persona autora y el título de la tesis doctoral. No se autoriza su reproducción u otras formas de explotación efectuadas con fines lucrativos ni su comunicación pública desde un sitio ajeno al servicio TDR. Tampoco se autoriza la presentación de su contenido en una ventana o marco ajeno a TDR (framing). Esta reserva de derechos afecta tanto al contenido de la tesis como a sus resúmenes e índices.

WARNING. Access to the contents of this doctoral thesis and its use must respect the rights of the author. It can be used for reference or private study, as well as research and learning activities or materials in the terms established by the 32nd article of the Spanish Consolidated Copyright Act (RDL 1/1996). Express and previous authorization of the author is required for any other uses. In any case, when using its content, full name of the author and title of the thesis must be clearly indicated. Reproduction or other forms of for profit use or public communication from outside TDX service is not allowed. Presentation of its content in a window or frame external to TDX (framing) is not authorized either. These rights affect both the content of the thesis and its abstracts and indexes.

Adrià Rodríguez-Pérez

SECRET TEXTS AND CIPHERBALLOTS: SECRET SUFFRAGE AND REMOTE ELECTRONIC VOTING

PhD Thesis

Universitat Rovira i Virgili

Scytl Election Technologies, S.L.U.

UNIVERSITAT ROVIRA i VIRGILI

UNIVERSITAT ROVIRA I VIRGILI
SECRET TEXTS AND CIPHERBALLOTS: SECRET SUFFRAGE AND REMOTE ELECTRONIC VOTING
Adrià Rodríguez-Pérez

Adrià Rodríguez-Pérez

SECRET TEXTS AND CIPHERBALLOTS: SECRET SUFFRAGE AND REMOTE ELECTRONIC VOTING

PhD Thesis

Supervisor: Dr. Jordi Barrat i Esteve

Department of Public Law

Universitat Rovira i Virgili

Scytl Election Technologies, S.L.U.

UNIVERSITAT ROVIRA i VIRGILI

Barcelona

May 2022

UNIVERSITAT
ROVIRA i VIRGILI

I STATE that the present study, entitled “Secret texts and cipherballots: secret suffrage and remote electronic voting”, presented by Adrià Rodríguez-Pérez for the award of the degree of Doctor, has been carried out under my supervision at the Department of Public Law of this university.

Reus, 27 May 2022

Doctoral Thesis Supervisor

Dr. Jordi Barrat i Esteve

To Lluís: because I connected most of the dots
when you forced me to go for a stroll.

Acknowledgements

This PhD is the result of an industrial doctorate[1] done at Scytl Election Technologies, S.L.U. in close collaboration with Dr. Jordi Barrat, from Universitat Rovira i Virgili. The main objective of this kind of PhD is to do applied research and encourage collaboration between the country's socioeconomic and academic sectors, with a view to stimulate competitivity and innovation through knowledge transfer. Therefore, and as a member of Scytl's Research and Security Department, I must thank the invaluable contribution of its team members, current and past, to this research. Being able to pursue my doctoral studies at Scytl has provided an important input into making my research useful and understandable for everyone (or, at least, so I tried). At the same time, and industrial PhD is still a PhD, and therefore I must thank both my universities as well: Universitat Pompeu Fabra and Universitat Rovira I Virgili. At Universitat Pompeu Fabra's Department of International Law and International Relations I have found an academic team that has provided an outstanding research environment. As my supervisor, in Jordi Barrat from Universitat Rovira i Virgili I have found the necessary guidance to undergo this six-year PhD.

This journey would not have succeeded without the restlessness support of my family, who even took the risk of hosting me again during the most stressful stage of the research. *Mama, yaya, Pili, imuchísimas gracias!* Also, thanks to my PhD family, my PhD twin: Marta Galceran. I hope you have found in me at least half the support you have always given me. I also want to acknowledge the assistance from two colleagues at Scytl who have guided me in my approach towards information security and (post-quantum) cryptography: Jordi Cucurull and Núria Costa. I must thank them for their review of one the latest version of this draft and your helpful suggestions (and which have prevented me from looking like a fool when discussing topics that I was not even aware that existed before I started working with you). And last, but definitely not least, I have to thank Silvia Caparrós and Jordi Puiggalí. Without them, nobody would be reading these pages today. Thanks for your support and for trusting me, even when I had already given up.

[1] Grant DI 2016 0026 by the Catalan government (*Generalitat de Catalunya*). Furthermore, part of the research conducted at Scytl has received funding from the European Commission under the auspices of PROMETHEUS Project, Horizon 2020 Research and Innovation action (Grant Agreement No. 780701).

Abstract

One of the key concerns about remote electronic voting is how to preserve secret suffrage. The list of authors who claim that Internet voting is incompatible with the secrecy of the vote is actually quite long. Even if later studies that analysed the actual implementation of remote electronic voting in public political elections had more nuanced findings, concerns about secret suffrage and remote electronic voting remain. Addressing these concerns becomes an inescapable obligation. In this context, our research is quite novel. First and foremost, our starting point is not based on pre-existing legal definitions that are accepted as given. Drawing from the universalist approach to comparative constitutional law, we have understood that the principle of secret suffrage exists in such a way that it transcends the culture bound opinions and conventions of particular political communities. This core understanding has been translated into three standards: individuality, confidentiality, and anonymity. These standards should apply to any voting channel. Second, we have taken a wider approach at the enforcement of this principle. We have showed that secret suffrage may be enforced through law, code, norms, and even the market. Current regulations tend to be constrained because they resort to analogies with paper-based voting channels and fail to acknowledge the specificities of remote electronic voting. In contrast, we have examined the role played by (and the limitations of) asymmetric encryption, anonymization based on mix-nets or homomorphic tallying, and of multiple voting to enforce secret suffrage. We have argued that remote electronic voting regulations should be more detailed when it comes to specifying how these architectures of cyberspace could contribute towards the enforcement of legal principles. Therefore, this PhD provides an overarching framework to guide the examination of how digital technologies impact on electoral processes and the principles for democratic elections.

Resum

Una de les principals preocupacions sobre el vot telemàtic és com preservar el sufragi secret. La llista d'estudis que afirmen que el vot per Internet és incompatible amb el secret del vot és força extensa. Si bé estudis posteriors sobre experiències reals han tingut resultats més matisats, les preocupacions sobre el sufragi secret i el vot telemàtic es mantenen. Abordar aquestes preocupacions esdevé una obligació ineludible. En aquest context, la nostra recerca és novadora. En primer lloc, el nostre punt de partida no es basa en definicions legals preexistents que s'accepten com a donades. Partint de l'enfocament universalista del dret constitucional comparat, hem entès que el principi del sufragi secret transcendeix les opinions i convencions lligades a comunitats polítiques concretes. Aquesta concepció comú i bàsica s'ha traduït en tres estàndards: individualitat, confidencialitat i anonimat. Aquests estàndards s'han de satisfer en qualsevol canal de votació. En segon lloc, hem adoptat un enfocament més ampli en l'aplicació d'aquest principi al vot telemàtic. Hem demostrat que el sufragi secret es pot garantir mitjançant la llei, el codi informàtic, les normes i fins i tot el mercat. La normativa actual tendeix a ser limitada perquè recorre a analogies amb els canals de votació en paper i no reconeix les especificitats del vot telemàtic. Per contra, aquí hem examinat el paper que exerceixen (i les limitacions pròpies) del xifrat asimètric, l'anonimització basada en *mix-nets* o el recompte homomòrfic, i el vot múltiple. Hem argumentat que les regulacions del vot electrònic a distància haurien de ser més detallades a l'hora d'especificar com aquestes arquitectures del ciberespai podrien contribuir al compliment dels principis legals. Per tant, aquest doctorat ofereix un marc general per orientar l'examen sobre com les tecnologies digitals repercuteixen en els processos electorals i els principis de les eleccions democràtiques.

Resumen

Una de las principales preocupaciones sobre el voto telemático es cómo garantizar el secreto del voto. La lista de autores que afirman que el voto por Internet es incompatible con el sufragio secreto es considerable. Aunque las conclusiones de estudios posteriores sobre experiencias reales hayan sido más matizadas, las preocupaciones sobre el sufragio secreto y el voto telemático se mantienen. Abordar estas preocupaciones constituye en una obligación ineludible. En este contexto, nuestra investigación es novedosa. En primer lugar, nuestro punto de partida no se basa en definiciones legales preexistentes que se aceptan como dadas. Partiendo del enfoque universalista del derecho constitucional comparado, hemos entendido que el principio del sufragio secreto trasciende las opiniones y convenciones ligadas a la cultura de comunidades políticas concretas. Esta concepción se ha traducido en tres normas: individualidad, confidencialidad y anonimato. Estas normas deberían aplicarse a cualquier canal de votación. En segundo lugar, hemos adoptado un enfoque más amplio sobre la aplicación de este principio. Hemos demostrado que el sufragio secreto puede garantizarse mediante la ley, el código, las normas e incluso el mercado. La normativa actual tiende a ser limitada porque recurre a analogías con los canales de votación en papel y no reconoce las especificidades del voto telemático. Por el contrario, aquí hemos examinado el papel que desempeñan (y las limitaciones de) el cifrado asimétrico, la anonimización basada en *mix-nets* o el recuento homomórfico, y el voto múltiple para aplicar el sufragio secreto. Hemos argumentado que las regulaciones del voto telemático deberían ser más detalladas y especificar cómo estas arquitecturas del ciberespacio podrían contribuir al cumplimiento de los principios legales. Por lo tanto, este doctorado proporciona un marco general para orientar el examen de cómo las tecnologías digitales repercuten sobre los procesos electorales y los principios de las elecciones democráticas.

Acronyms

ANSSI	*Agence nationale de la sécurité des systèmes d'information* (France)
CC	Common Criteria
ChF	*Chancellerie Fédérale* (Switzerland)
CNIL	*Commission Nationale de l'Informatique et des Libertés* (France)
CSCE	Conference on Security and Co-operation in Europe
DRE	Direct-Record Electronic voting machines
E2E	End-to-end
EET	Election Expert Team (OSCE/ODIHR)
EAM	Election Assessment Mission (OSCE/ODIHR)
ENISA	EU Agency for Cybersecurity
EOM	Election Observation Mission (OSCE/ODIHR)
EPFZ	*École polytechnique fédérale de Zurich* (Switzerland)
EU	European Union
GEVE	*Groupe d'experts Vote électronique* (Switzerland)
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
GSU	*Guichet Sécurisé Unique* (Neuchâtel, Switzerland)
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communication Technologies
NAM	Needs Assessment Mission (OSCE/ODIHR)
NEC	National Electoral Committee (Estonia)
NSA	National Security Agency (USA)
NVT	New Voting Technologies (OSCE/ODIHR)
ODIHR	Office for Democratic Institutions and Human Rights (OSCE)
OSCE	Organization for Security and Co-operation in Europe
OSE	*Organisation des Suisses de l'étranger* (Switzerland)
PACE	Parliamentary Assembly of the Council of Europe
PIT	Public Intrusion Test (Switzerland)
PP	Protection Profile

REV	Remote Electronic Voting
RGAA	*Référentiel général d'accessibilité pour les administrations* (ANSSI, France)
RGS	*Référentiel générale de sécurité* (ANSSI, France)
SAS	*Service d'accréditation suisse* (Switzerland)
SEO	State Electoral Office (Estonia)
SFR	Security Functional Requirements
SMS	Short Message Service
UK	United Kingdom
USA	United States of America
VE	*Vote électronique*
VEleS	Federal Chancellery's Ordinance of 13 December 2012 on Electronic Voting (Switzerland)
VIV	Verifiable internet voting
VVPAT	Voter-Verified Paper-Audit Trial

Table of contents

1. Introduction

Digital technologies are changing the way we think, the way we read, and the way we remember (Carr, 2011). And yet, they do not seem to have substantially changed the way we vote. They are changing the way we think about our private space and about ourselves (Silverman, 2015). And yet, do we think that they are not going to change our preference-formation, a key step in democratic and electoral processes? Amidst a global health crisis brought by the Covid-19 pandemic and its long-lasting effects, answering these questions may be even more necessary than before. François-Noël Buffet could not have said it better: the health crisis inevitably leads us to question our democratic practices (2020: 5).

Law tends to be reluctant to change, even when technologies compel regulations to do so. There are many examples of this, in elections as well: when social media enters into the electoral campaign arena, we ask it to behave as traditional broadcast media; when cryptocurrencies flood finances (including in elections), we look at them as if they were fiat; when votes are cast electronically, we speak about "digital envelopes", "virtual voting booths", and "electronic ballot boxes". But encryption is not a digital envelope, casting multiple votes is not a virtual voting booth, and a computer server is not an electronic ballot box. In the case of Internet or remote electronic voting[2], ciphertexts are not secret ballots.

Furthermore, traditional approaches to regulating technologies in elections fail at acknowledging one key issue: that Information and Communication Technologies (ICT) do not only provide new spaces that need to be regulated, but they also transform the non-digital realities that ICT mediate. Technology and law are reconciled by society and failing to recognise this intercourse may render current regulations not only ineffective, but also illegitimate at the eyes of those who are regulated. This may seem obvious, but it is especially difficult for some fields to accept. Electoral law, being so closely related to the core of fundamental rights in a democratic society, is one of such fields. Yet, social practices make no exceptions.

In the following pages, we will approach the challenges that current electoral regulations will face because of the introduction digital technologies in voting processes. The case of internet voting is of paramount importance. When delegates of the 47 members States of the Council of Europe gathered in the 2004 to draft international standards for electronic voting for the first time, they concluded that e-enabled elections should "be as reliable and secure as democratic elections and referendums which do not involve the use of electronic means" [emphasis added] (Council of Europe, 2004a: i). Soon after, this approach proved to be flawed. Currently, the benchmark in the updated Rec(2017)5 "is [the] respect for all principles of democratic elections and referendums" (Driza Maurer, 2017: 154). This includes, of course, the principle of secret suffrage.

Notwithstanding, an overarching framework allowing us to assess whether, when, and how does remote electronic voting comply with the principle of secret suffrage is still missing. Nathan Licht et al. argue that "there is a lack of a general legal and technical

[2] We use indistinguishably the terms "remote electronic voting", "internet voting", and "online voting" (also in their shorter versions as "remote e-voting" or "i-voting") to refer to e-casting technologies used from remote environments, both controlled and uncontrolled. A more detailed definition of these terms is provided in Section I.1 in this chapter.

framework/design that describes and defines the appropriated provisions of i-voting systems. This lack becomes a barrier because the standard according to which a potentially suitable system would be compared against does not exist, and hence the debate is less structured" (2021: 97). When it comes to secret suffrage, Arne Koitmäe, Jan Willemson and Priit Vinkel argue that "the concepts of the secret ballot and secret vote have strong ties to voting in a controlled environment in the polling station, and remote electronic methods like postal voting or Internet voting need to employ specifical measures and approaches to achieve similar results" (2021: 140).

Therefore, we will argue that respecting all principles of democratic elections and referendums is not enough: How are those principles understood? Can they be translated to non-paper elections? What if the principles in which democratic elections lay should be also revisited considering new social practices? Even where digital technologies are not voluntarily introduced by election administrators, they may end up disrupting electoral processes as well. Secret suffrage in remote electronic voting is paramount. Therefore, the challenge is not just how digital technologies may fit traditional legal frameworks, but how to avoid that the social practices that result from the spread of digital technologies end up compromising the democratic values behind electoral standards.

I. STATE OF THE ART: REMOTE ELECTRONIC VOTING AND SECRET SUFFRAGE

1. On remote electronic voting

It is first necessary to provide an accepted definition of remote electronic voting. The use of digital technology in elections is indistinctly referred to as electronic voting, e-voting, voting technology, etc. Yet, there are different technologies, and they need to be clearly distinguished. A first distinction must be drawn between those technologies that are used to cast the vote *vis-à-vis* other electoral technologies. Our focus is on the former, and we therefore exclude election modernisation technologies such as voter registration portals, electoral management systems, or even ballot counting and tabulation technologies[3]. These technologies must be distinguished from electronic voting since they do not deal with the casting of the vote[4].

The fact that votes are cast using electronic means may be worth studying on its own, even from the perspective of secret suffrage. Notwithstanding, when it comes to e-casting technologies we must further distinguish between remote and non-remote electronic voting[5]. Whereas the first set of technologies (i.e., remote) rely on the Internet to cast the

[3] On the use of digital technologies for the tabulation of election results, we suggest the paper written by Adrià Rodríguez-Pérez, Pol Valletbó-Montfort, and Jordi Cucurull (2019).

[4] Therefore, our approach is narrower than the understanding of electronic voting in international standards such as the Council of Europe's Recommendation on e-voting or the OSCE/ODIHR's methodology for observing new voting technologies (NVT). The reference to e-voting or NVT is confusing, since both organisations consider technologies used only to count paper-based ballots as well (that is: e-counting, but not e-voting, technologies). More details about the two organisation's standards on e-voting are provided in chapter 3.

[5] This is, of course, a simplification. For example, Chantal Enguehard (2010) identifies up to eight different electronic voting technologies. Notwithstanding, most of them are non-remote electronic

vote from the voter device to a (usually) centralised voting server, non-remote electronic voting technologies are used to cast, store, and count the votes. The majority of electronic voting technologies used nowadays are non-remote: voting machines such as Direct-Record Electronic voting machines (DRE), with or without Voter-Verified Paper-Audit Trial (VVPAT). Yet, our focus is on remote electronic voting channels. These can take also many forms and shapes, but they share one characteristic: the device used to vote (be it a computer or a laptop, a smartphone or even a smart TV) are located remotely from the voting or counting servers, and the connection between the two depends upon the Internet as the voting channel. That is why remote electronic voting is sometimes referred to as Internet voting (and i-voting), or online voting. From now on, we will use these terms indistinctively to refer to remote electronic voting.

Because the voting device and the voting server are distant from each other, a third distinction is also possible, depending on the location from where votes can be cast. In principle, Internet voting could be used from any device, even those that are not under the supervision of the electoral authorities[6]. It is because remote electronic voting opens the door to voting from uncontrolled or unsupervised environments that it is interesting to study it from the perspective of secret suffrage. If votes are cast beyond the reach of the election administration, what ensures that they are cast in secret? What prevents that a voter is coerced or bribed when casting their electronic vote? Therefore, our focus will be on remote electronic voting, and more specifically on remote electronic voting from uncontrolled environments.

Trends on the adoption of remote electronic voting call for addressing these questions, regardless of whether "the technology has been around for over two decades and has not diffused as it was expected that it would be" (Licht et al., 2021: 92).

According to Gibson et al., "a 'political race' began in the mid 1990s to see which country[7] would be the first to allow for Internet voting in their general elections" (2016: 280). In 2007, Robert Krimmer, Stefan Triessnig, and Melanie Volkamer had "identified 139 elections in 16 countries within the time period of 1996 to the 30th of April 2007 were

voting technologies, that we will not address here, and therefore the simplified distinction is enough. Some forms of remote electronic voting, such as digital pens or voting through SMS, are not considered here since they are not currently used in public political elections.

[6] In turn, the resort to remote electronic voting does not necessarily translate as voters being able to vote from anywhere, anytime. In some cases, remote electronic voting is offered only from specific devices, which also rely on the Internet for the casting of the vote, but that are under the control of the election administration (for example, if they are deployed in voting centres, libraries, etc.). At the same time, it is possible to offer both options: general voters can cast their vote from any device, and in addition to it the election administration sets up voting centres where electronic devices are devoted to the casting of the votes by voters who may not meet the technical requirements (be it in terms of devices or connectivity) to do it from their home or any other location.

[7] The focus of this PhD will be on remote electronic voting for political public elections, that is: elections that are held at the governmental level (be it for a national parliament, local government elections, or direct democracy instruments such as referendums). In fact, the use of remote electronic voting is much more widespread among other organisations, such as universities professional associations, and political parties. For the later group, there is a recent study conducted by Adrià Rodríguez-Pérez and Jordi Puiggalí (2019). Similarly, remote electronic voting has also been used extensively by assemblies and collegiate bodies, such as parliaments (Rodríguez Pérez, and Puiggalí, 2020). Whereas our focus is on political public elections, the conclusions of this research could be in principle applied to any election in which secret suffrage is a requirement.

remote e-voting occurred" (2007: 7). Almost ten years later, Gibson et al. came up a categorisation of "different stages that countries followed in the adoption of REV" (2016: 2016). These included: promoting adoption (Ghana, New Zealand, Greece, Jordan, Nigeria, and Turkey); considering (Switzerland, the United Kingdom, Iceland, Finland, and Lithuania); small-scale trials (France, Spain, and the United Arab Emirates); large-scale trials (Australia and India); evaluating (Canada); adopted (Estonia); and rejected (the Netherlands, Austria, Germany, Kazakhstan, and Norway).

According to the International Institute for Democracy and Electoral Assistance (International IDEA)[8], remote electronic voting is currently being used in 13 countries around the world: Canada, Mexico, Panamá, and Ecuador in the Americas; France, Estonia, the Russian Federation, and Armenia in Europe; the United Arab Emirates, Oman, and Pakistan in Asia; as well as Australia and New Zealand in Oceania.

The implementation of remote electronic voting in the last two decades has spurred a considerable amount of research on the topic[9]. Since remote electronic voting "is not purely a technical issue" (Gibson et al., 2016: 280), these research spans from technologies to political, social, and legal matters. In this context, Robert Krimmer came up with the idea of the e-voting mirabilis flower to encompass a multidisciplinary approach when applying and analysing e-voting technologies: "[t]he conceptual framework […] consists of four main macro dimensions – Technology, Law, Politics and Society – that explain the areas that influence e-voting deployment" (Krimmer, 2012: 12).

Regarding the legal issues, he argued that "the legal dimension regulates how the electoral code can be changed in order to allow votes cast by electronic means and to provide necessary accountability to the voter" (Krimmer, 2012: 14). On legal matters, Richard Hill has provided an overview of "scholarly writings on requirements (doctrine), laws and principles for electronic voting systems (case law)" (2016: 125). The author has also discussed the issue of "why not allow[ing] voters to use, if they wish, an alternative voting channel that [in his opinion] does not fully guarantee secrecy" (Hill, 2016: 132-135). On her side, Leontine Loeber has identified some of the "dilemmas" of introducing electronic voting for the legislators (2017). They include general dilemmas, such as whether running experiments or not, the level of legislation and the timeframe; dilemmas regarding the scope of the legislation (i.e., division of competences, judicial procedures, and criminal law) as well as dilemma's concerning other actors, for example manufacturers and vendors. Lastly, some of these dilemmas include technical issues, including legislating for emergencies or dual systems.

More recently, end-to-end verifiability has become central to the debates on remote electronic voting, both from a technological and a legal perspective. Verifiability in remote electronic voting means two things. According to Rojan Gharadaghy and Melanie Volkamer (2010: 152-153):

> "First of all, this means that it is possible for the voter to audit that his/her vote has been properly created (in general encrypted), stored, and tallied (the so-called *individual verifiability*). Further, this means that everyone can audit the fact that only votes from

[8] International IDEA's ICTs in elections database is publicly available online: <https://www.idea.int/data-tools/question-view/743> [retrieved: 27 May 2022]

[9] Only in the context of the E-Vote-ID Conference, a total of 228 articles had been published by 2019. These include 628 collaborators, between authors and editors, since 2004 (Krimmer, Volkamer, Duenas-Cid, 2019: 3).

> eligible voters are stored in a ballot box, and that all stored votes are properly tallied (the so-called *universal verifiability*)."

Therefore, end-to-end verifiable remote electronic voting systems offer some additional guarantees by ensuring that "voters have an opportunity to verify that their vote is cast as they intended and correctly recorded (individual verifiability), and anyone can verify that all recorded voters were properly included in the tally (universal verifiability)" (Gibson et al., 2016: 281). According to Nathan Licht et al., "[o]ne of the biggest challenges from the technology side is to provide either individual or universal verifiability" (2021: 98). But many questions in remote electronic voting remain unaddressed beyond the provision of end-to-end verifiability. Our goal is precisely to address one of these issues: secret suffrage.

2. On secret suffrage and remote electronic voting

One of the key concerns about remote electronic voting is how to preserve secret suffrage. The list of authors who claim that Internet voting is incompatible with the secrecy of the vote is actually quite long. For example, Bertrand Manin has bluntly claimed that "some current practices of online voting de facto undermine the norm of secret voting that seemed well established so far" (2015: 209). Similarly, Jan Teorell, Daniel Ziblatt, and Fabrice Lehoucq (2017: 547) had argue that

> "Internet voting in private homes not 'make it *impossible* for the voter to prove how they voted to those he [sic] *does* want to know'. In other words, regardless of the exact voting technique in use, no one can prevent citizens from making a screen dump or some other printed copy of his or her vote electoral choice to display the world after the election. For citizens wanting to sell their votes or for parties wanting to purchase them, electronic voting from home presents excellent but unforeseen opportunities."

In this regard, Hubertus Buchstein has also argued that "[o]nline voting via home PCs or smartphones shifts the burden of ensuring secrecy of the vote from the electoral authorities back to the individual citizen" (2015: 16). In the opinion of this author, "[t]he widespread introduction of online voting in the twenty-first century seriously challenges the normative status of the secret ballot" (Buchstein, 2015: 16). On her side, Chantal Enguehard (2010) contends that (remote) electronic voting presents an assembly of irreconcilable [sic] properties: transparency, anonymity of votes and dematerialization of choices made by voters. Other authors are more nuanced and have framed the issue within a broader tension of "voting technologies leading to unforeseen and unintended consequences impacting election principles, such as ballot secrecy" (Essex and Goodman, 2020: 174). Assessing to what degree such claims are accurate is one of our goals.

In the meantime, the claims have found a fertile ground among electoral legislators and policymakers. Nowadays, concerns about secret suffrage are the main reason for not adopting remote electronic voting in many countries (or at least that is what they claim). For example, the Parliamentary Assembly of the Council of Europe[10] (PACE), has stressed that (2007b: 4) [emphasis added]:

[10] The Council of Europe must not be confused with the European Union (EU) or any of its bodies. The Council of Europe is an international organisation in Strasbourg which comprises 46 countries. It was set up to protect and promote democracy, human rights, and the rule of law in Europe.

> "E-voting or electronic voting is the most recent voting method to have been experimented. In this case voters express their preference using equipment derived from advanced technologies, whether an electronic voting machine or voting by Internet. The vote is not materialised on paper. Voting may take place in a supervised on in unsupervised surroundings, for instance the voter's home. Here too, the secrecy of the ballot is not fully [sic] guaranteed."

In a recent survey among the member states of the Council of Europe, 5[11] out of 32 respondents (equivalent to 14%) mentioned the "inability to (permanently) guarantee secrecy of vote" as one reason for not implementing e-voting solutions" (European Committee on Democracy and Governance, 2021b: 6). For example, the respondent(s) on behalf of the Czech Republic stated that "[a]mong the main problems [of e-voting], the following are usually mentioned: […] potential breaking of the principle of 'secret suffrage'" (European Committee on Democracy and Governance, 2021a: 16). Likewise, the Latvian respondents reported that the "Latvian IT community [has concluded] that both secret and secure e-voting is impossible at the present moment" (European Committee on Democracy and Governance, 2021a: 33).

Interestingly, Nathan Licht et al. have suggested that perceptions of remote electronic voting are influenced by "differences in the interpretation of vote secrecy and universal suffrage" (2021: 95). In their opinion, they observe (Licht et al., 2021: 95)

> "that a relatively relaxed understanding of secrecy and a strong approach towards universal access might lead to enhanced i-voting. On the contrary, where a particular emphasis on secrecy is present, further i-voting diffusion might be rejected if not enough proof is given via universal verifiability of how a vote is cast, counted and kept secret."

In fact, research on secret suffrage and remote electronic voting is far from new, even from a legal perspective. Some authors have looked at the general impact of remote electronic voting in secret suffrage in the context of national experiences. The first studies on secret suffrage and remote electronic voting came up with critical conclusions. For example, Sara Birch and Bob Watt[12] concluded that "[t]here are both legal and normative reasons for believing that remote voting is *inherently* incompatible with the secret ballot" (2004: 62) They argued that (Birch and Watt, 2004: 68):

> "the free expression of democratic preferences will be threatened if voting is transferred from the protected and controlled environment of the polling station to the unregulated and unequal domain of the home. The maintenance of traditional polling stations in parallel would be unlikely to be sufficient provision to prevent domestic vote manipulation. Those whose vote choice in the homes is controlled may well find that their choice to exit the home and vote in a polling station may also be subject to influence."

In a similar way, Kåre Vollan focused on the challenges of voting from uncontrolled environments. He concluded that in remote electronic voting "the secrecy of an

[11] These include the Czech Republic (European Committee on Democracy and Governance, 2021a: 16), Latvia (European Committee on Democracy and Governance, 2021a: 33), Lithuania (European Committee on Democracy and Governance, 2021a: 36), Portugal (European Committee on Democracy and Governance, 2021a: 51), and the Slovak Republic (European Committee on Democracy and Governance, 2021a: 63)

[12] In a previous article, Bob Watt had concluded that "[i]f voting takes place in a family group or amongst a group of friends the conscience of individual voters may be passed to another or others for reasons of group loyalty or family bound. In any of these cases the voter is, whether they like it or not, degraded just as surely as if they had been tortured" (2002: 206).

uncontrolled vote cannot be guaranteed. Even if there is a possibility to regret an uncontrolled vote and vote again in a polling station on election day, the free choice may be only theoretical for groups of voters" (Vollan, 2006: 168).

However, later studies that analysed the actual implementation of remote electronic voting in public political elections had more nuanced findings. Some examples include the study of the first stages in the introduction of remote electronic voting in Switzerland by Nadja Braun (2005). In Estonia, Priit Vinkel has also looked at the legality of remote electronic voting, with special focus on the principles of equal and secret suffrage (2015). When looking at the feasibility of remote electronic voting in Mexico, Jordi Barrat i Esteve[13] identified the following arguments based on actual remote electronic voting experiences in different countries (2012: 68-69): that the risks of remote electronic voting and secret suffrage were equivalent to those of postal voting; that multiple voting should be an option; that remote electronic voting should be considered as an additional voting channel; and, that the separate storage of the contents of the vote and identification data should be ensured.

Regarding the experiences in Norway, Jo Saglie and Signe Bock Segaard went a step further and wondered whether the introduction of remote electronic voting could affect the practice of the secret ballot. By looking at the Norwegian experience, they found that "the popular understanding of ballot secrecy differs from the legal understanding" (2016: 166), confirming some prior research about the impact of technologies in the understanding of legal principles. According to these authors (Saglie and Segaard, 2016: 165):

> "the principle of ballot secrecy is challenged when it is put to the test of concrete situations. Citizens are sceptical of attempts to influence or pressure others, or letting others vote on one's behalf. When such elements are absent, many are willing to accept that voting is observed by others. This does not necessary mean that they *themselves* would let anybody see how they voted, but indicates that a breach of the norm of ballot secrecy will not be met with social sanctions."

With the steady adoption of end-to-end verifiable remote electronic voting systems, debates about secret suffrage and remote electronic voting have resumed. For example, Jordi Barrat et al. addressed the issue of individual verifiability and whether cast-as-intended verifiability based on return codes in Norway met international standards on e-voting or was a breach of secret suffrage (2012: 40-43). At the time, return codes were combined with multiple voting, which meant that a voter could always cancel a vote cast under duress by voting again[14]. More recently, Arne Koitmäe, Jan Willemson and Priit Vinkel have examined the advantages and limitations of offering a feedback channel for remote

[13] In the original (Barrat i Esteve, 2012: 68-69):

> "[e]l secreto del voto se halla pues amenazado por el voto por internet salvo que se apliquen ciertas medidas especialmente ideadas para afrontar los riesgos descritos. Si atendemos a lo desarrollado por los países que ya utilizan la modalidad de voto por internet, comprobaremos como los argumentos son fundamentalmente las [sic] siguientes: equiparar los peligros del voto por internet con los del sufragio postal, permitir la revocación de los votos, considerar el voto por internet como un medio meramente opcional de votación y finalmente garantizar técnicamente la separación entre el contenido del voto y los datos identificativos."

[14] Jordi Barrat et al. looked at return codes as implemented in the 2011 elections, when voters had no way to know which vote had been actually included in the final tally due to the option to re-vote. As a result, they concluded that the combination of both return codes and multiple voting mitigated any concerns about vote-buying and coercion. However, "[t]he voter's opportunity to verify his/her vote was extended in the 2013 trial to improve the security system. In addition to verifying that the vote was registered correctly, it was also possible to verify that the vote was correctly stored in the database of the Internet voting system" (Saglie and Segaard, 2016: 160).

e-voters in Estonia (2021: 140). This feedback would allow them to know which is the last vote that they have cast and that has been tallied, thus providing additional verifiability. However, it would also cancel out the advantages of multiple voting by providing actual evidence of the specific vote being included in the final count.

Nowadays, on-going events and claims of espionage force us to look once again into the issue of secret suffrage in remote electronic voting. Taking into account the latest revelations on state espionage by Eduard Snowden, revisiting these debates becomes an inescapable obligation. According to Carissa Véliz, "most of what we know about mass surveillance […] we learned through the revelations of Edward Snowden, a National Security Agency (NSA) contractor turned whistleblower, in 2013" (2020: 37). What Edward Snowden revealed about the surveillance practices of national governments has clear consequences for the secret ballot in remote electronic voting. Jan Teorell, Daniel Ziblatt, and Fabrice Lehoucq have raised the issue as follows (2017: 547),

> "Taking the allegations of Edward Snowden on the expansive surveillance activities performed by the American National Security Agency into consideration, for example, this perception of non-anonymity on the Internet may also be quite extensive in the developed world. In an age where the borders between the online and the offline world are being blurred continuously, and where larger parts of people's live and activities take place in the cyber real, this might have important repercussions for the privacy of individual political preferences more generally."

More recently, the concern has shifted from national to private intelligence agencies. Ronald Deibert even speaks of an "age of private espionage" (2022). Neri Ziber has reported that "companies apply techniques as sophisticated, or perhaps sometimes more sophisticated, than U.S. intelligence agencies" (2018). Between 2016 and 2018, at least 175 people were targeted by the NSO Group's spyware according to Citizen Lab (Zilber, 2016). Nowadays, NSO Group's Pegasus spyware is all over the news: cases in Spain (which have targeted even the country's President and the Ministers of Defence and Foreign Affairs, not to mention Catalan politicians and representatives from civil society) (Manancourt, 2022), France (Henley and Kirchgaessner, 2021), the United Kingdom (Nichols, 2022), and even in the institutions of the European Union (EU) (Satter and Bing, 2022).

But espionage attempts should not be seen as an isolated concern. In fact, it is possible to speak about a wider shift in the contemporary economy towards what Shoshanna Zuboff has called "surveillance capitalism" (2019) For Shoshanna Zuboff (2019: 91):

> "commercial surveillance is not merely an unfortunate accident or occasional lapse. It is neither a necessary development of information capitalism nor a necessary product of digital technology or the internet. It is a specially constructed human choice, an unprecedented market form, an original solution to emergency, and the underlying mechanism through which a new asset class is created on the cheap and converted to revenue. Surveillance is the path to profit."

In this context, the current research will offer insights and guidance at the intersection of ongoing debates about the national and transnational dimensions of electoral principles (section II.1 below) as well as the still unsolved engagement of legal and technological regulations (section II.2). All in all, advancing existing research on secret suffrage and remote electronic voting is still necessary to fully understand, as put by Ardita Driza Maurer, "the challenge of regulating a domain at the cross-roads of law and technology"

(2013:16). The following section offers thus a first insight into these two academic debates, with a view to identify a series of aspects which are relevant from a theoretical perspective in the study of secret suffrage and remote electronic voting (section II.3).

II. A FRAMEWORK TO ANALYSE SECRET SUFFRAGE IN REMOTE ELECTRONIC VOTING: TRANSNATIONAL ELECTORAL PRINCIPLES AND THEIR INTERFACE WITH DIGITAL TECHNOLOGY

Prior to discussing how the introduction of digital technology in electoral processes may be shaping the legal principles that guide the conduct of democratic elections, and especially secret suffrage, several aspects need to be clarified. Some questions can be raised at this stage: is each interpretation of the principle of secret suffrage based on national constitutional traditions or is it possible to speak about a common, shared definition of this electoral principle? Shouldn't electoral principles be interpreted independently from the voting channels available in an election? Why should we expect that they are somehow affected by the introduction of digital technology in electoral processes? To answer these questions, we must necessarily deepen in the theories and methods that will allow us to compare how secret suffrage is being shaped by the use of digital technology in different countries.

For this analysis, we will first resort to the principles and tools of comparative constitutional law. Comparative constitutional law will help us clarify the scope of secret suffrage as our object for comparison, its function(s), as well as factors such as the nature of a principle in a given domestic order, the nature of translational sources, as well as the comparability of contexts (Jackson, 2010: 323). The theories allowing us to do so are discussed in Section II.1, where we provide an overview of some (ongoing) discussions on the existence of universal legal principles and their framing in (post)national constitutionalism. Second, in section II.2 we aim at understanding the broader trends about the regulation of digital technology and especially of the regulations related to the Internet. This approach is not only of theoretical value, but necessary for our later analysis. Hardly will we be able to develop a general explanation about legal principles and remote electronic voting if we do not first grasp the broader trends about the regulations of the Internet. Thus, the analysis in Section II.2 is devoted to understanding the main approaches towards regulating digital technologies.

While it is not our point to participate in these debates, approaching both of them will shed light on the interaction between digital technology and the regulation of constitutional principles (i.e., secret suffrage). Drawing from the conclusion in Sections II.1 and II.2, it is possible to identify some trends and open questions that will help us analyse how the introduction of remote electronic voting technologies in electoral processes may be shaping the constitutional principle of secret suffrage. This is done in Section II.3.

1. Towards postnational principles for free and fair (e-enabled) elections

National regulations are presumed to be self-sufficient and, therefore, adequate for addressing any circumstance that may require regulation. Yet, this should not preclude the existence of connections with foreign legal frameworks (De Vergottini, 2005: 12). Such is the assumption behind the so-called universalist approach to comparative constitutional law (Choudhry, 1999). Its goal is "to identify and highlight the common or universal

principles and to determine how particular constitutional jurisprudence do, or may be made to, conform to those principles" (Rosenfeld and Sajó, 2012: 12).

a) Shared principles beyond national legal traditions

The universalist search for just or good principles argues for the existence of principles of justice and political obligations that transcend the culture bound opinions and conventions of a particular political community (Jackson, 2012: 61). According to Michel Rosenfeld and András Sajó (2012), some examples of its use include those revisiting the relationship between constitutionalism and democratic politics by authors like Ulrich K. Preuss (1995) and Andrew Arato (2000); Michel Rosenfeld's essential considerations of the rule of law in different legal traditions (2001); the study by Wojciech Sadurski (2008) on the relationship of equality to legitimacy; as well as by Jeremy Waldron (2009) on the relationship of judicial review and democracy.

By resorting to the universalist approach, we should thus be able to clarify the transborder common content of a principle such as secret suffrage. In this way, this methodology will allow us to study secret suffrage with a view towards constructing a general theory of this principle, using various legal sources as examples to help refine, and to clarify, the analytics of the general problem posed by this particular requirement for democratic elections. While there are no clear methodological specifications on the adoption of this approach, common elements of previous research conducted using it will be considered with a view to replicate its more common elements and good practices.

The value of drawing on comparative experiences regarding constitutional comparation comes from different sources. Such an exercise may be aimed at (1) adopting foreign constitutional institutions into national regulations (De Vergottini, 2005: 16; Jackson, 2010: 320; Krisch: 2011: 144); (2) identifying and embracing legal principles accepted by several constitutional orders (De Vergottini, 2005: 16; Jackson, 2010: 319); as well as, (3) understanding and interpreting the role of given international institutions in the national legislation (De Vergottini, 2005: 12; Jackson, 2010: 321). Therefore, comparison here becomes of utmost importance, since our goal is not only to understand the principle of secret suffrage as embraced by several legislations, but also to understand the accommodation of such international institution in a given national legal framework.

More important, this analysis will allow us both to identify the core elements of secret suffrage as well as to study the reasons for which a given system may be considered to depart from the ideal model (and subsequently, assess the lawfulness of such departure) (Jackson, 2012: 62). In this way, we will be able to identify why certain understandings of secret suffrage are normatively more attractive and justice-seeking than others.

b) From shared legal principles to postnational constitutionalism

Even if we admit the relevance of a comparative approach to the study of the principle of secret suffrage, a doubt remains. Namely: which is the reference model against which we compare? (De Vergottini, 2005: 38). As Vicki C. Jackson has put it, implicit in resorting to such an approach "is the idea that one can agree on or develop a notion of the normative good […] a normative baseline" (2010: 321). Authors resorting to the methodology of the universalist search for just or good principles tend to take as reference model their own legislation, another country's legislation, as well as international standards on a given

subject. This task is rather complex. Since our goal is to understand the transborder nature of a constitutional principle, we cannot rely on how it is defined by a national constitution only.

Thus, prior to studying of the interplay between digital technology and secret suffrage, we will need to understand how postnational constitutional trends may be shaping the later principle. This is especially important since the end of the Cold War has driven us to a perception of a convergence of political ideas which has been encapsulated in the notion of an international community that shares common values and a stronger common normative framework. In an era of postnational politics in which the distinction between national and international politics disappears, so does the one between national and international law (Krisch, 2011: 27). As pointed out by Peer Zumbansen (2012, 77):

> "we need to ask whether or not the increasing "migration of constitutional ideas", the phenomenon of "judicial globalisation", and the impregnation of constitutional cultures through "foreign" norms and principles, while reflecting on a considerable degree of transformation, opening and "internationalization", still leaves the systematic structure intact."

By postnational we therefore mean the current scenario in which the national sphere – and even if it retains importance in regulatory matters– is no longer the paradigmatic anchor of the whole order (Krisch, 2011: 4). It is a scenario in which not only constitutional principles transcend the limits of national borders, but in which some of the assumptions behind (traditional)[15] constitutionalism are put into question. Here is where the distinction between postnational (traditional) constitutionalism and pluralism emerges. As pointed out by Nico Krisch, postnational (traditional) constitutionalism "attempts to provide continuity with the domestic constitutionalist tradition by constructing and overarching legal framework that determines the relationship of the different levels of law and the distribution of powers among their institutions" (2011: 23). On the other side, pluralism (Krisch, 2011: 23)

> "is a less orderly affair. It sees such as overarching framework as neither practically possible nor normatively desirable and seeks to discern a model of order that relies less on unity and more on the heterarchical interaction of the various layers of law. Legally, the relationship of the parts of the overall order in pluralism remains open-governed by the potentially competing rules of the various sub-orders, each with its own ultimate point of reference and supremacy claim, the relationships between them are left to be determined ultimately through political, not rule-based processes."

In this scenario, the case of human rights is of paramount importance. As Anne Peters has noted, "globalization facilitates, but also renders more difficult the fulfilment of traditional constitutional precepts. A *positive* consequence of global governance is the significant horizontal and vertical convergence of constitutional institutions and values. State constitutions are permeated by international law, notably by international human" (2007: 307).

[15] Nico Krisch does not use the adjective "traditional" to refer to postnational constitutionalism in the same way that we do. He simply establishes a distinction between "postnational constitutionalism", on the one hand, and "pluralism", on the other. Since we do not see the need for postnational constitutionalism not to be pluralist in nature, we prefer distinguishing between "postnational (traditional) constitutionalism" and "postnational pluralist constitutionalism", the latter being more often referred to simply as "pluralism".

Specifically, and as pointed out by Nico Krisch, "European human rights are often seen as a particularly good example of postnational constitutionalisation" (2011: 105). This is not a nuance if we take into account that the constitutional principle that we are analysis here, as we will see in the next chapter, is at the core of the so-called European Electoral Heritage, meaning the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights) and its related standards, as well as the case-law developed by the European Court of Human Rights surrounding them.

In this regard, it is generally accepted that compliance rates by Council of Europe's member States with the judgements of the European Court of Human Rights are high, and national courts in many jurisdictions refer to the Court's case-law often. At the same time, however, when constitutional courts were consulted about whether they were bound by the rulings of the European Court of Human Rights, 21 out of 32 respondents declared themselves not bound by Strasbourg rulings. In this way, as Nico Krisch has suggested (2011: 111),

> "the ECtHR has, over the almost fifty years of its existence, gained remarkable authority; that its judgements enjoy high rates of compliance; and that they are now regularly cited by national courts in many, perhaps most member states. Yet this ever close linkage between the national and European levels of human rights protection has been accompanied by reservations in many national legal systems, and in remarkably similar terms. As a result, it is no longer useful to see domestic and European human rights law, in the classical domestic/international dichotomy, as different legal orders."

This has been the result, mainly, of two strategies by the European Court of Human Rights: first, an evolutive approach to implementation on national level, being initially more permissive about national deviations from human rights standards. Second, what is known as margin of appreciation. Based on this doctrine, the Strasbourg Court has limited the stringency of the proportionality tests by deferring them to the judgment of member States. In this regard (Krisch, 2011: 140),

> "the Court usually emphasises the degree of consensus among member states, and on particularly contentious issues it has indeed stepped back to await the crystallisation of a common European approach and has sought to respond to political movement within the member States concerned."

2. Digitising the law? Regulating (electoral) practices related to the Internet

Knowing that a shared understanding of secret suffrage across constitutional traditions can be found answers our first question. However, the issue of whether digital technology impacts legal principles is still unresolved. We need to know why, if so, electoral legal principles may be affected by the introduction of digital technology. The second trend that we need to approach is therefore related to digital election technology and its regulation. Since the early nineties, legal practitioners have been extensively discussing how to better regulate the Internet and its related fields[16].

[16] To identify such positions, we need to grasp the discussions in several debates related to the nature of Internet whose contribution is of value to our study. First, there is the debate on the nature of cyberspace and its regulation. Second, the so-called cyberlaw debate, which centres on whether there should be a branch of law devoted to the regulation of cyberspace and/or to the

If we would align the different stances about the regulation of cyberspace across an axis, one could position on one side those scholars who argued that cyberspace cannot be regulated at all. These authors are generally branded as belonging to the cyberlibertarian school[17]. On the other side, and completely opposite to the former, we would have those

aspects related to computing and/or to the Internet, whose positions mostly draw from the assumptions of the former. Although these two debates have been described as distinct, they do not operate independently. On the contrary, they interact: many of their foundations are shared and feed each other. Chronologically, both debates also take place in parallel, whit their origins being traceable back to 1996. Furthermore, their most prominent figures end to have stakes on both debates.

Most salient issues include (but are not limited to) data protection, computer misuse, and computer evidence, copyright and digital rights management and/or criminal content liability and defamation, to name just a few examples.

[17] Cyberlibertarian or Cyberanarchist School has been the term used by authors such as Jack L Goldsmith (1998) or Andrew D. Murray (2011b) to describe the first thinkers of this movement. Other terms, such as "regulator sceptics", are also used. The origins of the debate can be traced back to John Perry Barlow's Declaration of the Independence of Cyberspace (1996). In his declaration, the founding member of the Electronic Frontier Foundation and the Freedom of the Press Foundation declared (Barlow, 1996),

> "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."

With the Declaration, John Perry Barlow established the foundations of the so-called cyberlibertarian school. Their basic principles state the following: first, "cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communication" (Barrow, 1996). As the author claimed, "[c]yberspace is no matter but thought" (Barrow, 1996). Second, and as a result, cyberspace has no geography. As argued by David R. Johnson and David Post, "[g]lobal computer-based communication cut across territorial borders, creating a new realm of human activity and undermining the feasibility -and legitimacy- of laws based on geographical boundaries" (1996: 1370-1371). Since cyberspace is not based on matter, but on thought (Johnson and Post, 1996: 1370-1371):

> "[m]essages can be transmitted from one physical location to any other location without degradation, decay, or substantial delay, and without any physical cues or barriers that might otherwise keep certain geographically remote places separate from one another […] The system is indifferent to the physical location of those machines, and there is no necessary connection between and Internet address and a physical jurisdiction."

Thirdly, cyberspace is not only a different space from a factual dimension, but also from a normative one. According to John Perry Barlow, "[national governments] have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours" (1996). As a matter of fact, this point would have been better described by one of the detractors of the so-called cyberlibertarian school. In this sense, according to Jack L. Goldsmith, "[regulation sceptics] argue that because cyberspace transaction occurs "simultaneously and equally" in all national jurisdictions, regulation of the flow of this information by any particular national jurisdiction illegitimacy produces significant negative spillover effects in other jurisdictions" (1998: 1199).

Out of these principles, a logical conclusion emerged: cyberspace cannot be regulated. On his side, John Perry Barlow stated that "legal concepts of property, expression, identity, movement, and context do not apply to us […] We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge" (1996). On their side, David R. Johnson and David Post have also concluded that "[c]yberspace requires a system of rules quite distinct from the laws that regulate physical, geographically-defined territories" (1996: 1367). This would be the result of four key factors or trends related to the non-geography of cyberspace, as identified by David R. Johnson and David Post: (1) the power of local governments to assert control over online behaviours is limited if not null; (2) the effects of online behaviour on individuals of things; (3) the legitimacy of a local sovereign's effort to regulate global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply. To sum up, and since "the new online sphere is cut off, at

authors who claim that Internet regulation is no different than *meatspace*[18] regulation. That is the position adopted by many scholars in what could be called the cyber-realist school[19]. In between both ends, several positions have been emerging that claim that cyberspace has a specific nature and thus requires tailored regulation.

From these debates, two main lessons can be drawn that are relevant for our work. First, we need to understand the regulatory power of code, and how software code can modify the behaviour to the same extent (if not even more) than other regulatory sources, such as the law, norms or the market. Additionally, and following from this lesson, special

least to some extent, from rule-making institutions in the material world and required the creation of a distinct law applicable just to the online sphere" (1996).

Yet, and contrary to the qualification received by later authors, cyberanarchists were not anarchists. As they themselves acknowledged, "cyberspace is anything but anarchic; its distinct rule sets are becoming more robust everyday" (Johnson and Post, 1996: 1389). Instead, it would be appropriate to rather call them cybercommunitarists. At the heart of their approach laid the idea that "the Net can develop its own effective legal institutions" (Johnson and Post, 1996: 1387). Similarly, John Perry Barlow concluded that "[cyberspace is] forming [their] own Social Contract" (1996).

[18] The term *meatspace* is usually associated to John Perry Barlow, although it was not used in his declaration to refer to the non-cyberspace. As a matter of fact, authors tend to use "realspace" as the flipside of cyberspace. In our case, and since the distinction between "realspace" and "cyberspace" carries not only a descriptive but also a normative overtone (isn't cyberspace real as well?), we will be using *meatspace* instead.

[19] Criticism against the cyberlibertarian school arrived earlier on, both in terms of their conception on the nature of cyberspace (the first debate) and also regarding the emergence of a new field of law aimed at regulating it (the second debate).

Regarding the former, its representatives argued that "from the perspective of jurisdiction and choice of law, regulation of cyberspace transactions is no less feasible than regulation of other transnational transaction" (Goldsmith, 1998: 2010). Existing institutions, such as technical standards or informal norms, can condition cyberspace's networks and communities (e.g. by limiting who has access to them, blocking access to certain information or performing compliance monitoring functions). More important, the possibility of extraterritorial and multiple regulation remains.

But the fiercest criticism came from the ideas related to the second debate: that of cyberlaw. The first and foremost contribution was the one by Judge Frank H. Easterbrook, who claimed that "most behaviour in cyberspace is easy to classify under current property principles" (1996: 210). According to Judge Easterbrook, studying cyberspace and its dynamics independently, isolating the subject from the rest of the existing law, makes any assessment weaker. He did not claim that the emerge of Internet had no impact over existing practices. Notwithstanding, Judge Easterbrook suggested that "[i]f something about the nature of cyberspace has made application of the distribution right cloudy, then by all means clear it up again, so that people may make their own arrangements" (1996: 211).

Therefore, the problem was not so much whether cyberspace could be regulated (which, he claimed, could be) but on identifying the principles that should inform both *meatspace* and cyberspace regulations. More important, what was needed was "to bring the Internet into the world of property law" (Easterbrook, 1996: 212)

This idea was further developed by Joseph H. Sommer (2000). He claimed that "most legal issues posed by these technologies are not new at all and that existing law is flexible enough to deal with such issues" (Sommer, 2000: 1145). He backed on the idea that technology was not enough to transform regulation, but that "the connections between law and technology are almost always mediated by social practice" (Sommer, 2000: 1147). As Judge Easterbrook, Joseph H. Sommer agrees on the fact that when applying "old" law to cyberspace, some matters may afresh. Yet, legal principles should still apply. As Joseph H. Sommer has argued (2000: 1158-1159),

> "[m]any of the legal problems of the present were seen in the past. The law -especially the common law- tend to be conservative, accretive, and inductive as opposed to revolutionary, novel, and deductive. […] New information technologies are not likely to produce new fields of law, but they are likely to encourage legal analyses that incorporate, expand and generalise on what came before them."

attention must be paid to how to translate to electronic voting channels those electoral principles that were designed with paper-based elections in mind. The third lesson that is relevant is that cyberspace trends and regulations also impact realities based on paper.

a) Regulation based on code

One of the main figures emerging from the debates on the regulation of cyberspace is Lawrence Lessig. By positioning himself on the two debates, Lawrence Lessig was able to synthesise them both. This is so because, as he argued, "from thinking in particular about how law and cyberspace connect [can we think] about the limits on law as a regulator and about the techniques for escaping those limits" (Lessig, 1999: 502).

According to Lawrence Lessig, law is just one among several tools that society has at hand for affecting constraints upon behaviour. Being based on code[20], cyberspace may limit the reach of law. Yet, he argued, not only the nature of cyberspace is not fixed but also can governments take steps to change its architecture, including with the controls it enables. According to Lawrence Lessig, the contrary assumption (that of the cyberlibertarians) is flawed: "code can change, either because it evolves in a different way, or because government or business pushes it to evolve in a particular way" (Lessig, 1999: 506). Lawrence Lessig developed a framework for understanding how behaviour regulation worked based on four modalities or constraints: (1) law, which orders people to behave in certain ways; (2) social norms, which works as law but on the grounds of a decentralised punishment system; (3) markets, which regulate by price; and, finally, (4) architecture[21], by which he meant "the physical world as we find it, even if "*as we find it"* is simply *how it has already been made*" (Lessig, 1999: 507). In cyberspace, it is its architecture -namely, code- which better regulates behaviour.

Therefore, for Lawrence Lessig cyberspace is not inherently "unregulable", but its "regulability" is a function of its design. For Lawrence Lessig, some designs make behaviour more regulable, while others make it less regulable. In its current design, code sets the features of cyberspace, and these are features selected by code writers. Therefore –and whereas the "regulability" of cyberspace depends upon its architecture– this architecture can be changed. Since there are different sources of regulation, it is possible as well that in a given setting the regulations set up by code and the ones from the law are in conflict. According to Lawrence Lessig, "where architectures of code change the constraints of law, they in effect displace values in the law. Lawmakers will then have to decide whether to reinforce these existing values, or to allow the change to occur" (1999: 522). Yet, he adds that "[t]o the extent that these code structures displace values of public law, public law

[20] Lawrence Lessig defines code as "the software and hardware that constitutes the cyberspace as it is - or, more accurately, the ruled and instructions embedded in the software and hardware that together constitute cyberspace as it is" (1999: 405).

[21] In the context of paper-based elections, the technologies that enforce secret suffrage could be understood as their architecture. For example: voting booths, envelopes, transparent ballot boxes, etc. These specific technologies of secret suffrage will be further discussed in chapter 2.

has a reason to intervene to restore these public values" (Lessig, 1999: 530). To sum up, and as it has been highlighted by Lawrence Lessig[22] himself (1999: 546),

> "[t]he threat to values implicit in the law – threats raised by changes in the architecture of code – are just particular examples of a more general point: that more than law alone enables legal values, and law alone cannot guarantee them. If our objective is a world constituted by these values, then it is as much these other regulators – code, but also norms and the market – that must be addressed. Cyberspace makes plain not just how this interaction takes place, but also the urgency of understanding how to affect it."

b) Translating laws to cyberspace and latent ambiguities

If behaviour in cyberspace can be regulated both with law and with code, and at least the possibility exists that they may be based on different normative assumptions and values, how can we make sure that laws apply to cyberspace as they do in *meatspace*? More important, can rules developed for *meatspace* can be applied *mutatis mutandis* to behaviours in cyberspace?

[22] Advancing on Lawrence Lessig's approach to cyberspace, Andrew D. Murray has more recently come up with a new approach which focuses on the community-based character of cyberspace regulation. Murray re-examines Lawrence Lessig's proposal "in which a pathetic dot is found to reside among four regulatory modalities which act as a constraint on the choice of actions of that dot" (2011b: 276). To this dot, Andrew D. Murray applies the theories of Actor Network Theory (ANT) and Social Systems Theory (SST). As a result, Andrew D. Murray ends up seeing the dot as part of a matrix of dots, namely: as part of the wider community. Thus, he realises that three out of the four regulatory dimensions identified by Lawrence Lessig (laws, norms and markets) are actually a proxy for community-based control. He therefore terms these "socially mediated modalities", reflecting an active role for the dot in the regulatory process. Therefore, "far from being a pathetic dot which was the subject of external regulatory forces, "[f]ar from being a "pathetic dot" which is the subject of external regulatory forces the dot is in fact an "active dot" taking part in the regulatory process" (Murray, 2011a: 205).

More recently, Andrew D. Murray has advanced on his initial theory, which he labels as Network Communitarianism. In his new approach, Andrew D. Murray has acknowledged that his initial model "requires to be amended to take account of the fact that the community is actually multiple overlapping matrices where individual members or nodes have membership of a number of groups" (Murray, 2011a: 211). Second, he has also introduced a distinction between capacity and legitimacy, where the latter is drawn from the acquiescence of the community. In this way, he is able to identify regulators (like gatekeepers), which may find themselves in a position to regulate, but not necessarily legitimated by the community. As it has been stated by Mark Leiser (2016: 3),

> "Murray also posited that there are clear similarities between nodal governance theory, the theory of the post-regulatory state, Lessig's theory of cyberpaternalism and his version of network communitarianism. What each hits at but does not completely address is where the divergent centres of power are to be found. This is one of the keys to effective governance in the online environment."

Therefore, Andrew D. Murray develops the idea of internet gatekeepers. In his Network Communitarianist approach, "Internet gatekeepers are being used to regulate in accordance with the traditional nodal governance model: the harnessing of communicative power by external regulators to achieve a regulatory settlement through the capture of a key gatekeeper as a regulatory proxy" (Murray, 2011: 217). Notwithstanding, gatekeepers do not occupy a position in the network equal to that of the other "dots", but their position as gatekeepers gives them regulatory capacity. According to Andrew D. Murray, "regulators are likely to rely ever more on gatekeepers as proxies in their attempts to control online activities" (2011: 213).

As a result, Andrew D. Murray concludes that when we are dealing with Internet regulation, a whole set of institutions emerge, such as governments, gatekeepers, private citizens un positions of power, multinational companies, local authorities, lobbying groups and/or organisations, etc. each of them with a given capacity and legitimacy to regulate cyberspace.

According to Gregory N. Mandel, one of the lessons that can be drawn from experiences with law and (digital) technology is that "pre-existing legal categories may no longer apply to new law and technology disputes" (2017: 227). In the opinion of this author, "there often appears to be a strong inclination towards handling new technology disputes under existing law" (Mandel, 2017: 238). For example, he describes how with the advent of the telegraph new rules had to be drafted. First, courts "analogized the delivery of a message by telegraph to the delivery of a message (a letter) by physical means, and because letter carriers fell into the pre-existing legal category of common carriers, the court classified telegraph companies as common carriers as well" (Mandel, 2017: 229). In the long term, it became evident that "telegraph messages to be a new form of message delivery distinguishable from prior systems" (Mandel, 2017: 229).

Another lesson stressed by Gregory N. Mandel is that "the types of legal disputes that will arise from new technology are often unforeseeable" (2017: 227). One example is "the "horseless carriage" to which people reverted when confronted with the unprecedented facts of the automobile (Zuboff, 2019: 12). According to Shoshana Zuboff, "[w]hen we encounter something unprecedented, we automatically interpret it through the lenses of familiar categories, thereby rendering invisible precisely that which is unprecedented" (2019: 18).

Applying these pre-existing legal categories of laws developed for *meatspace* to cyberspace may result in what Lawrence Lessig has defined as latent ambiguities. According to Lawrence Lessig, latent ambiguities emerge when "[i]n the original context, the rule was clear […] but in the current context, the rule depends upon which value the Constitution was meant to protect. The question is now ambiguous between (at least) two different answers. Either answer is possible, depending upon the value, so now we must choose one or the other" (2006: 25). Lawrence Lessig was able to identify several latent ambiguities in the regulation of cyberspace, including issues related to intellectual property, privacy, and freedom of expression. As we will see in the next pages, applying laws that have been designed with paper-based voting methods in mind to remote electronic voting also raises latent ambiguities. Interestingly, most of them are actually related to secret suffrage.

To sum up, pre-existing legal categories may neither be necessary nor sufficient when it comes to regulating behaviour in cyberspace.

c) The infosphere

So far, we have addressed *meatspace* and cyberspace as two distinct realities. However, it can be argued that what happens now in cyberspace can also shape our behaviour in *meatspace*. As Manuel Castells has put it, "at the end of the twentieth century, we lived through one of these rare intervals in history. An interval characterized by the transformation of our "material culture" by the works of a new technological paradigm organized around information technologies" (2010: 28). According to this author (Castells 2010: 406),

> "the new communication system radically transforms space and time, the fundamental dimensions of human life. Localities become disembodied from their cultural, historical, geographical meaning, and reintegrated into functional networks, or into image collages, inducing a space of flows that substitutes for the space of places. Time is erased in the

> new communication system when past, present, and future can be programmed to interact with each other in the same message."

In this regard, the regulation of digital technologies and cyberspace should take also into account that *meatspace* becomes digitally infused: "the digital is spilling over into the analogue and merging with it" (Floridi, 2007: 6). This results in what Luciano Floridi has defined as the "infosphere", that is: "the whole informational environment constituted by all informational entities, their properties, interactions, processes and mutual relations" (2007: 3). For Luciano Floridi, cyberspace becomes only a subregion of the infosphere, since it also includes the off-line and analogue spaces of information. The impact of ICT is blurring the threshold between what previous approaches considered what the *meatspace* and the cyberspace were.

More important, this process is not neutral[23]. Thus, regulatory approaches to the cyberspace need to be reused also in the other subregions of the infosphere. As Corinne Cath and Luciano Floridi have put it (2017: 454),

> "[t]echnology is not neutral. Technology, by its very nature, is inherently connected the practices of its use. Such practices are embedded in culture, which means that technology cannot be detached from the context in which it is applied and, by extension, its ethical and legal principles."

3. A non-originalist perspective towards secret suffrage in remote electronic voting

As we have seen, technological change has a great impact on law. It "raises new questions concerning the legitimacy of laws, individual autonomy and privacy, deleterious effects on human health or the environment, and impacts on community or moral values" (Mandel, 2017: 226). More important, as the lessons in the previous section have shown, the emergence of a technology such as cyberspace may even prevent law from achieving its very goal: regulating human behaviour. Our analysis has also shown that these effects are magnified when digital technology meets constitutional standards closely linked to human rights, such is the case of the right to vote (and, therefore, the principle of secret suffrage).

Therefore, it becomes necessary that we approach the subject of our analysis from a non-originalist perspective. While traditional originalist approaches to comparative constitutional law believe that legislation should be interpreted consistently with the intent of, or the meaning it had for, its framers and are more prone to concentrate on historical analysis, non-originalist approaches are rather preoccupied with how best law can be adapted to fit the needs of the current generation (Rosenfeld and Sajó, 2012: 17). Our analysis allows us to outline three main trends about how the introduction of digital technology in electoral processes may be reshaping the traditional configuration of secret suffrage as a constitutional principle for democratic elections. Based on what we have seen so far, the following three trends will be outlined: (1) the relevance of new regulatory structures; (2) the proliferation of regulatory agents; and (3) the emerge of new social practices.

[23] Neither is code neutral. "As sites of control over technology, the decisions embedded within protocols embed values and reflect the socioeconomic and political interests of protocol developments" (DeNardis, 2013: 10).

Regarding the relevance of new regulatory structures, we can see the influence of two new frameworks. On the one hand, international laws in addition to national ones. Furthermore, regulatory structures different from laws as such (including code, norms, or even the market) need to be taken into account. In this regard, and as the literature on the European human rights regime shows, even in countries generally regarded as examples of the constitutionalist story, progress in the direction of a unified, well-ordered law with the European Court of Human Rights at its top is not unequivocal (Krisch, 2011: 126). In this regard, observance of international standards by domestic legislations does not indicate the emergence of a unified, hierarchically ordered system along constitutionalist lines (Krisch, 2011: 151). This is not limited to human rights. Overall, postnational constitutionalism seems to be characterised by a pluralism that "acknowledges that a relationship may be governed by competing rules from a number of […] layers" (Krisch, 2011: 77-78), such as national and international layers, but also regionally, personally or functionally defined layers.

More important, and in parallel to the previous phenomenon, such progress seems to be guided not only by traditional hard law instruments -such as treaties- but "dense cooperation in government networks […] largely uses 'soft' instruments […] relies on consensus and non-binding commitments that leave all actors formally free" (Krisch, 2011: 228). The focus on "soft" instruments is of paramount importance for the study of electoral principles, such as secret suffrage (as it will be seen in chapter 3). Beyond soft-law as traditionally understood in the field of law, it will be important to also look at the guidelines and standards setting the architecture of cyberspace as an important regulatory structure when it comes to remote electronic voting.

Second, and linked to the proliferation of regulatory agents, it can be argued that there is a "dispersal of capacitates and resources relevant to the exercise of power among a wide range of state, non-state and supranational actors" (Scott, 2004: 145). Our broader understanding of law (meaning both hard and soft-law) and our focus on code as a regulatory modality means that the number of agents involved in behaviour-making is also broader. From constitution-making in a narrow sense, we may need to take into account the regulatory agency of the international fora, of technical agencies within governments that may have little to do with electoral frameworks, and even of the code architects and writers themselves when regulations on remote electronic voting are not detailed enough.

Similar situations have been identified when it comes to the postnational legal order. In this regard, it is worth noticing the role that courts have played in shaping international rules, especially in the case of the European human rights regimes. In this regard, not only international courts have taken on such role, but also domestic and internationals courts have dialogued on the degree of obligations at each level. As Nico Krisch has pointed out (2011:126),

> "[t]he challenges to the constitutionalist narrative are not only factual, in that domestic courts sometimes do not follow Strasbourg judgements, evade them or misinterpret them. They are instead of a principles nature: domestic courts assert a power to decide on the limits of the authority of the ECtHR, and because of the very vague indications as to when this power con be exercised, it appears as essentially discretionary."

Nico Krisch argues that if the different layers of law have come together, "the interaction between courts has been central to these relations" (2011: 286). Other authors, such as Neil MacCormick, have even claimed that (1993: 10)

> "from a jurisprudential point of view, there is no compulsion to regard 'sovereignty,' or even hierarchical relationships of superordination and subordination, as necessary to our understanding of legal order in the complex interaction of overlapping legalities which characterises our contemporary Europe, especially within the European Community. Sovereignty, if it exists or is in issue at all, is not made necessarily in issue by reason of the very fact that we have law."

As we will see later, the role of constitutional courts has been crucial in many countries that have aimed at introducing internet voting, and it is likely to continue when it comes to assessing the role of digital election technology *versus* constitutional principles, such as secret suffrage.

At the same time, postnational constitutionalism neither precludes the role of private agents in postnational regulation. If any, they are rather concerned about the normative dimensions of such private regulation. As Nico Krisch puts it, ""[p]rivate regulation may easily fail to satisfy public autonomy demands-it typically represents rule-making efforts by corporate actors without broader civil society input or a link to domestic political processes. [Yet, at the same time he acknowledges] Some forms of private regulation may be able to make more plausible claims" (2011: 102).

Lastly, we have also acknowledged that the emergence of an infosphere has brought about a new scenario in which "dots" –as regulatory agents ranging from public administrations to individuals and including with private operators– set the regulatory framework of cyberspace. This is the idea behind the theory of the active dot, but it is not limited to the approaches of network communitarianism or the regulatory gravity theory. Other scholars, including those belonging to cyber-realism, already pointed towards the role of individuals in mediating between law and digital technology. In a similar fashion, Gregory N. Mandel has developed a clear idea on how (digital) technology and law are mediated by social practice. As he puts it (Mandel, 2017: 231),

> "[l]egal categories are not developed based simply on the function of the underlying technology, but on how that function interacts in society. Thus, rather than asking whether a new technology plays a similar role to that of prior technology […], a legal decision maker must consider the rationale for the existing legal categories in the first instance. Only after examining the basis for legal categories can one evaluate whether the rationale that established such categories also applies to a new technology as well."

Additionally, the relevance of social practices in mediating law is not limited to those ventures which involve the use of digital technology. There is also mediation when it comes to transnational legal principles. As pointed out by Nico Krisch, "for a rule of recognition to be in place it needs to be generally accepted by decision-makers and public officials" (2011: 11). As a result, in a postnational order it is "the public autonomy of citizens, not abstract moral considerations, [which] carries the central burden" (Krisch, 2011: 96).

III. THE RESEARCH AND THE PHD

1. Our contribution

All things considered, our research is quite novel. First and foremost, our starting point is not based on pre-existing legal definitions that are accepted as given. This is legal research, but our definition of secret suffrage is not based on the provisions of national constitutions

or electoral laws. When we speak about secret suffrage, we have something else in mind: its shared understanding between and across countries. Drawing from the universalist approach to comparative constitutional law, we understand that the principle of secret suffrage exists in such a way that it transcends the culture bound opinions and conventions of particular political communities. Therefore, we understand secret suffrage as an international or transnational principle that, regardless of differences in their implementation[24], presents a core understanding that is shared across different national legal traditions. That is why our national case studies –Switzerland, France, and Estonia– are compared between them and against international standards. Moreover, and taking stock of the contribution by postnational constitutionalism, we understand that this core understanding must be found in a hierarchy of legal sources, spanning from hard and soft law, and including technical standards as well.

Second, we also take a wider approach at the enforcement of this principle. Secret suffrage may be enforced through law, code, norms, and even the market. In fact, we reject the idea that technologies only enforce legal principles. Instead, the legal and the technological dimensions interact with each other, redefining what may have been considered as given. This is the reason way the contribution of Lawrence Lessig's theory about the regulation of cyberspace is so important here: because it helps us identify other sources of behaviour control beyond the legal framework *strictu sensu*. More important, it also helps us pinpoint latent ambiguities that may emerge as a result of translating legal principles from *meatspace* into cyberspace. We will argue that the legal definition of secret suffrage has shifted as a consequence of the introduction of digital technology in electoral processes –any, not just e-casting, technologies. The question that must be asked from a legal perspective is therefore to what extent this shift in the legal principle is in line with the original goals that the principle was aimed at achieving.

Therefore, and while we acknowledge that there is already a (substantial) body of research –both on remote electronic voting as well as on the interplay between remote electronic voting and secret suffrage– we also sustain that "[t]he issue of regulation of election technologies is [still] a new area of governance that will likely grown in importance as elections around the world digitize" (Essex and Goodman, 2020: 176). By offering a comparative assessment of secret suffrage and remote electronic voting, this research aims to go beyond specific case studies about Internet voting (be they focused or not on secret suffrage), as well as on the broader interaction between (international) electoral principles and digital technologies.

2. On the methodology

Methodologically, the project will be based on comparative methods. Comparative methods are chosen because of "its capacity to go beyond descriptive statistical measures, towards an in-depth understanding of historical processes and individual motivations" (della Porta, 2008: 202). Paraphrasing Donatella della Porta, our goal is to understand secret suffrage in Internet voting as "a complex unity rather than establish relationships between

[24] For example, Ardita Driza Maurer notes that "[e]ven for terms that are used in one context alone (legal terms such as vote secrecy), attention should be paid to distinguish between different ways to implement the same term in different countries" (Driza Maurer, 2013: 15). More specifically, the different ways in which absolute and relative or conditional secrecy is implemented will be assessed throughout these pages.

variables" (2008: 204). Following Max Weber, we could say that the research is aimed at building an *ideal type* for secret suffrage, that is: an "idea", a "unified ideal construct", "abstracted out of certain features" (1949: 91). To that end, the project focuses on three case studies where Internet voting has been used for the last two decades: Switzerland, France, and Estonia[25].

The choice of the three case studies provides a comprehensive and balanced approach to the study of our research topic. Switzerland offers a unique set of data, having organised more than 300.000 electoral events since remote electronic voting was first used in 2003. Switzerland is in fact one of the first countries that has adopted Internet voting for politically binding elections. In turn, the pave of the adoption of remote electronic voting in the country has not been steady, and we can observe attempts to stop and discontinue the use of this channel both at the cantonal (as in Geneva[26]) and national levels (as in the current situation). Lastly, the main voting channel in the country is currently postal voting (with rates of up to 85% of the votes being cast by post) which may explain why secret suffrage has not been as central in the discussions about remote electronic voting if compared to other countries.

France also provides some relevant insights[27]. A pioneer in the introduction of remote electronic voting as well, the country has been experimenting with this technology that has been offered to voters abroad for different contests: first for the elections to the Assembly of French Citizens Abroad, followed by the elections to the National Assembly and the representative bodies of French citizens abroad. The decision not to offer remote electronic voting for the 2017 as an exception to this process of steady adoption also offers some food for thought on this case study. More interestingly, France remains the only of the three case studies where cast-as-intended verifiability is not being offered (although it has been recommended and considered a requirement for some elections). If we take into account some claims that remote electronic voting may be generalised any time soon, studying this experience may also throw some light on the debate about verifiability and secret suffrage.

Lastly, it is not an option not to study Estonia in a research project about remote electronic voting. The country remains to date the first and only European experience where remote electronic voting is offered to all the population, for all contest: national, local, and to the European parliament. When it comes to secret suffrage, the country has adopted quite an innovative approach to understand the constraints imposed by this

[25] Throughout the research we list the three case studies based on chronological parameters, depending on when they first used remote electronic voting: Switzerland in January 2003 (in the *commune* of Anières, in Geneva), France in June 2003 (with a pilot project for the partial election of the *Conseil supérieur des Français de l'étranger*), and Estonia in October 2005 (for local government councils).

[26] In Geneva, the piloting of remote electronic voting was stopped during 2005-2007 since opponents claimed that without a proper legal basis this voting channel should not be used (Germann and Serdült, 2017).

[27] The choice of France has been challenging. Even if the country has a legal framework for remote electronic voting since 2003, the information that exists is scarce. It has been highlighted by some researchers. For example, Régis Dandoy and Tudi Kernalegenn have recently concluded that (2021: 2)

> "Internet voting has also been largely overlooked in the literature, especially the French context and for external voting […] the literature on Internet voting from abroad remains in its infancy […] This includes the French case since another type of electronic voting –the DREs or machines à voter'– has attracted most of the academic attention on this country."

principle. From the outset, the country has advocated for a teleological interpretation of secret suffrage, but without understanding that the electoral administration has no role in ensuring that votes can cast their votes secretly even when voting from unsupervised environments. As a result, Estonia is the only of the three case studies where voters have the option to cast several electronic votes[28], and can even cancel any electronic ballot they have cast by casting a paper ballot in polling stations. In the last elections, they could even cancel their electronic ballot on e-day, something that was not possible until then as it could have breached the principle of equal suffrage by creating different options for advanced paper-based and remote electronic voters.

In addition to the three national case studies, the research is complemented with a detailed analysis of international electoral standards. By looking at the international standards, it is possible to find the common elements to secret suffrage that travel across the tree national legal traditions: a "unified ideal construct" of secret suffrage and remote electronic voting in the European Electoral Heritage. More specifically, we will look at the Council of Europe's Recommendation(s), which remain to date the only intergovernmental source in the field. Additionally, we also look at the methodologies and election observation reports by the OSCE/ODIHR. By identifying the issues that need to be observed when electoral technologies are used, the OSCE/ODIHR shows which are the values that a democratic election must meet (i.e., the electoral principles) and the mechanisms that may help contribute to complying with those values.

For all these cases, data has been gathered from primary sources such as the international standards themselves, national legal instruments, as well as case-law. This data has been complemented with secondary sources, such as election observation and assessment reports, legal analysis, as well as academic publications and articles. The data has been triangulated with the findings from the primary sources, the literature review, and among them.

3. About the structure

The remainder of this research is organised around four main chapters and the conclusions section. The two following chapters look at secret suffrage and remote electronic voting separately. Their goal is to understand the legal principles and the technologies in their specific context. The last two chapters bridge secret suffrage and remote electronic voting. First, by looking into the details of their interplay in the international standards and national case studies. Second, challenging some of the approaches towards secret suffrage in remote electronic voting. This challenge is two-fold: first, we have aimed at understanding the specifics of secret suffrage and remote electronic vote-casting, without falling into the trap of pre-existing legal categories. Second, we put secret suffrage and remote electronic voting in context, by arguing how secret suffrage may have to be leveraged against other electoral principles.

More specifically, chapter 2 looks at the origins and evolution of secret suffrage. We look both at the actual practices and how they have been enshrined in international standards and national legal frameworks. The goal of this chapter is to look independently at secret suffrage to understand that this is a contingent legal principle that has resulted

[28] Yet, it is not the only one. As we have mentioned above, such a possibility existed as well during the pilots with online voting in Norway in 2011 and 2013 (section I.2).

from specific national contexts. Furthermore, it will be evidenced that the way in which this principle is understood nowadays is based on paper-based voting channels. Therefore, great deal of the effort is put into coming up with a set of standards for this principle so it can be applied as well to non-paper-based voting channels. Lastly, the chapter identifies some challenges to the principle itself, some based on actual electoral practice (i.e., the resort to alternative voting methods) and also from a theoretical perspective (that is, authors challenging the normative value of secret suffrage).

Chapter 3, in contrast, focuses on remote electronic voting. The goal of this chapter is to provide a broader picture of the three national case studies: when was remote electronic voting introduced, why, how has it been regulated and how the technologies have evolved. In addition to the case studies, the chapter also looks at the international standards on remote electronic voting, understood in a broader sense. Therefore, our focus is not only on actual legal standards, but also on related practices. In this regard, the observation methodologies for new voting technologies (NVT) also helps us in looking into the specifics of secret suffrage and remote electronic voting. Following the tenets of postnational constitutionalism, this chapter also helps us identify the interplay between national and international regulatory structures. Furthermore, and to comprehend the regulatory capacities of code, we also look at some of the technical standards for remote electronic voting.

Chapter 4 then brings the two previous chapters together. The goal of this chapter is to look at secret suffrage in remote electronic voting with more detail. This is done through two separate but linked exercises. First, we look at secret suffrage and remote electronic voting in each of the four case studies (including the international standards). Second, we use the standards identified in chapter 2 for a cross-comparison of secret suffrage in remote electronic voting in terms of compliance with the dimensions of individuality, confidentiality, and anonymity.

Chapter 5 then looks at the previous findings from a critical perspective. Two main issues have been identified as part of this PhD that are challenging. On the one hand, the fact the secret suffrage in remote electronic voting tends to be regulated by analogy[29] to other remote voting channels, and particularly to postal voting. This approach fails at identifying -or even results in disregarding- the specifics of secret suffrage and remote electronic voting (i.e., the unforeseeable disputes that arise from Internet voting, the unprecedented). On the other hand, special attention will be paid to the need to rebalance secret suffrage vis-à-vis other electoral principles (i.e., to the latent ambiguities), with special focus on universal and free suffrage. Notwithstanding, and in contrast to general understandings, we will argue that secret suffrage and the transparency of elections are not irreconcilable values. Instead, they need to go hand in hand, and it is important to

[29] We understand analogy (*analogia legis* or *analogia iuris*) as a legal interpretative argument that is aimed at addressing gaps and lacunae in legal norms (Moreso and Vilajosana, 2004: 133). By means of analogy, a normative answer meant for a specific case (C1) is applied to another one (C2) that is in principle not regulated, but that is considered essentially or relevantly similar to the regulated one (Moreso and Vilajosana, 2004: 167). While this one is not the only interpretation of analogy, it is the most common in legal reasoning (Atienza, 1986: 179-180). As we will see in the next pages, regulations or principles developed for paper-based voting channels (either in polling stations or postal voting) are often applied to electronic voting because of the assumed similarity between these channels.

come up with mechanisms to ensure that secret suffrage can be observed, also in remote electronic voting.

Lastly, the conclusions provide a summary of the main findings in our research. Aware of the limitations of this PhD, we also suggest some follow-up work that could be used to complement and/or challenge our conclusions.

2. Secret suffrage: its historical and legal accounts

Secret suffrage is a "vital part of all democratic processes" (PACE, 2007a: 1). In Europe, it is understood as the right and duty of voters not to have the content of their ballots disclosed[30] (Venice Commission, 2002a: 4.a). Together with universal, equal, free and direct suffrage, it is one of the five principles that any election must observe to be considered democratic. However, how do we define and assess compliance with secret suffrage?

In traditional paper-based elections, the impossibility to trace the content of a vote to the identity of the voter who has cast it is usually ensured by physically breaking the link between the voter and their ballot when the latter is cast into the ballot box. Furthermore, confidentiality measures (such as ballot booths) may be set in place for voters to be able to make their choices in private prior to casting their vote. Nevertheless, election observation efforts such as those carried out by the PACE have "noted very different standards and practices regarding secret ballots. In some cases, secrecy is not always ensured, usually owing to national traditions" (2007b: para. 9). As a result, the Assembly concludes, "there is no uniform approach to secret voting" (2007b: para. 11). In fact, "[t]here [is] a variety of ways in which States protect the secret ballot. Many States have requirements that voters enter polling booths alone and many States penalize individuals that reveal how a voter voted" (Meagher, 2009: 362).

In the previous chapter we have already established some of the issues raised by the introduction of remote electronic voting. Amongst them, we have identified compliance with the principle of secret suffrage as a major concern. In fact, several authors even claimed that secret suffrage and remote electronic voting were incompatible. To assess these claims, we have also provided an overarching framework for the study of secret suffrage and remote electronic voting: a non-originalist perspective towards secret suffrage in remote electronic voting. Because our research is related to the regulation of a transnational principle, in between law and digital technologies, we have resorted to the universalist search for just or good principles and the theories of postnational constitutionalism to approach it[31]. In this regard, it is first necessary to identify the transborder common content of secret suffrage, its existence as a that transcend the culture bound opinions and conventions of a particular political community.

In this chapter we therefore analyse the historical origins, evolution, and current configuration of secret suffrage in the European Electoral Heritage. Despite our focus being on Europe, non-European experiences are also considered since understanding them is paramount to inform the evolution of secret suffrage. Once the historical roots of this principle are set (section I), we will focus on identifying the legal international and

[30] As we will see in the next pages, "[t]wo primary reasons support keeping the voting process secret -ensuring that voters are free from undue influence when casting their vote and ensuring the right of voters to cast their ballots in private" (Meagher, 2009: 362). According to Sutton Meagher, "voter coercion or undue influence generally can arise at two different times during the voting process: as the voter is voting and after the vote has cast his [sic] ballot" (2009: 363).

[31] Additionally, Lawrence Lessig's theories on the regulation of cyberspace and Luciano Floridi's "infosphere" will help inform the digital dimension of secret suffrage in remote electronic voting. Together, both sets of theories will allow us to cope with the relevance of new regulatory structures, the proliferation of regulatory agents, and the emerge of new social practices for secret suffrage in remote electronic voting.

European frameworks on secret suffrage and democratic elections (section II). The last section of this chapter deals with some limitations of the current configurations of secret suffrage, including how paper-based voting methods usually prevent some voters from casting their votes in secret and how certain technologies are overcoming the existing protections for secret suffrage in polling stations (section III).

I. THE HISTORICAL ROOTS OF SECRET SUFFRAGE

1. The history of the secret ballot

a) The origins of democracy: instead of elections, public deliberation

In ancient Greece[32], "[t]he Spartan *gerousia* (Council of Elders) has generally been taken to be one of the first bodies in which the vote was introduced" (Schwartzberg, 2010: 453)[33]. The Council would have come into being in c. 750 BC. It gathered aristocrats and employed formal voting methods (Staveley, 1977: 19). Since the *gerousia* was as small body, it is expected that voting would have taken place aloud, "by calling the role, each juror pronouncing his verdict" (Staveley, 1977: 77). The emergence of a popular Assembly at Sparta formally expressing itself by vote is regarded as a later development (Staveley, 1977: 21). On its side, the Spartan assembly (the *apella*) "voted by shouting. When a simple yes-or-no decision was needed, as for whether or not to go to war, the side which the presiding ephor thought shouted more loudly carried the point" (Lendon, 2001: 169). Thus, J. E. Lendon (2001: 174) argues that

> "voting by shouting in Sparta may not have been a clumsy democratic method of voting, but an aristocratic method: it ensured that men of the greatest ἀρετή would have the most say in the management of the state; it gave greater weight to the ἀγαθοί as opposed to the *κακοί*. Voting by shouting was appropriate to a state which some ancient thinkers classified as, or though approached, having aristocratic constitution."

When acclamation left any room for doubt, there was also the option to call on "citizens to divide by taking up places on either side of the arena according to their individual point of view" (Staveley, 1977: 76).

In Athens, it is also reported that formal voting would have been adopted first in the aristocratic Council of the *Aeropagus* (Staveley, 1977: 23). Notwithstanding, elections were not the only selection mechanism. Other procedures, such as conscription and sortition

[32] While we do not mean to imply that the origins of elections can be traced back to Ancient Greece, we have limited the study of the archaeology of voting to Sparta, Athens and the Republican Rome since these are "the only communities concerning whose voting procedures there exist any coherent body of evidence" (Staveley, 1972: 9).

[33] According to Melissa Schwartzberg (2010: 454), "[t]he Athenian *aeropagus* is a second possible source for the origin of counting votes". This case, however, is more complex since the role of the *aeropagus* "prior to Solon – whether it served as council or as a homicide court – remains unresolved" (Schwartzberg, 2010: 454).

from among candidates on a previously selected list (*clerosis ek procriton*[34]), were extensively used (Staveley, 1977: 34). For instance, lots were used for the appointment of the magistrates, treasurers, or the members of the Council of the Five Hundred. As a matter of fact, the list of offices chosen by direct election is known to have been smaller than the one of those selected by lot (van Reybrouck, 2016: 61). According to Erbert Samuel Staveley, elections were reserved for military offices and civil magistrates with specialised duties. Usually these were positions which required special qualities (e.g., magistrates) or dealt with matters of urgent national concern (e.g., special commissions)[35]. As it happened in Sparta, the Athenian *ekklesia*[36] (assembly) also voted openly, usually by show of hands (Elster, 2015: 8). Votes were then counted "by a hand-count (*cheirotonia*), which was always estimated[37]" (Schwartzberg, 2010: 453).

However, exceptions were made for "many specific decisions of the Assembly [that] were required by law to be ratified with a quorum of 6.000, voting by ballot and not by show of hands" (Hansen, 1991: 130). The procedures for voting under the plenary assembly were different depending upon the decision to be made. For votes on ostracism, plain pieces of tile or potsherd (*ostraca*) were used where voters could write the name of the candidate to be expelled from the polis. This procedure has been described by Erbert Samuel Staveley: "[i]n the central part of the market-place was erected a circular enclosure constructed from wooden material, in which there were ten openings. In order to cast their votes, the citizens passed through the particular opening which corresponded to their tribe and deposited their ballots in vessels inside the enclose" (1977: 89).

In case of a yes or no decision, pebbles were used instead. In this case, two voting receptacles were provided. Voters would then deposit their pebble in one of the receptacles, depending on the choice they supported. This mechanism was also used for the elections at the Council and the courts. These bodies used bronze tokens (*psephoi*), olive leaves, mussels' shells or imitation shells made of bronze to cast their ballot. For court jurors, a procedure has been also described for a yes or no decision in which they would draw a short or a long line in a waxed tablet depending on whether they supported (long line) or not (short line) the penalty suggested for a plaintiff.

It is worth noting that the secrecy provided by any of these mechanisms was far from complete. In ostracism votes, nothing prevented a voter from showing the name that they had written on the *ostraka* before casting it. When two receptacles were used, only if voters extended their hands over each of the two vessels could they hide their choice from any

[34] Erbert Samuel Staveley provides an explanation of how this process may have been used after 487 BCE: "[f]irst, each tribe selected ten of its members by lot at tribe level, and then one archon was chosen by lot from each group of then at state level" (1977: 38-39). Before 487 BCE, it is possible that direct election in the first round was used instead.

[35] Erbert Samuel Staveley (1977:103) argues that

> "the offices to which appointment was made by direct vote at Athens were few comparatively few, and the reason that this they were not thrown open to the lot along with the rest was quite simply that there was demanded of their incumbents a measure of skill and expertise which was to be found only in a select few. […] Athenians regarded an election as an opportunity to assess the relative worth of the candidate".

[36] Erbert Samuel Staveley (1977: 41) also argues that "the most vital of the electoral process was conducted at the local level, in demes or in tribes" and not by the Athenian assembly itself, except for issues and positions considered of national interest.

[37] On this matter, Erbert Samuel Staveley adds that "[t]he weakness of the Athenian system lay simply in the inevitable imprecision of the count, when large numbers of people voted in the mass by raising their hands" (1997: 114).

observer. Acknowledging this, voting procedures in Athenian courts were latter enhanced. To better preserve privacy, discs of bronze (*psephoi*) were introduced. This voting procedure is described by Erbert Samuel Staveley (1977: 97), as follows:

> "two such discs were distributed in full public view to each juror by four tellers, who had been appointed by lot before the start of the proceedings. One of these had a solid shaft, while that of the other was hollow. The two discs were placed in a special stand, in front of each juror. Then, after enquiring whether there were any outstanding objections to the evidence from the litigants, the herald called for the vote, announcing, 'The hollow token for the plaintiff (or "for condemnation"); the solid token for the defendant (or "for acquittal")'. At this point the juror took their tokens from the stand, holding them by the ends of the shafts in such a way as not to reveal which hand held the hollow token and which the solid one, and proved to the front of the court, where there stood two vessels, one of bronze and one of wood. Into the bronze urn, which had a slot in its top just wide enough to permit the insertion of a single disc, they deposited the token which represented the sense of their verdict; into the wooden urn, which was wide open at the top, they deposited the other."

Regarding the reasons behind the adoption of these voting methods, Jon Elster (2015: 8-9) identifies two main drivers. One is technical, since it was not possible to count hands or murmurs, counting tokens was always more accurate. In this regard, Erbert Samuel Staveley argues that "[w]hen voting was by ballot, it was no doubt easier to take proper precautions both to protect against the possibility of double voting and to ensure the accuracy of the count" (1977: 114). Notwithstanding, ballot voting also carried irregularities. For the case of ostracism, Erbert Samuel Staveley (1977:114) identifies instances where more than one *ostraca* had the same handwriting, which can be seen as pre-written ballots being handed to voters, especially to illiterate ones. Instances of multiple voting, in which more votes were cast than voters were entitled to vote, have been also documented (Staveley, 1977: 114-115). The second motivation would be political: these votes were secret, meaning that people could not to know how others were voting. Erbert Samuel Staveley (1977) and J. E. Lendon (2001) support this explanation.

While it is not our goal to adjudicate between these opposed claims, it seems reasonable that confidentiality and the need to mitigate coercion were some of the aims behind the introduction of secret voting methods. At the end of the day, alternative mechanisms already existed which allowed for an accurate vote count while preserving the open nature of voting[38]. This is the case, for instance, of voting pebbles as used by the Athenian assembly in its early days. The fact that secret voting was reserved for elections where the rights and status of an individual were involved (e.g., ostracism, immunity, disciplinary

[38] It is worth considering, however, whether all forms of open voting as practiced in ancient Greece (e.g., *cheirotonia* in Athens and shouting in Sparta) provided for the same degree of coercion. As J. E. Lendon argues, as compared to acclamation, "[t]he process of voting by division will have been both longer and les anonymous than voting by shouting: any coercion, be it moral or patronal, could be applied more, not less, effectively" (2001: 174). Erbert Samuel Staveley (1977: 107) provides a similar assessment for voting procedures in the Athenian democracy, since

> "they could no doubt arrange for contingents of voters in suitable numbers to come in from the outlying areas, and they could ensure that groups on sympathizers placed themselves strategically in the voting arena so as to be able to exert the maximum influence upon the hesitant and indifferent voters around them. It should be remembered that the method of voting by show of hands lent itself particularly to the influencing of the mass".

procedures, or court judgements[39]) also seems to support this latter approach. At the same time, however, if secrecy was a value to fully preserve, one would have expected the court voting procedures already described to be extended to other voting procedures, including those by the Assembly and the Council.

Voting was also common in the republican Rome[40]. The assembly elected all their annual magistrate, supernumerary officials, approved and rejected legislation, and sat in judgment as court of appeal. Voting was also common in the Senate and in the special criminal courts (*quaestiones*). Yet, voting procedures in Rome were different from those in Greece. One the one hand, the Assembly meet in several different forms[41]. On the other, voting took place in groups. According to Erbert Samuel Staveley (1977: 157), voting in the Roman assemblies changed at least twice. Initially, Romans also voted by acclamation. Acclamation would be abandoned around the first half of the fifth century BCE to exclude patricians from the voting process. Instead, oral vote would have been adopted. Erbert Samuel Staveley (1977: 158) describes this process as follows:

> "The individual member of each voting unit filed past an official known as the *rogator* (questioner), who was appointed by the presiding magistrate. As they did so, they announced their answer to the question put, or, in the case of an election, named the candidates for their choice. The *rogator* in turn recorded the votes by making a mark (*punctum*) with a sharp instrument on a large waxed table against the appropriate verdict or name."

A second set of reforms was adopted in the second half of the second century BCE. These were also driven by popular demand to reduce the influence of the higher classes when voting was open (Manin, 2015: 213). On her side, Mary Beard (2017) considers this reform as an attempt to introduce new voting methods protecting the privacy of voters. As she argues, "the conservative huffing and puffing of Cicero makes it clear that this was an ideologically loaded, democratic reform, which aimed to stop the elite putting pressure on the votes of the poor" (Beard, 2017). A similar argument is provided by Bernard Manin[42] (2015: 213).

[39] In the case of courts, more procedures were even in place to ensure an entirely secret vote "when the jurors were required to determine penalties than when they were called on to decide upon guilty or liability" (Staveley, 1977: 99), as the example of voting on waxed tables shows.

[40] By obvious reasons, none of the procedures here described were common during the Imperial Rome. In this regard, Erbert Samuel Staveley has reported that (1977: 223)

> "[a]ll things considered, therefore, the electoral contests of the imperial age bore little practical resemblance to those of the free Republic. Within a year short space of time the effective right of suffrage came to be confined to members of the Senate, and event their freedom of choice was appreciable restricted both by the *Princep*'s use of *commendatio* [publishing an official list of those whose candidature he favoured] and by the control which he chose to exercise over the composition of the lists of candidates"

[41] Erbert Samuel Staveley provides the following account of the Roman assembly (1977: 122):

> "there were at Rome from quite early times no fewer than three [assemblies] – the comitia *curiata*, in which the unit of vote was the curia, the comitia *centuriata*, in which it was the century, and the comitia tribute, in which it was the local tribe. Furthermore, the last category embraced two distinct assemblies, the tribal assembly of the whole people (comitia populi *tributa*) and the tribal assembly of the plebs, from which patricians were technically excluded (*concilium plebis*)."

[42] According to this author, "[t]he laws introducing tablets at the end of the second century BCE amounted to establishing a secret voting in the Comitia. Cicero's rhetoric about the *boni viri* should not obscure the fact that what was in question was the influence of the wealthier strata of the Roman citizenry" (Manin, 2015: 213)

Three main ballot laws introduced written voting for elections (*lex Gabinia* of 139), most judicial decisions (*lex Cassia* of 137), and legislative votes (*lex Papiria* of 130). With written voting, Romans used small wooden tables covered with wax as ballots. For elections, the tables were blank, and they had to introduce the name or initials of the candidates for which they wished to vote. In case of a judgment, a tablet was handed to them with two initials (*L* for acquittal and *D* for condemnation), and they had to cross the option that they did not support. In the case of legislative procedures, evidence seems to support that the voters were handed two tablets, one with the letter U for 'yes' (*uti rogas*) and one with the letter A for 'no' *(antiquo*), and voters cast the one containing their voting option (Staveley, 1977: 160). As ballot boxes, Romans used a large urn made of wickers or stone (*cista*). The urns were placed on top of a wooden platform, so their opening was at the level of the voter's shoulder on average.

b) The Australian and the French ballots

In spite of previous accounts of secret voting, "[t]he emphasis placed on the secrecy of casting the vote is mainly a phenomenon of the late nineteenth and twentieth centuries" (Buchstein, 2015: 19). More specifically, voting in secret was introduced "in Australia (1856), the United Kingdom (1872), the United States (1888–1892) and France (1914) to put an end to the carnivalesque atmosphere – which included rioting, drinking, cheering, booing, blocking or even kidnapping and molesting voters – that often-characterized elections with open voting" (Engelen and Nys, 2013: 491). The origins of the secret ballot are therefore usually traced back to Australia. According to Mark McKenna, the most powerful themes associated with the introduction of the secret ballot in Australia were "the vulnerability of the poor voter in nineteenth-century Britain under the system" (2001: 46). In this regard, "[m]aking it impossible to check how votes were cast, it precluded previously widespread attempts to influence voters through social chastisement or other sanctions" (Mitchell, 2008 in Engelen and Nys, 2013: 491).

The Australian ballot thus became "the most well-known way to prevent the world from monitoring a citizen's vote" (Teorell, Ziblatt and Lehoucq, 2016: 535). More specifically, "'[t]he Australian ballot' fixed upon the idea of centralising ballot production to safeguard the privacy rights of voters (Teorell, Ziblatt and Lehoucq, 2016: 535). By the late 1840s there were already advocates of the secret ballot for parliamentary elections in New South Wales[43]. Moreover, but "it was only in South Australia in the early 1850s that the issue of the ballot received the exclusive focus of liberals eager to democratise the Legislative Council" (McKenna, 2011: 51). In this regard, "the Adelaide meetings of the South Australian Ballot Association in February 1851 represent the 'earliest expression of public opinion on the subject in Australia'" (Scott, 1920 in McKenna, 2011: 52). "In 1856, the Legislative Council of Victoria passed the law that would allow voters to cast ballots in genuine secret" (Teorell, Ziblatt and Lehoucq, 2016: 535). According to Michael Maley (2018: 10),

[43] According to Mark McKenna, "'freedom of election', avoiding corruption, and the 'drunkenness and tumult' associated with open voting […] Under the ballot, the individual's 'own will' would 'become his sole law' and the elector would be free to vote according to his conscience" (2011: 53). As this author has pointed out, "the arguments put in favour of the ballot were identical to those articulated in England in the 1830s and 1840s" (Mark McKenna, 2001: 52).

> "The 'Australian ballot' as originally implemented in Victoria in 1856 has two key elements which have since been replicated in many systems of secret voting around the world: the ballot paper on which the candidates are listed is supplied by the government, with a generally uniform appearance; and eligible voters, having been provided with the ballot, are required to take it to a voting compartment where it is marked in private, with the ballot then being deposited in a ballot box along with all the other ballots in such a way that nobody can see for whom the vote has been cast."

However, Victoria's initial legislation "provided for secrecy, but because it stipulated that pre-printed ballot papers bearing the candidates' names be marked by the Returning Officer with the elector's number on the electoral roll, it allowed for the tracing and testing of votes in the case of alleged impersonation" (McKenna, 2001: 55). For Mark McKenna it is the South Australian Ballot and not the Victorian ballot that actually resembles the secret ballot used nowadays in Australia (2001: 56). According to this author (McKenna, 2001: 56),

> "[i]n 1858 William Boothby drafted the South Australian Electoral Act. Boothby's legislation provided a more complete form of secrecy by collecting and counting votes in such a wat that the vote of an individual could not be traced back to him. He also rejected Chapman's system of crossing out candidates, opting instead for a cross to be placed in a box beside the name of the preferred candidate. Both of these measures were subsequently adopted by the federal parliament in the Commonwealth Electoral Act of 1920 and were first used in the federal elections in June 1903."

Several states followed the reforms introduced in Australia and, shortly after, Britain introduced it as well in 1872[44]. In the United Kingdom, Gladstone's government passed the

[44] As a matter of fact, Mark McKenna has argued that "[t]he secret ballot was as much English as it was Australian, but it was first realised in Australia because of the lack of class impediments and strong opposition" (2001: 58). According to Philip Schofield (2004), in Britain, the secret ballot was proposed by Westminster Committee as early as 1780 (in Aidt and Jensen, 2017: 570).

In fact, "bribery had been a *corrupt and illegal practice* under British law since 1696. This meant that participants to bribery were subject to significant legal penalties (£500 until 1854 and £10 thereafter), and further that, a single proven case of bribery was sufficient to void an election" (Kam, 2017: 600). Yet, it did not prevent British electoral politics from exhibiting "a broad mix of irregularities, including vote-buying, entertaining potential voters, and intimidation" (Kasara and Mares, 2017: 638). "In 1818, Jeremy Bentham published his *Plan of Parliamentary Reform* in which he insisted on universal suffrage accompanied by the 'necessary shield of secrecy'. Bentham believed that the secret ballot would exclude the possibility of 'terrorism' and 'bribery' at the polling booth" (McKenna, 2001: 48-49). The proposal was received with fierce opposition. "Arguments against the introduction of the ballot, relied upon by Tories and Whigs alike, drew heavily on traditional English notions of self-respect and freedom, the 'national characteristics' of 'manly pride that scorns concealment, and the sturdy will that refuses to bend to coercion' (McKenna, 2001: 49).

According to Kimuli Kasara and Isabela Mares (2017: 640-641) the British Parliament's most systematic attempt to address bribery in British elections was however the Corrupt Practices Prevention Act of 1854. The Act provided a systemic definition of bribery and identified seven instances of corruption. This comprehensive definition of bribery was adopted in the Corrupt Practices Act of 1883 with little modification. Lawmakers viewed treating -the provision of "drinking or entertainment at times of elections"- as corruption distinct from vote-buying. The Treating Resolution or 1677 prohibited "excessive entertainment of voters to be given at any other place than the giver's own dwelling house". The *Treating Act and the Bribery Election Act* took additional steps in defining punishments for these electoral practices.

A final political strategy used to influence voters was more coercive -the use of threats and intimidation. The legal term used by British legislators to encompass all these different strategies was "undue influence". The Corrupt Practices Prevention Act of 1854 was the first legislation to

Ballot Act, which render compulsory the secret ballot for parliamentary and municipal elections in Britain. Cristopher Kam (2016: 601) provides a detailed account of the new procedures set by the Act:

> "The *Ballot Act* set out a detailed procedure for the conduct of elections designed to protect the secrecy and integrity of the vote. Although printed by local rather than central authorities, the ballots had to be uniform in appearance, without nothing but a list of the candidate's names arranged alphabetically on the front and room on the back for a stamp bearing the name of the constituency and date of the election. The stamp itself was to be applied to the front and back of the ballot by the presiding officer just before the ballot was handed over to the voter. The voter was then directed to a private compartment where he was to mark and fold his ballot so as to conceal his vote […] Procedures were also designed to guard against the interference of local officials. Prior to polling, for example, the presiding officer was to open the ballot box in the presence of the candidates' agents so that they might verify that the boxes were empty. The boxes were then locked and sealed."

Germany also introduced secret ballots in the seventies at the same time as universal manhood suffrage. Article 10 of Germany's electoral law mandated that "the right to vote will be exercised in person, through covered and unsigned ballots that have to be placed in an urn". However, the imperfect regulation of many details of the voting process, such as the design of the ballot and urns, still allowed politicians and their supporters to violate electoral secrecy routinely[45] (Kasara and Mares, 2017: 642).

In the United States of America[46], "[t]he Australian ballot was first adopted in municipal elections […] in the mid-1880s. By 1891, the majority of states used some form of the

define undue influence. Under this act, people were guilty of exerting "undue influence" on voters if they "made use or threatened to make use of any force violence or restraint or threatened to inflict any temporal or spiritual injury in order to induce such person to vote or not to vote (Kasara and Mares, 2017: 641)

In the end, rules for full secrecy were introduced in Britain in 1872.

[45] According to Kimuli Kasara and Isabela Mares (2017: 643)

> "German electoral law punished electoral irregularities unevenly. On one hand, German lawmakers mandated harsh punishments for vote buying, which they viewed as a particularly pernicious form of electoral intervention. People using money or gifts to buy votes could be punished under the penal code and faced up to 2 years of imprisonment. By contract, other irregularities were punished less stringently. The most striking omission of the German electoral law was the absence of any punishment for the electoral participation of employers. This resulted in unprecedent electoral intimidation by private actors in German elections, which included threats of layoffs and other post-electoral punishments. Private actors' threats were highly credible due to the observability of the vote."

[46] Before the Australian ballot, electoral corruption in the United States was widespread. The introduction in many states of the ticket system prior to the Australian ballot not only provided some privacy for voters but also stressed that the degree of secrecy should not be overstated. The issue was that parties were able to ascertain voter behaviour because they supplied voters with ballot papers (Lehoucq, 2007 in Aidt and Jensen, 2017: 574). Fredman (1968: 22, in Aidt and Jensen, 2017: 574) has described how it worked:

> "[t]he simplest form of bribery occurred when ballot peddlers or district captains paid a voter as he emerged from the polling place. To check that he actually used the ballot it was coloured or otherwise recognisable and the compliant voter was followed up to the booth"

McCook estimates that "16% of voters in Connecticut were up for sale at prices ranging from US$2 to US$20. The most corrupt 19th-century state elections are said to have occurred in New York and San Francisco. The reason was the high concentration of poor voters and recent immigrants unused to the franchise" (Aidt and Jensen, 2017: 575). "The Australian ballot, by contrast, made the state responsible for printing ballots at public expense. Ballots included candidates from all parties, were distributed only at the polls, and were marked in secret" (Kuo and Teorell, 2017: 668)

Australian ballot, and by 1912, only four former Confederate states had not yet introduced it" (Kuo and Teorell, 2017: 669). The first state to adopt the secret ballot state-wide was Massachusetts in 1888 and the last one was South Carolina in 1950. According to Didi Kuo and Jan Teorell (2017: 668),

> "[a]lthough most states had introduced printed ballot by 1890 (only Kentucky maintained viva voce until 1891) the ballots had been previously been printed and distributed by the parties themselves. Election secrecy was easy to violate, because the tickets varied in colour and size, and the party agents near the polling stations could monitor with whom the voters associated before they approached the voting window."

An alternative approach to the Australian ballot was the so-called 'French-type' or 'ballot and envelope' model[47] (Teorell, Ziblatt and Lehoucq, 2016: 535). According to Toke S. Aidt and Peter S. Jensen (2017: 569)

> "[a]nother arrangement is the so-called 'ballot and envelope' system, practiced in, for example, France, Sweden, and Spain. It requires the state to print the ballot papers, but one ballot is printed per party or candidate. The voter then choses the paper for the party / candidate he [sic] wants to cast his [sic] vote for, puts it in an envelope, and deliver it to the ballot box. This type of arrangements (and others like it) is more open to abuse than the Australian ballot, but de jure make the ballot secret."

In fact, France conducted secret elections at an even earlier stage than Australia. According to Hubertus Buchstein, "[a]lready during the revolution, most elections in France were secret. Voters were asked to cast paper ballots, produced by the candidates or their supporters" (2016: 19). In France, electoral procedures remained a well-known practice before 1690 for the appointment of municipal bodies, religious institutions or corporations, or deputies to the Estates General (Tanchoux, 2004: 10). Yet, it is in the second half of the XVIII century that elections became a common practice, its evidence growing between 1789 and 1870. Ahead the French Revolution, two big electoral experiences provide evidence of the French voting methods, namely: the provincial assemblies of 1778 and 1787, as well as the Estates General of 1789. These assemblies used alternatively open (oral[48]) and written voting, depending upon the literacy of the voters and the relevance of the issues under discussion (Tanchoux, 2004: 68). Yet, open voting seems to have remained the norm in this period.

Furthermore, the actual implementation of secret suffrage in French elections had several shortcomings. "Some of the first elections with secret voting were conducted in France during the revolution, but the implementation was inconsistent and weak, and the various French electoral always had different secrecy requirements -if any- because of different dominating views on the issues" (Elklit, 2018: 1). In this regard, and while "Alexis de Tocqueville observed that while the French electoral law of 1820 declared that the vote should be secret, it did not contain the means of implementing secrecy, which emerged

[47] As a result, there is a very diverse environment when it comes to secret suffrage. According to a recent survey of 113 countries (Brent, 2018), most countries use the Australian ballot (60.2%), while less systems are based on the French one (21.2%).

[48] Oral voting in the assemblies worked as follows (Tanchoux, 2004: 70):

> "[l]e président ou le secrétaire appelle les noms des membres de l'assemblée, lesquels annoncent à haute et intelligible voix leur option. Parfois, l'électeur se déplace au burau pour ce faire, mais aucun serment n'est imposé aux scrutateurs pour conserver secrète une voix. L'opinion est immédiatement notée."

only informally. It took the law of 1831 to institutionalize provisions for effective secrecy" (Przeworski, 2015: 100). Therefore, it is only as of 1914 that we can speak of an actual secret ballot, when "the system with a ballot booth and a standard envelope was eventually introduced" (Elklit, 2018: 2)

2. The technologies[49] of secret suffrage (in paper-based elections)

All in all, these examples show that the key driver behind the introduction of the secret ballot was to avoid certain malpractices[50], such as bribery or voter coercion, and "their democratic distortions" (Engelen and Nys, 2013: 491). Succinctly, "[t]he secret ballot was instituted to protect against voter intimidation; as such, each voter has a right to the assurance that other voters have not been intimidated into disclosing their ballots or into voting a particular way" (Jones and Simons, 2012: 350). A recent assessment of secret ballot provisions has identified three main kinds of improper influence which anyone would want to denounce (Brennan and Pettit, 1990: 329): the first is bribery; the second is blackmail; and the third is a less explicit sort of intimidation[51].

[49] By technology we understand "a regulation of human practice that comes in a certain objectified form, as a set of objects (tools, machines, buildings), as a set of more or less explicit rules of their use, as a ritual or an exemplar of conduct, or as a disciplinary apparatus" (Pels, 2000 in Bertrand, Briquet and Pels, 2006: 8)

[50] Additionally, less benign explanations have been offered for the introduction of secret suffrage as well, including turnout (Heckelman, 2000) and incumbency preservation (Heckelman and Yates, 2002) (in Davies, 2004). On his side, Adam Przeworski provides evidence that "as long as the electorate was homogeneous in terms of property or income, voting tended to be public" (2015: 99). According to Kimuli Kasara and Isabela Mares, contextual factors also played a role in the politicians' support for secret ballot. In this regard, they show that resource-constrained candidates were more likely to support the introduction of electoral reforms: "[i]n Britain, where most irregular electoral practices required money, they show that candidate who could outspend their opponents opposed electoral reforms limiting electoral bribery. In Germany, resource-constrained politicians, who supported reform, lacked the ability to enlist state employees, or private actors as their brokers" (2017: 659):

Didi Kuo and Jan Teorell also provide evidence that "procedural changes in the conduct of elections may serve the interest of political officials, either by disenfranchising part of the electorate or by making other manipulation strategies more effective" (2017: 666). According to these authors, "the secret ballot would have been adopted, along with literacy requirements and poll taxes, as a way to disenfranchise African Americans. The Republican strongholds of Northern and Western states were motivated to reduce the electoral power of newly arrived and illiterate immigrations" (Kuo and Teorell, 2017: 669). Similarly, Daniel Gingerich (2013) has found that the adoption of the Australian ballot in Brazil was motivated by a desire to disenfranchise illiterate and poor voters

[51] Geoffrey Brennan and Philip Pettit provide a description for these three forms of improper influence, as follows:

- Bribery is neutralised by a regime of secrecy, since the briber is not in a position to know whether he gets what his bribe is designed to;
- Where bribery promises a reward for supporting a politician or party, blackmail would threaten punishment for not providing such support. As blackmail is usually envisaged, the fear is that the employer or landlord or union boss (anyone enjoying power over others) will threaten to punish those dependent on him unless they vote his line; or, more subtly, that he will establish a presumption in the minds of dependants that the first to suffer in any reaction of favour would be non-supporters.
- Intimidation is the influence effected through producing in people a diffuse sense of fear about what may happen to them if they do not vote a particular line. Geoffrey Brennan and

According to Jean-Marie Baland and Jim Robinson, "[t]he secret ballot is considered a critical protection against fraud, because it undermines the ability of brokers to monitor, and therefore to punish or reward, vote choice" (in Kuo and Teorell, 2017: 666). At the end of the day, it is generally argued that "those with the most resources at their disposal are in a better position to influence the behaviour of others if such behaviour takes place in the open than if it is performed in secrecy"[52] (Manin, 2015: 214).

Notwithstanding, a more detailed account of these cases shows that variances in how the secret ballot was introduced had different impacts on the very practices that it aimed at outlawing[53]. Furthermore, some scholars have defined secret suffrage as a political technology both sufficiently autonomous from specific socio-cultural and historical circumstances to travel widely without seeming to change shape radically, and yet flexible enough to adapt successfully to many different circumstances (Bertrand, Briquet and Pels, 2006). In this regard, it is worth noticing that when introducing secret suffrage not all countries set in place the same mechanisms to protect it[54]. Even when the same technologies for the guarantee of secret suffrage have been put in place, they have not always met the same requirements. That is the case, for instance, of polling booths in the English[55] and French traditions (Garrigou, 1988). Therefore, instead of looking at the aims

Philip Pettit (1990: 331) admit that rules of secrecy probably do offer a distinctive insurance against intimidation, at least if voters can be persuaded of their effectiveness.

At the same time, Michael Maley also finds "that there are forms of pressure, especially within families, which fall into something of a grey area between illegal coercion and legitimate persuasion, but may nevertheless diminish a person's sense of freedom to vote in a particular way; and the secret ballot remains important in protecting voters from these" (2018: 6). Family voting (even if only to help disadvantaged voters) also puts repressed family members in a complicated situation, if they want to vote differently from their repressors (Elklit, 2018: 8). As we will see in section II, international standards are clearly against any form of family voting and clearly understood it as yet another form of voter coercion.

[52] In this regard, it can be argued that "voter coercion compromises not just freedom, but also equality: those who have the power to control votes through coercion are in effect able to cast multiple votes themselves, in breach of the basic principle of "one person, one vote" (Maley, 2018: 8)

[53] As we have seen, the 'Australian ballot' actually refers to a bundle of measures, the most important of which is the use of identical paper ballots, each of which lists the names of all candidates and/or parties (Teorell, Ziblatt and Lehoucq, 2016: 535). This system requires, at least, two things: first, all parties and/or candidates are listed and printed on the same ballot paper, and second, these ballot papers are printed by the state at the public's expense and distributed only at the polling stations and placed in a standard-sized urn in privacy (Aidt and Jensen, 2017: 569). Nowadays also in nearly all versions of the French ballot the state supplies voting papers as well, presenting the elector with a variety to choose from, one or several (depending on the voting system) for each party or candidate. In addition, it appears that sometimes the act of choosing the ballot is performed in the voting compartment (Israel), or behind a screen (Norway) elsewhere it occurs in full view of others (Sweden) which renders secrecy optional. And in some, parties "are still allowed to distribute their voting papers outside polling stations" (Brent, 2018: 8)

[54] For example, India adopted the secret ballot in 1971, but voting booths were only introduced in 1980 (Jaffrelot, 2006: 87-89).

[55] Yet a more striking case in the United Kingdom is the use of counterfoils on ballot papers. In spite of the adoption of the *Ballot Act* that enshrined the Australian Ballot in the United Kingdom (Teorell, Ziblatt and Lehoucq, 2016: 535), the use of numbered counterfoils on the ballot papers remained a threat to the secrecy of the vote. According to Cristopher Kam, "[t]his device was intended to facilitate a scrutiny and recounting of votes in the event that the election was petitioned, but it aroused suspicion as it theoretically enabled authorities to match voters to votes" (2016: 601).

that motivated the introduction of secret suffrage, it is also interesting to take account for the actual technologies that were used to enforce it and how they were implemented[56].

Hubertus Buchstein argues that "there is a broad consensus among defenders of secret voting to refer to a model that can be labelled 'the modernization model'" (2015: 17), the one proposed by Stein Rokkan (1961). For Stein Rokkan, regardless of the whether the Australian or French systems are used, there are two distinct elements in the provisions ensuring secrecy: "[t]he first is to make it possible for the voter to keep his [sic] decision private and avoid sanctions form those he [sic] does not want to know; the second is to make it impossible for the voter to prove how he [sic] voted to hose he [sic] does want to know" (1961: 143). These two broad practical aims have tended to be supported by reference to three higher objectives: ensuring the right to privacy of personal political beliefs; discouraging coercion of voters; and preventing corrupt vote-buying (Maley, 2018: 5).

Alternatively, Isabela Mares (2015: 134-138) speaks of three main electoral reforms or technologies that contributed to enforce the principle of secret suffrage[57]: ballot envelopes, isolating spaces, and the design of the urn. A similar account is offered by Jan Teorell, Daniel Ziblatt, and Fabrice Lehoucq (2016: 535-537). According to these authors, three dimensions or mechanisms contributed to the actual enforcement of secret suffrage: the transition from oral to written voting[58], how paper ballot themselves were printed and distributed[59], and the use of a private space or room to mark or select their choices[60].

[56] Furthermore, it is also important to stress that "[t] nominal adoption of the secret ballot, however, did not fully protect voters' electoral autonomy nor did it end all electoral irregularities" (Mares, 2015: 3). Therefore, "[a] second generation of electoral reforms adopted several decades after the introduction of voting secrecy attempted to protect voters' electoral autonomy" (Kasara and Mares, 2017: 637). These reforms prevented voters from "sway[ing] voters' choices, taking advantage of both poorly designed legal punishments for election irregularities and of flaws in voting technology that pierced voting secrecy (Mares, 2015: 3). In this regard, to Toke S. Aidt and Peter S. Jensen also agree that *de jure* secrecy may not be de facto secrecy (2017: 569).

[57] According to Isabela Mares, politicians could continue taking advantage of poorly designed legal punishments and of flaws in voting technology "because of non-standard ballot paper of different colours or shapes, because of no-standard urns (for example, a small urn which preserves the order of coting can reveal the choices of individual voters ex post), or because of the absence of a place where the ballot can be filed in and placed in the urn without outsiders being able to observe the act" (2015: 4-5).

[58] According to Jan Teorell, Daniel Ziblatt, and Fabrice Lehoucq, "[t]he first dimension concerns the transition from oral to written voting. Although other technical solutions exist and have existed, the introduction of paper ballots initially promised to breach this connection between the identity of the voter and his or her vote choice" (2016: 535).

[59] According to Jan Teorell, Daniel Ziblatt, and Fabrice Lehoucq, "[a] second dimension of reform refers to how paper ballot themselves were printed and distributed. As parties printed and distributed ballots, they varied them in size and colour, so that partisan poll watchers could monitor the behaviour of voters on election day" (2016: 536).

[60] In the words of Michael Maley, the "[p]hysical isolation of the voter" (2018: 15). According to Jan Teorell, Daniel Ziblatt, and Fabrice Lehoucq (2016: 537):

> "regardless of the type of paper ballot in use, the voter must somehow record his or her vote choice, either by ticking a box next to the party or candidate on Australian ballots or by folding and placing the ballot paper from the preferred party or candidate into a uniform envelope with the French system. […] Without a screen shielding voters, the use of a private room, or the similar arrangements, the 'curious' may nevertheless figure out for whom a voter has cast a ballot. Similarly, without a ballot box or 'urn' that mixes all votes and stores them securely until opened, elaborate systems f backward identification might still allow polling station officials or poll watchers to decipher a voter's choices."

In both cases, if secret suffrage is going to be enforced through a set of mechanisms, it may be necessary to observe how effective these mechanisms are. According to George E. Hill, "[t]he secret ballot protects voters from these disturbing interferences, not by outlawing or sanctioning the practices themselves but by making them ineffective. Its purpose was not 'not to provide penalties for such corruption […], but rather to prevent such corruption by rendering it unprofitable because uncertain" (in Engelen and Nys, 2013: 492). "The whole point is that attempts to bribery, corruption and intimidation are less likely to work if there can be no proof of compliance" (Engelen and Nys, 2013: 492).

Therefore, and as paradoxical as it may sound, secret suffrage in democratic elections calls for "transparent secrecy" (Maley. 2018: 11). In this regard, it should be possible to ascertain that pre-printed ballots are indistinguishable from each other, that envelopes do prevent curious from gazing at their contents, that spaces effectively isolate voters, and the design of the urn ensures that it is not possible to link a vote cast to the identity of the voter who has cast it.

Furthermore, the introduction of the secret ballot may have had unintended effects as well. Jon Elster raises the issue in the following terms (2015: 8):

> "[g]iven a regime of publicity or secrecy, we can ask two causal questions: Why was it adopted? What were its effects? The questions are linked, since a regime may have been adopted for certain intended effects that did in fact materialize, but many effects are either not foreseen or, if foreseen, do no enter among the reasons for adopting the regime."

This is not a nuance if we take into account that "apparently neutral institutional choices can have significant substantive effects on outcomes" (Ferejohn, 2015: 238). Evidence has been furnished that the secret ballot had *real* consequences, even if those consequences were multifaceted and occasionally unexpected (Teorell, Ziblatt and Lehoucq, 2016: 543-544). In this regard, three unintended consequences of the introduction of secret suffrage can be observed: the prevalence of coercion; a shift towards other forms of intimidation and turnout-buying; and effects on turnout.

Regarding the prevalence of coercion, Susan C. Stokes *et al.* emphasise that the Australian ballot reduced the effectiveness of vote buying in the United States and that it did so by diminishing "the observability of voter's choices" (2013: 183). Roger D. Congleton (2011: 560) has noted that the introduction of the Australian ballot "allowed votes to be cast without fear of rebuke by landlords of employers" (in Aidt and Jensen, 2017: 575). In the case of Chile, however, there is evidence that after the introduction of the Australian Ballot in 1958 vote-buying and other clientelist practices were reduced (Kuo and Teorell, 2017: 686). Notwithstanding, Christopher Kam argues that "there is scattered evidence to suggest that the ballot had fundamentally altered the dynamics of vote-buying" (2017: 602). All things considered, it is important to take into account that regardless of these reforms "vote buying and political clientelism, through which citizen political support is exchanged for material inducements, are pervasive in the world today" (Teorell, Ziblatt and Lehoucq, 2016: 545).

In this regard, there is a good deal of scholarly ambivalence as to the ballot's role in suppressing bribery at elections. One example concerns Victorian Britain. Two noted histories of the period (in Kam, 2017: 595) express that the ballot, although effectively eliminating the intimidation of voters by landlords and employers, had little practical effect

on bribery. Therefore, authors disagree on whether any reduction in vote buying is explained by the secret ballot, by the effects of modernisation in undermining the vote market, or even by a combination of both (see for instance Aidt and Jensen, 2017: 557). In the case of the United States –and using a new measure for fraud in elections to the House of Representatives from 1860 to 1930– Didi Kuo and Jan Teorell (2017: 665) find that the Australian ballot and disenfranchisement measures reduced vote buying and voter intimidation. The Australian ballot reduced voter manipulation by making it more difficult for election agents to monitor the effects of intimidation and vote-buying. Howerver, agents relied more heavily on fraudulent ballot and registration tactics, such as manipulating election registers and stealing elections at the ballot box (Kuo and Teorell, 2017: 686)

In this regard, evidence shows that ballot reform did not erase 'election fraud and corruption' but rather transformed it, "leading to the substitution of one form of corruption for another" (Teorell, Ziblatt and Lehoucq, 2016: 543-544). For example, the introduction of secret ballot in many countries resulted in a shift from vote buying to participation and/or abstention buying. As a result, the concern may be not so much about people being coerced into voting for a particular party or candidate, but by reason of having voted at all, or alternatively of having abstained (Maley, 2018: 6). Therefore, it is deemed that ballot secrecy should also pertain to whether or not a voter voted, especially as non-voting in authoritarian electoral systems can also be an expression of political (opposition) attitudes (Elklit, 2018: 1).

When it comes to the effects in turnout, Converse (1974), Rusk (1074) and Heckelman (1995) have argued that the introduction of the secret ballot would have reduced electoral turnout[61] (in Aidt and Jensen, 2017: 577). In fact, electoral turnout increased by approximately 3% following the secret ballot's adoption in the United States (Kam, 2017: 596). In the opinion of Christopher Kam, "[t]hese results are consistent with the thesis that candidates increasingly directed their financial resources away from direct bribery of voters and toward treating (i.e., the provision of food and drink) and turnout buying (i.e., paying potential supporters to show up at the polls)" (2017: 596).

II. SECRET SUFFRAGE AND THE RIGHT TO FREE ELECTIONS

Secret suffrage is a well stablished principle of democratic elections[62]. It is enshrined in several hard law instruments, including art. 25 of the International Covenant on Civil and

[61] The elimination of the vote market is, however, not the only possible explanation for a fall in turnout after the secret ballot. For example, these results may account for a shift from vote buying toward negative turnout buying (i.e., to pay expected opposition voters to stay at home). The seminal study by Cox and Kousser (1981) of newspaper reports in New York State about instances of electoral corruption before and after the introduction of the secret ballot in 1980 provides examples of this (in Aidt and Jensen, 2017: 574). It is also possible that turnout would increase as a consequence of the secret ballot. This would be the case if the expressive benefit of voting shoots up by making the act of voting private or if the secret ballot "protects" voters and gives them the freedom to vote how they like. A possible example of this is Imperial Germany where the adoption of the secret ballot was correlated with an increase in turnout. Turnout could also increase if parties start using "brokers" to deliver blocks of voters (Stokes et al., 2013).

[62] The *Election Obligations & Standards* database maintained by the Carter Center returns 48 results based on international documents, law, and treaties to the query "secret". Available at: <https://eos.cartercenter.org/quotes?action=index&controller=results&q=secret> [retrieved: 27 May 2022]

Political Rights (ICCPR). It recognises and protects the right of every citizen to " vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors" (art. 25 ICCPR).

Likewise, the principle is well stablished in human rights regional instruments, such as in article 23 of the American Convention on Human Rights. Curiously enough, there are also regional instruments that, while they enshrine the right to free elections, make no explicit mention to secret suffrage. That is the case of the African Charter on Democracy, Elections and Governance, which in its article 3 sets the obligation for the State Parties of "holding of regular, transparent, free and fair elections".

In Europe, the principle is also enshrined in the regional human rights instruments. The Document of the Copenhagen Meeting of the Conference on the Human Dimension of the Conference for the Security and Cooperation in Europe (CSCE) sets in its commitments 5.1 the value of "free elections that will be held at reasonable intervals by secret ballot or by equivalent free voting procedure". More specifically, in commitment 7.4 participating States commit to "ensure that votes are cast by secret ballot or by equivalent free voting procedure". While not in the European Convention on Human Rights itself, the principle is also enshrined in article 3 of Protocol I to the Convention. It means that citizens from member States of- the Council of Europe can lodge a complaint (application) whenever they consider that they have personally and directly been the victim of a violation of the right to vote and/or to stand for election committed by a State part to the Convention (provided they have used all the remedies in the State concerned).

1. Secret suffrage and international human rights law

Secret suffrage is one of the key principles of the right to free elections. The obligation to guarantee the secrecy of the ballot features in both Article 21(3) of the Universal Declaration on Human Rights (UDHR) as 'secret vote'[63] as well as in Article 25(b) of the International Covenant on Civil and Political Rights as elections held by 'secret ballot'[64] (International IDEA, 2014: 43).

In this regard, Sutton Meagher stresses that (2009: 361)

> "[t]he ICCPR is an important standard […] containing specific guidelines and requirements for elections that are made binding on States that sign or ratify the ICCPR. The United Nations Human Rights Committee, which oversees the implementation of the ICCPR, has not made any recommendations on the specific type of voting system that a State should implement, but supports any electoral framework that conforms to the principles contained in the ICCPR."

General Comment No 25 (57) of the Human Rights Committee has emphasised "[t]he continuous nature of the right to the secrecy of the vote, even in the run-up to election

[63] The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures."

[64] "Every citizen shall have the right and the opportunity, without any of the distinctions mentioned in article 2 and without unreasonable restrictions: […] (b) To vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors;"

day" (International IDEA, 2014: 43). According to the Human Rights Committee (1996, para. 20),

> "States should take measures to guarantee the requirement of the secrecy of the vote during elections including absentee voting, where such a system exists. This implies that voters should be protected from any form of coercion or compulsion to disclose how they intend to vote or how they voted, and from any unlawful or arbitrary interference with the voting process. Waiver of these rights is incompatible with article 25 of the Covenant."

Therefore, the United Nation's Human Rights Committee "has interpreted Article 25 as imposing an affirmative obligation on States to protect voters from […] coercion" (Meagher, 2008: 362). Furthermore, the General Comment also "adds that the voter cannot waive his or her right to a secret vote" (International IDEA, 2014: 43).

2. Secret suffrage in the European Electoral Heritage

a) The Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocol

In Europe, the right to free elections is enshrined in Article 3 of the Protocol (no. 1) to the European Convention on Human Rights: "[t]he High Contracting Parties undertake to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature".

While article 3 only imposes an obligation on the contracting parties to hold free elections, the European Court of Human Rights has acknowledged the evolving nature of this principle towards the subjective dimension of the right to free elections. It means that citizens from member States of the Council of Europe can lodge a complaint (application) whenever they consider that they have personally and directly been the victim of a violation of the right to vote and/or to stand for election committed by a State part to the Convention (provided they have used all the remedies in the State concerned).

In this sense, Article 3 of the Protocol explicitly recognises that democratic elections are to be held by secret ballot. In this sense, "the secrecy of the vote is [considered] an aspect of free suffrage, which aims to shield voters from any pressure that might result from the knowledge of his [sic] choice by third parties and, in fine, to ensure the honesty and sincerity of the vote" (Lécuyer, 2014: 76).

Notwithstanding, the provisions of Article 3 of the Protocol are not specific enough regarding how secret suffrage is to be observed. At the same time, to date there is no case law by the European Court on Human Rights on this matter (Lécuyer, 2014: 78). No application has yet been lodged directly connected with a violation of the principle of secret suffrage. As a result, and while the rights to free elections is well stablished in international and regional human rights instruments, and it is clearly identified as a requirement for the full exercise of this right, the specific content of secret suffrage is far less clear.

This obliges us to resort to alternative interpretation methods to delve into the specificities of the principle of secret suffrage. Since the adoption of the Convention in 1969, the European Court of Human Rights has relied upon the provisions of the Vienna Convention on the Law of Treaties when it comes to interpretation. Article 31(3)(c) of the

Vienna Convention provides that the relevant rules of international law applicable in the relations between the parties are germane to the context of the treaty. These "relevant rules of international law come from several sources of which the three most important are identified in article 38(1) of the Stature of the International Court of Justice [namely]: treaties, customary law, and general principles" (Schabas, 2015: 37-38). Furthermore, the Court has often cited "intrinsically non-binding instruments of Council of Europe organs, in particular recommendations and resolutions of the Committee of Ministers and the Parliamentary Assembly" (European Court on Human Rights, 1997: para. 74) as well as opinions and reports by the European Commission for Democracy through Law[65] (more commonly known as the "Venice Commission"[66]).

Some of these non-binding instruments of the Council of Europe organs have indeed provided guidance on the "measures which would guarantee secret voting for all citizens including the most vulnerable groups" (PACE, 2007b: 1). In 2002, the Venice Commission (2002a; 2002b) adopted the *Code of Good Practice in Electoral Matters: Guidelines and explanatory report*[67]. Although the Code is non-binding, (i.e., it is a soft-law instrument), "it has become the central source of reference for setting standards in elections" (Úbeda de Torres, 2017: 37). Moreover, and as we have already seen, the Court often refers to Venice Commission's documents in its case-law[68].

In its *Code of Good Practice in Electoral Matters*, the Venice Commission identifies the five principles underlying the Eurpoean Electoral Heritage, namely: universal, equal, free, direct, and secret suffrage. Regarding secret suffrage, the Venice Commission states that secrecy of the ballot is one aspect of voter freedom, its purpose being to shield voters from pressures they might face if others learned how they had voted (2002b: para. 24). It highlights that secrecy must apply to the entire procedure - and particularly the casting and counting of votes (2002b: para. 24). Furthermore, it is claimed that not only are voters and entitled to it, but that must also respect it themselves ("secrecy is not only a right but also a duty") (Venice Commission, 2002a: 4a). The Venice Commission also identifies the conditions that are to be meet for the suffrage to be secret, namely: voting must be individual; the list of persons actually voting should not be published; and the violation of secret suffrage should be sanctioned.

The Venice Commission thus prescribes that voting must be individual (2002a: 4.b). This means that "[f]amily voting and any other form of control by one voter over the vote of another must be prohibited (Venice Commission, 2002a: 4.b). The Venice Commission

[65] See for instance: Demir and Baykara v. Turkey [GC], no. 34503/97, § 75, ECHR 2008; Russian Conservative Party of Entrepreneurs and Others v. Russia, nos 55066/00 and 55638/00, §§ 70–73, 11 January 2007; Basque Nationalist Party—Iparralde Regional Organisation v. France, no. 71251/01, §§ 45–52, ECHR 2007-II; and Çiloğlu and Others v. Turkey, no. 73333/01, § 17, 6 March 2007.

[66] The Venice Commission is an advisory body to the Council of Europe whose task is to assist and advise individual countries in constitutional matters in order to improve the functioning of democratic institutions and the protection of human rights.

[67] Similarly, the Venice Commission adopted the *Code of Good Practice on Referendums* in 2017. When it comes to the secret suffrage, the *Code of Good Practice on Referendums* echoes the provisions of the *Code of Good Practice on Electoral Matters*. For this reason we will use the earlier document as a reference from now on.

[68] While the Code of Good Practice in Electoral Matters is not a legal instrument and its provisions are not directly enforceable, the European Court of Human Rights has referred to it often, including to the provisions regarding secret suffrage. For instance, in the Judgment in Sitaropoulos and Giakoumopoulos v Greece of 15 March 2015.

also points out that the lists of persons actually voting should not be published (2002a: 4.c). In the opinion of the Venice Commission, abstention may indicate a political choice, and therefore secret suffrage should not only cover the contents of the vote cast, but also whether a voter has cast a vote at all (2002b: para. 54)[69]. Lastly, it is also stressed that that non-compliance with secrecy must be punishable and that any ballot paper whose content is disclosed must be disqualified and the violations of secret suffrage should be sanctioned (2002a: 4.a).

On their side, the PACE adopted in 2007 the Resolution 1590 on *Secret ballot – European code of conduct on secret balloting, including guidelines for politicians, observers and voters*. The Assembly recalls that ensuring the secrecy of voting remains a key aspect of free and fair elections. More specifically, the PACE highlights that (2007a: para. 3)

> "the secrecy of voting […] protects voters against any threats likely to impinge on their choices and safeguards their freedom of thought and their political and other beliefs. The secret ballot plays an integral part in legitimising the democratic process. It ensures that citizens are able to express themselves freely, that elected representatives are truly representative and that legislative and executive bodies are legitimate, thereby contributing to public trust in institutions."

The Assembly stresses that "the secrecy of the ballot implies not only the right, but also an obligation for voters to keep their vote secret. Nobody may have access to ballots once cast to discover how anyone has voted" (PACE, 2007a: para. 5). For this reason, "the Assembly strongly condemns all […] infringements of secret voting such as buying votes, voter harassement, multiple voting [sic], the stamping of ballot papers and a shortage of polling stations and polling booths" (PACE, 2007a: para. 9). Lastly, it calls on all member states "to guarantee secret voting for all citizens, including the most vulneravle groups […] and to make sure that appropriate facilities are provided to enable such individuals to vote in secrecy" (PACE, 2007a: para. 12.1)[70].

[69] In its *Interpretative Declaration to the Code of Good Practice in Electoral Matters on the Publication of Lists of Voters Having Participated in Elections*, the Venice Commission acknowledges that "access to the lists of voters having participated in elections may be granted to certain electoral stakeholders" (2016: 2). We will examine the implications of these provisions in chapter 4 (section II.2.c)

[70] More specifically, the Assembly calls on member states to [emphasis added] (2007a: para. 12.1):

> "12.1.1. preserve voter anonymity so that votes cannot be linked to voters;
>
> 12.1.2. respect individuality of voting and enable all voters to make their choices freely;
>
> 12.1.3. ensure maximum security in electronic voting by providing for secure data transfer and preserving voter anonymity;
>
> 12.1.4. make sure that election officials do not interfere with secret voting, namely that they do not read the ballot papers before the counting process;
>
> 12.1.5. provide and expand facilities and equipment that guarantee secret voting (polling stations, polling booths, mobile ballot boxes, etc.), thereby ensuring confidentiality;
>
> 12.1.6. abolish the use of ballot papers attached to counterfoils and bearing serial numbers;
>
> 12.1.7. for proven cases of electoral fraud, annul election results in the constituencies concerned and, if such fraud is likely to have influenced election results, rerun voting;
>
> 12.1.8. put an end to all forms of family voting and punish and prosecute those involved;
>
> 12.1.9. impose severe penalties for violations of the secrecy of voting such as buying votes, voter harassment, multiple voting and stamping of ballot papers, and take robust action against any shortage of polling stations or polling booths;
>
> 12.1.10. make sure that ballot papers are transported securely so as to preserve the secrecy of the ballot;"

Even more interestingly, in the Report linked to the Resolution, and based on the Venice Commission's *Code of Good Practice in Electoral Matters*, the Assembly (2007b: para. 23-36) identifies the following minimum standards for secret suffrage:

- Individuality, meaning that each voter makes an individual choice.
- Confidentiality, meaning that only the voter should know how they have voted, and they should be able to make their choices in private.
- Anonymity, meaning that there should not be a link between the vote cast and the identity of the voter who has cast it.

When it comes to individuality, it is defined as the requirement that "[e]very person registered on the electoral roll must be able to express his/her choice in person[71], and this personal choice must be counted as such" (PACE, 2007b: para. 24). It is obvious that any form of group voting would be contrary to this standard. Among them, the Assembly stresses family voting as "one of the most blatant breaches of the secrecy of the ballot, since the head of household's choice is imposed on other members of the family. There can be no secrecy of the ballot since certain voters have no choice" (PACE, 2007b: para. 5). While family voting is not unique to voting from unsupervised environments, the likelihood of this risk (or the difficulties in mitigating it) increase for remote voting channels (Vollan, 2006).

Second, confidentiality is closely linked to the common technologies enforcing secret suffrage (at least when voting takes place in polling stations): voting booths and envelopes. The Assembly stresses "the importance of the polling booth, a private place whether the voter's choice cannot be dictated or seen by anyone else" (2007b: para. 29). However, confidentiality not only addresses the moment a vote is cast, but "must apply from the start of the casting of votes until the announcement of the results, or even longer if there is a recount" (PACE, 2007b: para. 29). Therefore, the standard of confidentiality starts during the casting of the vote, but is not limited to the casting. At the same time, it is different from the standard of individuality, although some mechanisms may contribute to achieve both. In this regards, voting booths[72] contribute to both the individituality and the confidentiality of the vote, at least as long as it is supervised that people enter them on their own. When it comes to confidentiality, additional measures may be necessary as well. For example, if the voter makes their choice alone in the voting booth, but their choice is not somehow protected, one could see the ballots and/or their marks as soon as they leave the booth. According to the standard of confidentiality, "[l]egislation should make it clear

[71] This reference to "in person" does not preclude the use of remote voting channels. For example, the example used by the Assembly to illustrate the standard of individuality is based on remote voting in Sweden. This example is introduced as follows: "[i]n Sweden, for example, remote voting procedures requires the voter and any witnesses to the secrecy of the vote to sign either the outer envelope in which a postal vote is mailed or a statement attesting that the vote was both individual and secret" (PACE, 2007b: para. 25).

[72] According to the PACE, "[i]t is nevertheless possible to classify the degrees of secrecy, according to the type of vote and the environment in which it takes place. It goes without saying that a conventional paper ballot at a polling station offering complete secrecy (closed polling booths, no interference by poll officials, in particular) occupies the top position in this classification" (2007b: para. 30). In practice, however, closed polling booths prevent the secrecy of the vote from being supervised, and therefore voters could actually take advantage of this environment to generate a proof of how they have voted (by means of pictures or videos taken with their smartphones, for example).

that every voter's ballot paper must be marked, and their vote cast, individually and secretly" (PACE, 2007b: para. 32).

Lastly, there is the minimum standard of anonymity. Based on this standard, "[t]here must be no link between the vote cast and the voter's identity" (PACE, 2007b: para. 33). According to the PACE, "[a]nonymity of the vote guarantees the freedom of the choice, an essential element of the rule of law. Where it does not exist, freedom of opinion is endangered since the voter may be influenced by threat of sanctions or reprisals" (2007b: para. 33). Based on this wording, we wonder whether anonymity should be considered as a more important value than individuality and confidentiality. At the end of the day, if it is the anonymity of the vote what guarantees the freedom of the choice (inasmuch secret suffrage guarantees free suffrage), then the other standards may just be instrumental to achieving anonymity. In practice, however, it may not be necessary for a coercer or a vote buyer to be able to trace a vote to the voter who has cast it. Given that current practices ensure that once a vote is cast into the ballot box it will be included in the final tally, it may be enough to ensure that the voter makes the expected choice and casts the vote. From that moment on, they would not have expressed their opinion freely and nothing could be done to amend their choice. Therefore, we are of the opinion that it is the combination of the three standards, and not anonymity by itself[73], that guarantee the freedom of the choice.

In addition to the three standards[74], the report also touches upon two issues that while assessed in the framework of anonymity, we argue that do not fit well within any of the three standards separately. They are broader questions that touch upon secret suffrage more in general. On the one hand, the fact that in some countries ballots must be immediately destroyed by polling station officials at the end of the counting process. This practice may ensure anonymity (since some technologies could allow to link a vote to the

[73] Another issue that will not be addressed here, since it is not a practice in any of our three case studies, is the fact that "[s]ome legislation stipulate that ballot papers can be linked to individual voters after an election where there is allegation of fraud" (PACE, 2007b: para. 35). This form of pseudonymous voting would maintain some sort of link between each vote cast and the voter who has cast it, that would only be revealed in certain circumstances. Breaches of anonymity with pseudonymous voting would depend upon the operational mechanisms put in place, but they cannot be completely ruled out. Likewise, the practice of stamping ballots (especially when they are stamped after the voter has made their choice) could violate this standard if the polling station officer who has stamped the ballot could then link the contents of the vote to the person who has cast it.

[74] Additionally, these three standards may not be enough to prevent certain violations of secret suffrage. For example, none of these three standards can prevent negative vote-buying (or abstention-buying). Where vote buying includes providing a financial or material incentive (including the promise of jobs, loans, promotions, etc.) to a voter in exchange for a vote, "[n]egative vote buying occurs when a candidate is certain that a vote will not vote for him/her and pays that voter not to vote" (PACE, 2007b: para. 47). None of the measures that we have identified would prevent the success of these methods of abstention-buying, especially if it possible to monitor whether the voter stays at home during election day. Unless there are other options than voting in person in polling stations during e-day, it seems that the only way to prevent abstention-buying would be to make voting compulsory (Johnson and Orr, 2020). A similar issue is raised under provisional voting, when voters can cast a ballot whose validity will be decided at a later stage. This form of voting can be found, for example, in certain countries when a voter is not included in the electoral roll. The voter then casts their ballot, which is kept separately together with some link to the identity of the voter. Therefore, "the theoretical possibility remains that at the opening of the envelope it could be determined who has cast the vote it contained" (Maley, 2018: 16). In this case, the anonymity and confidentiality of the ballot depends upon the role of scrutineers, who "are entitled to be present at the process of opening the envelopes, so as to ensure its transparency" (Maley, 2018: 16).

voter who has cast it). However, our definition of confidentiality would be ensured as well (at the end of the day, if votes are no longer anonymous it would not be possible either to ensure that only the voter should know how they have voted).

The second issue is related to whether secret suffrage is a duty for voters, or just a right. In the opinion of the Assembly, as it is the case for the Venice Commission, "[t]he principle of the secrecy of the ballot requires that election legislation ensures that secret voting is not only a right for voters, but also an absolue obligation" (PACE, 2007b: para. 34). It is clear that certain electoral practices, such as disqualifying any vote with a distinctive mark, are the result of such approach (if secret suffrage were an absolute right, why should those ballots be deemed invalid?). Notwithstanding, in practice secret suffrage can be considered an absolute obligation only in certain circunstances. Based on some of the examples mentioned in the Report, the Assembly is likely aware of this fact as well: when voting remotely (such as in the Swedis example) or by proxy (PACE, 2007b: para. 31-32), it is not possible for the State to enforce such an obligation[75]. Therefore, this understanding of secret suffrage as an *absolute obligation* has to be understood rather as a declaration more than an actual constraint, otherwise many of the voting channels that the PACE does not preclude should be we found not to comply with this requirement.

b) The 1990 Copenhagen documents and the OSCE/ODIHR

In Europe, the principle of secret suffrage is also enshrined in other regional human rights instruments. For example, it is enshrined in the Document of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE (nowadays Organisation for the Security and Cooperation in Europe, OSCE). The Document sets in its commitments 5.1 the value of "free elections that will be held at reasonable intervals by secret ballot or by equivalent free voting procedure", and in commitment 7.4 participating States commit to "ensure that votes are cast by secret ballot or by equivalent free voting procedure."

Based on these provisions, the OSCE/ODIHR understands that "[v]oters must have a guarantee that their voting choices will not be disclosed to other persons and that they will not be intimidated or face retribution as a result of how they chose to mark their ballots" (2013: 54). The OSCE/ODIHR also stresses that "[t]he principle of secrecy of the vote requires legal provisions to ensure that secret voting is not only a right on the parto f the voter, but also an absolute obligation" [emphasis added] (2013: 55). As a result, "[e]lection officials should under no circumstances accept deviations from the principle of secrecy of the vote" (OSCE/ODIHR, 2013: 55). Amongst them, "open voting", "family" and "group voting" are specifically mentioned.

III. THE NOT-SO UNIVERSAL SECRET BALLOT: CHALLENGES TO SECRET SUFFRAGE

At this point, it must be acknowledged that regardless of some agreement having been reached regarding the specific content of secret suffrage, this is not without controversy. In previous sections, we have already stressed how not all countries adopted the same

[75] And as we will see in section III.1.c) below, not all countries disqualify any vote with a distinctive mark.

technologies to enforce secret suffrage, and that even similar technologies were implemented in different ways in each country.

In this section we deal with a similar issue: the fact that secret suffrage is not a universal technology. Among others, visually impaired and illiterate voters cannot vote in secret precisely because of the technologies used in contemporary elections: pen and paper. Likewise, there are alternative voting methods which do not fully comply with the above-mentioned standards, such as postal or proxy voting. All in all, these alternative voting methods oblige us to revisit the very foundations of secret suffrage since they open the door to casting votes from uncontrolled environments. Furthermore, some new technologies could overcome the very guarantees that were developed to ensure the casting of votes in secret, even in polling stations.

Lastly, the section closes with some discussions about the desirability of secret suffrage. This institution was challenged in the context of its introduction. Nowadays, when the problems it aimed at preventing do not seem so widespread, some authors are challenging it again.

1. The limitations of secret suffrage

Whereas pen and paper contribute to complying with secret suffrage, not all voters have benefited from these technologies in the same way. In fact, casting paper ballots means that some voters have to be assisted when casting their vote. This conundrum remains today. Furthermore, a steady adoption of alternative voting methods meant that some of these technologies could no longer be enforced: voting booths, envelopes, etc. may not be so efficient when it comes to voting by post or by proxy. They may no longer be so efficient even in polling stations, due to the development of technologies that allow the recording of the casting of votes.

Lastly, it is also important to ascertain the perceptions about secret suffrage[76]. After all, "[i]llicit influence of voters can also take place when a voter believes that he or she may face consequences for voting a particular way and the voter does not trust that the election officials or voting technology will keep his [sic] vote confidential. In this situation, a voter is likely to succumb to another party's influence over his [sic] voting decision" (Meagher, 2009: 363). Therefore, "[t]he voters must also believe that the election administration operates in a way that their choices are kept secret (psychological secret ballot)" (Koitmäe, Willemson, Vinkel, 2021: 143)[77].

In this section we briefly address some of these issues to highlight the political and context-dependent nature of secret suffrage and how it has been displaced in certain alternative voting methods. The goal is to highlight that even if a key principle of democratic elections, the way we think of secret suffrage has been developed with a

[76] In a study conducted in the US by Alan Gerber et al., it was found "that 82.6 per cent of the population believes either that their choices are not kept secret (25.5 per cent) or that they will reveal their choices 'almost all the time' or 'most of the time' (72.6 per cent)" (2013: 541). Along these lines, it has been argued that "it is the voter's *perception* of the secrecy of the ballot, rather than the actual secrecy, that affects their behaviour" (Saglie and Segaard, 2016: 158).

[77] For these authors, "[i]-voting adds another dimension here, since the voters must additionally believe that tother voters respect privacy and secrecy of the vote. Additionally, voters might feel socially obligated to reveal their votes, or they can believe that other voters might do so (social secrecy of the ballot)" (Koitmäe, Willemson, Vinkel, 2021: 143)

specific voting channel in mind: paper-based voting in polling stations, by the layperson. Therefore, challenges to secret suffrage are not unique to remote electronic voting. Lawmakers and election administrations already have had to revisit this principle of democratic elections to ensure the universal nature of secret suffrage and when considering the adoption of alternative voting channels. As we will show, new technological developments force us to revisit this principle again.

a) Assisted voting: equal and secret suffrage

Whereas paper ballots were introduced with a view to enforce secret suffrage, the very technologies used to preserve secrecy prevent certain voters from voting independently and by themselves. This is the case for voters with disabilities, especially blind and visually impaired voters, as well as illiterate voters[78]: they cannot use paper ballots by themselves and require the assistance of someone else to cast their vote. If they are assisted in voting, their choices are no longer confidential.

Therefore, the principle that "no member of a polling station Committee or any other person should be allowed to see a voter's marked ballot paper […] does not apply to a person legally authorised to assig a blind voter or a voter requiring assistance due to a physical incapacity or illiteracy" (PACE, 2007b: para 30). As the PACE acknowledges, "in nearly all countries electoral practice results in a blind citizen being dependent on someone else to cast his/her ballot […] which could jeopardise the secrecy of the vote" (2007b: para. 61).

In fact, assisted voting could breach both the principles of secret and free suffrage. The Assembly recognises that "[n]ot only do these people lose their right to a secret ballot, but they can never be sure that the person voting for them is actually putting down their voting choice" (2007b: para. 62). The same happens when these voters are allowed to appoint a proxy to vote on their behalf, since proxy voting neither addresses these concerns[79].

[78] As we have seen in footnote 50 above, Daniel Gingerich "demonstrates that the adoption of the Australian Ballot in Brazil in 1955 (for presidential and vice-presidential elections and subsequently for other offices) increased the number of null and invalid votes, presumably because illiterates were effectively disenfranchised" (2013). According to Cristopher Kam, in the United Kingdom assisted voting was used to maintain coercion and vote-buying following the adoption of the secret ballot (2016: 601),

> "[t]he […] more tangible threat to the secrecy of the vote were provisions that permitted incapacitated (e.g, blind) or illiterate voters to have the presiding officer mark their ballots in the presence of the candidates or their agents. Several of the witnesses who testifies at parliamentary hearings on the secret ballot's performance at the 1874 election stated that party agents responded to this clause by instructing supporters to claim illiteracy so that they might receive assistance in casting their votes".

[79] Proxy voting "enables people who are unable to vote themselves to designate someone else to do so on their behalf. This practice nonetheless poses a problem of secrecy. In principle, only the voter should know how he/she has voted, but that is not the case with proxy voting" (PACE, 2007b: para. 7). Jorgen Elklit defines proxy voting as those "situations, where voters, who can't make it to the polling station, are entitled to let another person (normally a registered voter) vote on his or her behalf" (2018: 8). Therefore, "[i]t was with such voters in mind [blind voters, voters requiring assistance due to a physical incapacity or illiteracy, etc.] that the practice of proxy voting was introduced in many […] states" (PACE, 2007b: para. 31). "Despite its practical advantages, proxy voting violates the secrecy of the ballot and is founded solely on the trust vested in the

According to the Assembly, however, there are other alternatives that would not breach the secrecy of the vote. Such measures include "designing ballot papers sensitive to voters' needs (including for example dual-language ballot papers, using party symbols and/or photographs)" (PACE, 2007b: para. 32). Similarly, ballot papers in Braille could be made available, but "the voting material should be in Braille and not only the ballot paper itself to preserve the secrecy during the ballot counting" (PACE, 2007b: para. 63). Otherwise, and since the number of ballots in Braille cast in each polling station would likely be too low, the anonymity of those ballots could not be preserved[80].

b) Convenience voting: universal against secret suffrage

Another instance where secret suffrage is balanced against universal suffrage is when voters are offered alternative voting methods, including remote voting channels in which they can cast their vote from supervised environments. This is clearly the case of postal voting, but alternative voting channels such as proxy or mobile ballot boxes also challenge this traditional approach to secret suffrage. According to Peter Brent, "[i]t is impossible to enforce secrecy for these forms of convenience voting, and yet their further increased use is all but inevitable" (Brent, 2018: 2). Arne Koitmäe, Jan Willmeson and Priit Vinkel have summarised this issue as follows (2021: 140):

> "the way we understand vote secrecy is closely related to the concept of traditional voting – the ballot box is filles in privately in the voting booth, and then deposited in the ballot box. However, many voting methods also deviate from this scheme. One example is postal voting, where there is no control whether the ballot is filled in privately, and no solid guarantees can be given that the ballot sent though mail is not lost, opened, or tampered with"

In recent years, a steady adoption of alternative voting channels has been observed in addition to proxy voting, such as mobile ballot boxes and postal voting. For example, Régis Dandoy and Rudi Kernalegenn notice that "[m]ost democracies have enfranchised their diaspora through allowing various forms of extraterritorial voting" (2021: 2). This trend has been consolidated with the outbreak of the Covid-19 pandemic and the generalisation of alternative voting methods for health reasons[81]. As a result, the OSCE/ODIHR published

person voting on behalf of the registered voter. There is nothing to prevent that person from "hijacking" the vote" (PACE, 2007b: para. 32).

Such concerns are echoed at the national level as well. For example, the French Senate report by François-Noël Buffet stresses the disadvantages of proxy voting: the voter must inform their proxy about their choice, which is a breach of the secrecy of the vote, and they have no means of verifying that their choice has been respected by the proxy (2020: 16). The report also highlights the fact that it is not possible to disregard external pressures (from the family or the community). More interestingly, it points out that such pressions do not disappear with paper-based voting in polling stations, but that they are just present to a lesser extent than in proxy or remote voting (Buffet, 2020: 16).

[80] A better alternative could be the combined used or remote electronic voting with assistive technologies, that we will address in chapter 5.

[81] Initially, these alternatives may had been envisaged as exceptions for certain voter groups who could not make it to the polling station, such as voters with reduced mobility or voters abroad (such as in France, where postal voting was maintained only for French voters living abroad). Alternatively, countries may have introduced them due to the high number of contents they held (such is the case in Switzerland). Regardless of the original aim, the Covid-19 pandemic has fuelled

a report on the benefits, risks, and practical considerations for alternative voting arrangements (2020).

There are several alternative voting methods. On the one hand, mobile ballot boxes are arrangements for voters whose mobility is impaired and who cannot travel to the polling station. For them to vote in secret, "members of the competent committee can, upon request, visit voters in their place of residence with a mobile ballot box"" (PACE, 2007b: para. 65) According to the OSCE/ODIHR, "[t]he secrecy of the vote is a primary concern for election officials using any home and institution-based voting method. Where possible, voting stands and ballot secrecy sleeves are used to administer either postal voting at the place of stay or voting via a mobile ballot box" (2020: 34). Notwithstanding, such arrangements may create other risks (to the secrecy as well as to the integrity of the elections) and involve cumbersome administrative formalities.

For these reasons, possibly the more extended alternative is postal voting. Postal voting "benefits people who are unable to attend at a polling station in person, either for physical reasons or because they are absent" (PACE, 2007b: para. 58). However, "[a]n election where ballot papers are distributed and/or returned by post […] raises a number of questions regarding compliance with the requirements of a secret ballot" (PACE, 2007b: para. 59). In this sense, in an unsupervised environment such as the voter's home it is not possible to guarantee that votes have been cast individually. In these cases, a voter may be forced to mark certain choices against their will, and then the coercer or vote-buyer could cast their vote on their behalf (especially if votes can be cast in mailboxes and do not need to be hand in person by the voters themselves). Interestingly, in this scenario anonymity would be preserved (once cast, nobody could link the vote back to the voter, not even the coercer or vote-buyer) but still their choices would not be secret.

c) Technological developments and secret suffrage

When it comes to digital technologies, the main concern is usually how to ensure secret suffrage when voters cast their votes electronically, be it from polling stations or from uncontrolled environments (something that we have already introduced in the previous chapter). In fact, the relationship between digital technology and secret suffrage is far more complex and digital technologies also pose new threats to secret suffrage when votes are cast in paper from polling station[82]. According to Hubertus Buchstein, "[k]eeping the vote secret is a permanent challenge for electoral authorities. New technologies lead to new possibilities to violate the secrecy of the vote" (2015: 16). In this regard, this author mentions some examples (Buchstein, 2015: 16):

this trend even further, to the extent of generalising these alternatives. In some cases, elections amidst the pandemic relied on these alternatives as the only voting channel available (Wagner, 2020).

[82] At the same time, the current guarantees for vote secrecy are quite weak. For example, the use of envelopes to preserve confidentiality is by itself rather limited, especially in remote postal voting. Regarding the protection offered by envelopes, Martin Keith notes that (2020: 13)

> "[a]n envelope offers a degree of physical protection to the contents from threats such as rough handling during the delivery journey. An envelope protects the contents from being seen by anyone other than the intended recipients. This protection is relatively weak, since envelopes are flimsy and easily opened. However, perhaps the most significant security provided by an envelope is that anyone opening it during its journey normally needs to break a seal. Unless this is done with great care, the recipient will notice the intrusion."

> "[d]uring the Roosevelt era in the United States, some voters feared that the government would take fingerprints from the ballot papers. In the 1960s, there were rumours in some countries that cameras installed in voting booths would illegally take pictures of the voting procedure. And in our days, voting authorities have to deal with the (much more real) challenge that it is easy for any voter to document his or her activity in the voting booth digitally on a cell phone."

The case of ballot selfies is quite a good example. The practice of sharing pictures of ballot papers online, more often known as ballot selfies, has been at the centre of legal debates for the last decade. The ability of the modern smart phone to capture an instant image without any need for back-end processing makes it especially well-suited to vote-buying (Maley, 2018: 16). A voter can take a picture of their vote as a proof, and as a guarantee for the vote-buyer, of how they have voted. According to Arne Koitmäe, Jan Willemson and Priit Vinkel (2021: 146)

> "[v]oters can take a photo of their ballots in the polling booth, or […] live broadcast their voting from the polling booth. This provides some (although quite a weak form of) proof that the vote has been cast correctly. This also lets the voter publishing the image of the ballot taking, thus conflicting the vote secrecy principle."

While those taking ballot selfies consider this exercise as a legitimate form of freedom of expression, it has been found to go against existing legal standards in several countries. At the same time, in several countries it has been found that ballot selfies go against existing legal standards. For instance, in Brazil, Canada, and Germany they are considered illegal. Ballots may be rendered invalid, and voters may be even fined if they are found to have had a picture taken of their marked ballot.

In the United States, a judge held in 2015 that a law in Massachusetts prohibiting voters from "taking a digital image or photograph of [one's] marked ballot and distributing or sharing the image via social media or by any other means" conflicted with the right to freedom of speech and freedom of expression enshrined in the First Amendment to the U.S. Constitution (Horowitz, 2016: 247). In Europe, a Dutch judge ruled in May 2014 that "although the disadvantages of 'stemfies' [i.e., ballot selfies] were in his eyes bigger than the advantages, the [Dutch] Election law does not prohibit their making" (Loeber, 2014: 45). In Europe, the European Court of Human Rights has ruled that a prohibition on sharing ballot selfies during a referendum held in Hungary in 2016 was contrary to the right to freedom of expression enshrined in Article 10 of the European Convention on Human Rights[83].

In this regard, Arne Koitmäe, Jan Willemson and Priit Vinkel stress that "[i]n the case of *stemfies* (ballot selfies), it is also apparent that the legislation and our general understanding of the secrecy have not kept up with the technological advancements" (2021: 146).

[83] However, in *Magyar Kétfarkú Kutya Párt v. Hungary* [2019] the Court only assessed whether a restriction on the use of a mobile application where voters could upload and share anonymous pictures of their invalid ballot papers (i.e., a restriction of the right to freedom of expression as enshrined in Article 10 freedom of expression and information of the European Convention on Human Rights) would be justified under the exception of the second paragraph of the same Article. However, the Court did not consider how to balance the two rights at stake under the phenomenon of ballot selfies. We have written a detailed (and critical) account of this case in Rodríguez-Pérez (2021).

All in all, these limitations and voting alternatives bring us back to the issue of whether secret suffrage should be understood as an obligation that voters must respect or a right that voters have. According to Ülle Madise, still nowadays "[t]here is a debate about whether observing the privacy aspect of the secret ballot principle constitutes a right or an obligation of the voter and, ideologically and legally speaking, this debate is central to the authorization of Internet-based voting" (2007: 17). We have seen that most international standards point towards secret suffrage as being an obligation that voters have, not just their right. Therefore, when voters overcome the guarantees of secret suffrage (e.g., by making a special mark on their ballot[84]), their vote should be disqualified.

For Hubertus Buchstein, "[t]he institutionalization of secret voting includes that the secrecy of the vote has to have a compulsory or *mandatory status*. It should not be up to the individual voters themselves to keep their votes secret. In such case, secrecy would not be fully guaranteed. Thus electoral authorities have to take care to create and safeguard secrecy" (2015: 16). According to this author[85], "secrecy is considered a mandatory lawful duty for every voter. You are free to tell anybody whom you voted for, but you are not free to prove this assertion. Only you will know whether what you said was true" (Buchstein, 2015: 42).

Jon Elster also provides a rationale for why secret suffrage should be mandatory. According to him, "a voter who opts publicly for secrecy (for herself) in a non-strict regime may by that act reveal her voting intention. A voter who proposes the secret ballot (for everybody) can run the same risk" (Elster, 2015: 8). Likewise, Adam Przeworski also agrees with Buchstein when he states that "voting is effectively secret only if secrecy is obligatory" (2015: 101). To sustain his claim, Przeworski provides the example of communist Poland, where (2015: 101)

> "one picked a ballot from a table on one side of a room and had to walk across it to deposit the ballot, with an option of entering a private booth in which one could modify the unique list that contained more candidates than places but in order preferred by the authorities. The booth was private, but one's trajectory across the room was nonchalantly observed by two uninformed gentlemen."

However, this approach has been contested. For Ülle Madise, "[m]andatory secrecy is a principle which goes beyond constitutional law, its fundaments are based on the idea of auto-paternalism and it is understood as a mechanism of self-binding of autonomous citizens in order to avoid situations of external pressure or corruption" (2007: 17). While this conundrum cannot be resolved here, it is obvious that there is a general trend towards interpreting secret suffrage rather as a right than an obligation. The alternative voting

[84] According to Arne Koitmäe, Jan Willemson and Priit Vinkel, "[v]oters can […] mark their paper ballots in a way that it would be recognizable during the vote counting. If the voter (or some other informed party) then observes the count, they can make notice whether and how their vote was counted" (2021: 146)

[85] To support his argument, Buschstein resorts to a classical justification of why secret suffrage should have a mandatory status as formulated by Thomas Schelling (1980: 91):

> "[t]he mandatory secret ballot is a scheme to deny the voter any means of providing which way he [sic] voted. Being stripped of this power to prove how he [sic] voted, he [sic] is stripped of his power to be intimidated"

methods discussed above are a good example of it and remote electronic voting will also have to be approached taking this issue into account[86].

In fact, Arne Koitmäe, Jan Willemson and Priit Vinkel already stress that the secret suffrage as an obligation is not even absolute when it comes to voting in polling stations. According to them, in Estonia the law does not prescribes that vote carrying a mark should be declared invalid. On the contrary, "if the ballot is not filles correctly (e.g. the number of the candidate is not written on the correct spot), but the choice of the voter is otherwise understood (e.g. the name of the candidate was written on the ballot), the ballot is considered valid" (Koitmäe, Willemson and Priit, 2021: 146).

2. Against secret suffrage. Old and new proposals for open voting

It is not just the compulsory nature that secret suffrage that can be debated. In fact, the very principle of secret suffrage has been put into question. Despite the PACE's claim that "the secrecy ballot is taken for granted as a basic principle. There is no longer any question of challenging it today" (2007a: 1), there are indeed some authors who challenge the principle of secret suffrage. In this regard, they have argued that an electoral system under which voting is secret does not encourage the sort of performance at the polls that we should be seeking (Brennan and Pettit, 1990: 311). For Jan Teorell, Daniel Ziblatt, and Fabrice Lehoucq, "[t]he nature of the ballot in fact has historically held, and even today holds, an ambiguous relationship to the idea of representative government itself" (Teorell, Ziblatt and Lehoucq, 2017: 532).

By the time of its adoption, the secret ballot received fierce opposition in Australia[87], in France[88], in Germany[89], and in the United Kingdom[90]. Nineteenth-century liberals such as

[86] In the opinion of Hubertus Buchstein, in remote electronic voting "[i]t is up to individual citizens again whether they want to share the act of casting the vote with others or not" (2015: 16). Therefore, he claims that "online voting has become the source of a new attack on mandatory secret voting, which has slowly been coming through the back door as a consequence of attempts at further technical modernization of our current mode of voting" (Buchstein, 2015: 41).

[87] In Australia (Brent, 2018: 6),

> "the move away from nomination on the hustings was identified at both the 1861 and 1865 House of Assembly Select Committees as a serious problem major reason for the lower turnout. A committee in 1865 recommended returning 'a return to the old form of nomination, which compelled the candidate to appear on the hustings' on the grounds that 'it would tend to destroy the apathy which now generally prevails during the elections'. Parliament did not agree; written nominations prevailed and remain to this day. And so, perhaps, does lack of interest in elections."

[88] The French sociologist Emile Durkheim also "expressed reservations about the system of secret balloting in France at the beginning of the twentieth century" (Buchstein, 2015: 25). "In his critique Durkheim points to the secret ballot in particular. He accuses it of not providing citizens with an incentive to engage in political thinking" (Buchstein, 2015: 26).

[89] According to Hubertus Buchstein, the Prussian constitutional law expert Rudolf von Gneist "was opposed to the secret ballot because it would downright educate citizens to act irresponsibly and provoke spontaneous moods swings in the political real" (Buschstein, 2015: 21). According to the constitutional law expert (in Buschstein 2015: 21),

> "[t]his explains the sudden changeover of party elections using secret balloting, as nobody needs to fear a feeling of moral responsibility or disapproval among his bourgeois neighbours if he pleases to cast his vote one way this time and another way the next, moved by the mood of the moment or changes in these interests. According to this idea, it is only the elected who is to be responsible."

[90] Bruze Kinzer's (1978) argues that the secret ballot was already "contested upon its introduction in nineteen century England because it was thought to be at odds with and detrimental to the

John Stuart Mill strongly opposed it (Buchstein, 2015). "In any political election," wrote Mill (in Teorell, Ziblatt and Lehoucq, 2016: 532):

> "even by universal suffrage…, the voter is under an absolute obligation to consider the interest of the public, not his private advantage, and give his vote, to the best of his judgement, exactly as he would be bound to do if he were the sole voter, and the election depended upon him alone. This being admitted, it is at least a prima facie consequence that the duty of voting, like any other public duty, should be performed under the eye and criticism of the public."

John Stuart Mill's most well-known critique against secret voting is that publicity promotes responsible voting, that public voting forces citizens, at least implicitly, to defend their vote choices before their peers. Bart Engelen and Thomas R.V. Nys have summarised the stance of the liberal politician as follows (2013: 494):

> "[i]n his tenth chapter of his Considerations on Representative Government, Mill expresses his concern that (the introduction of) the secret ballot would motivate citizens to vote without any reason whatsoever and without any reference to others. In contrast, open voting enables people to hold each other accountable, thereby impelling them to provide reasons for their choices, which is more in line with what can be expected of members of a real democracy."

Some contemporary authors echo Mill's critique of the secret ballot. They argue that it 'privatises politics', that it reduces the transformative potential of political democracy (Brennan & Pettit, 1990; Engelenen and Nys, 2013). These authors have identified a number of disadvantages of secret suffrage, compared with public voting. According to Hubertus Buchstein (2015: 17),

> "[t]heir criticism can be summarized in the suspicion that the secret ballot is an achievement of modern democracy with ambivalent consequences: Although they credit the secret ballot with securing the political autonomy of every individual citizen, they also blame it for being a source of fostering the privatization of politics and supporting egocentric motives in political decision making."

For instance, Tidd Davies highlights how the secret ballot: (1) undermines accountability of voters for their choices; (2) discards information that might assist voters with their decisions; (3) reinforces a norm of non-participation and apathy regarding political activity; (4) discourages voting by reducing the consequences of participation; (5) encourages a view of voting as an individual choice rather than as a social act; and (6), of special interest to theorists, reduces the possibility of cooperation across issues, e.g. vote trading that may improve overall welfare (2004). In contrast, "under open voting citizens are publicly answerable for their electoral choices and will be encouraged thereby to vote in a discursively defensive manner. Secret voting fails this test because citizens are protected from public scrutiny" (Brennan and Pettit, 1990: 311)

Geoffrey Brennan and Philip Pettit "argue that open voting induces voters to vote in a 'a discursively defensible manner'" (Manin, 2015: 210). As they put it (Brennan and Pettit, 1990: 324),

virtuous and honourable character of the English". As quoted by Engelen and Nys, a "system of secret voting might suit a nation whose people were hypocritical, cunning, furtibe, and deceitful […], but it had no place in a country like England, whose people - noted for their independence, manliness, honesty, and frankness – always preferred to conduct their affairs I the open and in the light of the day" (2013: 496)

> "[s]uppose that someone votes for A over B, or at least intends to do so, and that he wants to defend his vote discursively. It will not do for him to say, for example, simply that A suits his interest best. He puts himself beyond the pale of conversation, if he is unresponsive to the retort that it may suit his particular interests, but it is damaging for the country as a whole. He must be ready to argue that A is not damaging in this way or that if it is, the damage done is offset by some greater public benefit"

Similarly, Bart Engelen and Thomas R.V. Nys argue that (2013: 493)

> "[i]If you can be asked why you voted such-and-such, you will be more likely to refer to reasons that are as relevant to others as they are to yourself. The claim that a candidate serves your private interests will not be accepted as a legitimate argument in public and reasonable discussion. If the vote is unveiled and citizens can be challenged on their voting behaviour, they will think twice before voting on the basis of self-interested and antisocial considerations like 'prejudice, xenophobia, malice or caprice'."

Notwithstanding, this criticism does not yet address the negative impact that open voting has on elections and that we have discussed before (i.e., bribery, blackmail, and intimidation)[91]. More recently, Bernard Manin (2015) has come with an argument against public voting in general elections. This author argues that open voting would have three undesirable implications, namely: "(1) subjecting people's votes to the control of their social environment, (2) increasing the importance of private rewards and punishments in elections, [and] (3) increasing the influence of the rich and powerful strata of the citizenry" (Manin, 2015: 209).

Furthermore, open voting in general elections would not mean that the voter is subject to the judgement of the entire electorate (as proponents of public voting would argue). As he argues, "open voting does not place each voter under the control of the general public, but under the control of his [sic] social environment" (Manin, 2015: 211). In addition, those controlling how others vote may "intend to use their findings instrumentally to further their own private goals. In other words, checking the way other people vote is likely to be driven by private concerns, not by a concern for the common good" (Manin, 2015: 212). According to Bernard Manin (2015: 213),

> "open voting enables candidates to strike bargains with individual voters, offering a personal reward if the voter votes in the desired way and threatening sanctions if she does not. Since open voting makes compliance easily verifiable, such bargains would stick. One might object that this would amount to vote buying and that vote buying can be legally prohibited. This may be true in theory, but in practice such prohibitions would be hard to enforce. Short of a very intrusive government, not all interactions between candidates and voters may be monitored".

Therefore, it is easy to acknowledge, as Adrian Vemeule does, that both secret suffrage and public voting have "the familiar vices of its familiar virtues" (2015: 223). As he puts it (Vermeule, 2015: 223),

[91] In this regard, Geoffrey Brennan and Philip Pettit acknowledge that "[t]he question which faces us now, the practical issue, is whether in trying to get rid of the risk of whimsical or malicious voting by opening the vote to some measure of public scrutiny, we would not create other, worse, evils" (1990: 328). In their opinion, the possibility of bribery, intimidation or blackmail moderated any argument in favour of open voting. However, they claim that such dangers could be avoidable in many contemporary societies without recourse to secrecy (Brennan and Pettit, 1990: 311)

> "[o]pen voting can induce posturing, political correctness, or, what is equally bad, bending over backward to signal that the voter is not politically correct; it also makes possible credible commitments to corrupt bargains with other voter or third parties. Secret voting can free voters to pursue self-interest and may actually increase corrupt bargains by diminishing public monitoring."

In this regard, John Ferejohn (2015: 235-236) has provided a very illustrative analysis of the benefits and shortcomings of secret suffrage for liberals and republicans:

> "[r]epublicans may be less sympathetic to the secret ballot: They might argue that if votes are cast in public, people might be dissuaded from basing their votes on private considerations. Indeed, Cicero criticized the secret ballot on the grounds that it reduced the opportunity for ordinary people to follow the lead of the best men in the republic. […] Liberals insist on the secret ballot in order that, for example, members of unpopular minorities are not forces to object publicly to popular candidates who they fear would oppress them. A liberal insist is appropriate to object to a public project, however popular, for private reasons. […] Every modern democracy required that votes in elections be cast in secret. Republicans worry that if votes are public, ordinary people may be bribed or threatened from basing their votes on shared public interests. Liberals maybe more concerned that money and power can induce or intimidate people from revealing their private or partial interests, permitting governments to trespass on unrevealed minority interests and preventing desirable compromises from being struck".

To sum up, there is no doubt that "whether [secret suffrage] protects individual autonomy or discourages public deliberation remains a subject of contention among normative theorists of democracy" (Teorell, Ziblatt and Lehoucq, 2016: 533).

3. Remote electronic voting in practice: national experiences and international standards

In the previous chapter we have already introduced some of the challenges of (remote) electronic voting from unsupervised environments. We have depicted the regulation and the guarantees of secret suffrage as a result of historic processes and different attempts to guarantee voter's rights. As a result, the contemporary framework for the conduct of democratic elections is based on the casting of paper ballots in polling stations. The introduction of alternative voting channels (spanning from postal to proxy voting, or mobile ballot boxes) has therefore not always complied with these provisions and has sometimes been justified as a derogation of national and international electoral principles.

The case of remote electronic voting is even more intricate. Remote electronic voting also introduces complexities when it comes to complying with these standards as well as on how this compliance can be ascertained. However, and in contrast to other voting channels, the intricacies are twofold: in some cases, issues arrive because in remote electronic voting votes are cast from unsupervised environments; whereas in other is the electronic dimension of Internet voting that raises suspicion and concerns. As a result, some of the questions posed by remote electronic voting are unique to this channel, including when it comes to secret suffrage.

In order to (try to) answer these questions, this chapter provides a first approach towards remote electronic voting in practice, looking both at national experiences and to the development and institutionalisation of transnational standards. Therefore, this chapter aims at providing an understanding of how remote electronic voting has shaped the regulation of elections in different countries, as well as at the international level. More specifically, we will study the experiences in Switzerland, France, and Estonia. These countries have led the introduction of remote electronic voting in Europe from the early 2000[92] until today, even if in some cases the use of remote electronic has been halted. Analysing them will allow us to take stock of almost twenty years of experiences regulating electoral principles in the face of digital technology. Following, we will also analyse how international and European electoral standards have evolved to cope with these new developments, with specific focus on both legal and technological standards.

I. REMOTE ELECTRONIC VOTING: NATIONAL EXPERIENCES

Switzerland, Estonia, and France are not the only countries nor the first ones that introduced remote electronic voting in politically binding elections. "Remote electronic voting has been utilized on some level in more than twenty countries, and several countries analyse possible implementation" (Vinkel and Krimmer, 2016: 186). In Europe, the United

[92] Switzerland conducted the first trials in 2003, at the municipal level, and 2004 in national votes. Estonia is the only country where remote electronic voting is offered to all eligible voters. Lastly, France introduced it also in 2003 in the context of a pilot, and generalised its use in 2006. In this regard, it is even more of a pioneer country than acknowledge by Régis Dandoy and Tudi Kernalegenn. According to these authors, "France is among the world's pioneers of using Internet voting, given French citizens living abroad have been able to vote online since 2006 for select elections" (Dandoy and Kernalegenn, 2021: 1). Nevertheless, remote electronic voting was piloted already in 2003.

Kingdom already organised pilots with Internet voting in 2002, 2003 and 2007[93]. In the Netherlands, voters abroad were also able to vote online for the 2004 elections to the European Parliament and during the legislative elections of 2006[94]. Elsewhere, municipalities in Ontario also started offering remote electronic voting as soon as 2003. On their side, Norway introduced internet voting in some municipalities during the municipal elections of 2011 and the parliamentary elections of 2013[95].

Here we offer a comprehensive analysis of the three case studies, and we also analyse how international and regional standards have been adopted in parallel to the national implementations. This analysis is important since, according to Vinkel and Krimmer, "no single characteristic makes up a working system […] Each Internet voting system has been developed in line with the needs of the actual context it was implemented. Therefore, this does not allow for generalizing based on individual features; it is the complete solution that needs to be looked at" (2016: 188). Thus, understanding the broader political and legal context, as well as the overall functioning of their Internet voting systems, is a necessary first step for the analysis of secret suffrage and remote electronic voting in Switzerland, France, and Estonia.

1. Switzerland

Switzerland has always been considered a country that pioneered[96] the use of remote electronic voting[97], its introduction dating back to the early 2000. Already in 1998, the

[93] The UK experimented with electronic voting during several contests at the local level. The last tests took place during the local elections in May 2007. The Electoral Commissions and several advocacy groups contrary to electronic voting voiced their criticism against this voting channel. It is important to recall that the Electoral Commission was not responsible for the organisation of this pilots, since the administration of the elections is the responsibility of local governments.

[94] According to Carlos Vegas and Jordi Barrat (2016: 60),

> "in 2004, the government decided to launch an internet voting program. The Rijnland Internet Election System (RIES) was used first for the internal elections of some water management boards, but in 2006 it was admitted as a voting means for overseas electors. Moreover, it is worth mentioning that the internet voting system included cutting-edge innovations that aimed at providing full verifiability through questioning the secrecy of the vote."

A more detailed account of European experiences with (remote) electronic voting can be found in Gregor Stein and Robert Wenda (2014) for the period between 2004 and 2014, and at the international level in Jordi Barrat i Esteve, Ben Goldsmith, and John Turner (2012) for the period between 2000 and 2011. In addition to the cases already mentioned above, some relevant experiences in Europe include: a test carried out in Catalonia in 2003, a pilot in Finland in 2008, tests in Bulgaria in 2009, and i-voting by Armenians in diplomatic missions since 2012 (Stein and Wenda, 2014: 107-108).

[95] The evaluation of the pilot was overall positive and echoed a high level of trust on the system. 72,4% of advanced votes were cast electronically (Swiss Federal Council, 2013a: 48). A second pilot was held during the 2013 parliamentary elections, "the Norwegian government decided to discontinue Internet Voting pilots […] with the underlying reasons being the change in political leadership and the lack of trust the politicians held for the system" (Vinkel and Krimmer, 2016: 187). For this reason, and even if this case is the first experience with end-to-end verifiability in public governmental elections, we have decided to focus on those three cases in which remote electronic voting has remained available for longer period of times.

[96] As a matter of fact, research conducted by Nadja Braun (2005) has shown that Switzerland "liberalised" [sic] the vote earlier and to a greater extent than any other country.

[97] Switzerland refers to its internet voting project generally as electronic voting (in French, *vote électronique*) or e-voting. In Switzerland, this notion encompasses other measures other than

Swiss Federal Council's strategy for an information society provided that it would study the potential contribution of new information and communication technologies to the expression of Swiss' voters will (Swiss Federal Council[98], 2002: 617). In June 2000, the Swiss National Council mandated the Federal Council to study the advantages and disadvantages of electronic democracy and shortly after the Federal Government authorised three cantons to pilot the use of internet voting, launching a pilot phase that has last to date.

In an extended pilot stage, more than half of the cantons allowed either Swiss voters abroad and/or resident voters to vote online. Since then, more than 300 successful binding pilots have been conducted with Internet voting in up to 15 cantons (Swiss Federal Chancellery, 2020c: 3). However, following a series of events that took place in mid-2019 and that will be described with more detail in this section, currently no electronic voting options are available in Switzerland (Swiss Federal Chancellery, 2020c: 3). Notwithstanding, the authorities are already planning how to redesign and relaunch a new pilot phase with remote electronic voting in the country (Swiss Federal Chancellery, 2020c).

Switzerland is a parliamentary democracy with a long-standing tradition of direct democracy (OSCE/ODIHR, 2007c: 1). Legislative power rests on the bicameral Swiss Federal Assembly: the Swiss National Council (with 200 members representing the Swiss people) and the Swiss Council of States (with 46 members that represent the cantons). Executive powers are vested with the Swiss Federal Council. Its seven members are elected by a four-year term and the Presidency rotates annually among them[99] (OSCE/OIDHR, 2007c: 3). The Swiss Federal Council is supported in its work by the Federal Chancellery and the different Federal Departments.

A distinct feature of Swiss political life is also the prevalence of various forms of direct democracy at all levels of government, which gives voters choices on a range of issues throughout the year (OSCE/ODIHR, 2008: 1). The country has a long-standing tradition of direct democracy which has been institutionalised since 1848 (OSCE/ODIHR, 2007c: 2).

voting (for instance, the possibility to collect e-signatures for initiatives and referendums or the electronic submission of candidates' lists) none of which has been adopted so far. Notwithstanding, at the casting stage its understanding is limited to the use of remote electronic voting (remote e-voting) or remote voting by electronic means, such as Internet voting or voting by SMS (Swiss Federal Council, 2006: 5212). The Swiss Federal Council establishes draw a comparison between electronic voting and postal voting as follows: voting by post and electronic voting have in common that they are cast remotely. Voters are not required to go to a polling station to vote. They can fill out their ballot at home, for example at their desk or on their computer, and send it by post or electronically, respectively. The advantages of these voting channels are obvious: voters can vote at any time and from anywhere (2006: 5248). Electronic voting in Switzerland is thus remote, and votes are cast from non-controlled environments. Therefore, alternative non-remote e-voting methods (such as e-voting machines) are *a priori* excluded. Therefore, for the sake of consistency and accuracy, the terms "remote electronic voting", "Internet voting" and "online voting" will be used here when referring to the Swiss experience (instead of e-voting or *vote électronique*). As a matter of fact, in its 2013 report the Swiss Federal Council acknowledged that electronic voting and Internet voting could be used as synonyms (Swiss Federal Council, 2013: 24).

[98] Unless otherwise stated, the references from the reports by the Swiss National Council, the Swiss Federal Council, and the Swiss Federal Chancellery are based on their original version in French.

[99] The Swiss Federal Council is a collegial body which traditionally acts by consensus, rather than through majority voting. Each Federal Councillor shares the duties of Head of State (OSCE/ODIHR, 2011c: 3).

Swiss voters are often called upon to take part in national or cantonal votes[100] on specific issues between four and five times per year (Braun, 2004), sometimes even more[101] (Swiss Federal Chancellery, 2004: 34). The fact that Swiss voters vote so often may be the main reason why the country adopted, already in 1994, postal voting at the federal level (Swiss Federal Council, 2002: 616). It may also explain why it has become the main voting channel, with postal votes representing around 90% of all votes cast in elections and votes (OSCE/ODIHR, 2015c: 5). These rates can be even higher in more urbanised cantons, such as Geneva and Basel-Stadt, where postal voting can represent up to 95% of all votes cast (Swiss Federal Chancellery, 2004: 34).

Switzerland is also a federal state with three political levels: the federal level, the 26 cantons, and 2,200 communes (OSCE/ODIHR, 2019c: 3). The cantons enjoy wide-ranging autonomy and independence from the federal government, and have their own constitutions, laws, parliaments, and courts (OSCE/ODIHR, 2007c: 3). The communes either elect their own parliaments or may also use direct democracy in the form of local assemblies and town meetings to take decisions (OSCE/ODIHR, 2008: 3). The organisation of remote electronic in Switzerland responds to the federal organisation of the country (Driza Maurer, 2016a: 263). In this sense, the adoption and the exploitation of remote electronic voting systems is done by the cantons, who are responsible for the organisation and the conduct of the ballots, including at the federal level. Cantons are completely free to decide whether they want to offer internet voting or not (Mendez and Serdült, 2014). On their side, the Confederation defines the requirements for internet voting for federal ballots[102], verifies compliance with these requirements within the framework of an authorisation process and coordinates the cantonal projects[103] (Swiss Federal Council,

[100] Referenda and other direct-democracy procedures are referred to in Switzerland as "votes". See for example Title 2 of the Federal Act on Political Rights, indirectly defined as "proposals submitted to the vote of the People" (art. 10.1bis). Votes are further distinguished Referendums (regulated in Title 4 of the Federal Act on Political Rights) and Popular Initiatives (regulated in Title 5 of the Act) (see also footnote 101 below). Will not draw such distinctions here, merely referring to all direct-democracy procedures either as "ballots" or "votes" indistinctively.

[101] Swiss citizens have the right to launch popular initiatives in order to put their proposals on the political agenda and initiate a referendum on it. They can request a revision of the Constitution, the adoption of a new law, and repeal and/or amend existing law. Referendums can be mandatory or optional, depending on the issues. A referendum is mandatory for the amendment of the Constitution or regarding Switzerland's membership to international organisations. When referendums are mandatory, they also require a double majority: a majority of voters and a majority of cantons. Additionally, parliamentary decisions and law amendments can be put to an optional referendum if requested by 50.000 eligible voters. A popular initiative supported by 100.000 eligible voters can even propose a change of the Federal Constitution (OSCE/ODIHR, 2007c: 3).

[102] Cantons are in principle free when it comes to the organisation of cantonal and electoral votes, as long as they respect the general rules of Swiss federal constitutional law, and in particular the guarantee of political rights that protects secret suffrage [emphasis added] (Swiss Federal Council, 2013: 71). Overall, cantons have usually followed the requirements adopted by the Confederation for their communal and cantonal ballots as well (Driza Maurer, 2016a: 264-265).

[103] More specifically, the Swiss Federal Chancellery is responsible for spelling out and communicating the federal requirements, for receiving the requests from the cantons willing to conduct an online voting pilot, assessing them and issuing recommendations to the Federal Council, as well as for receiving the results of remote electronic voting and other statistical data and publishing them, among other tasks (Swiss Federal Council, 2013a: 39-40). In addition to the Chancellery, there are other federal institutions who are also involved in the development of remote electronic voting, such as the Federal department for foreign affairs, the Federal office for justice, the Federal data protection and information commissioner, the technology governance unit of the Confederation and the Federal office for the equality of persons with disabilities (Swiss Federal Council, 2013a: 40).

2013a: 25). At the cantonal level, the authority in charge of remote electronic voting is in all the cases the team responsible for political rights[104]. On their side, communal instances are not directly involved in remote electronic voting, since it is centralised at the cantonal level[105] (Swiss Federal Council, 2013a: 42).

The applicable regulation for elections and popular ballots comprises the Federal Constitution, the federal acts on Political Rights (161.1) and on Swiss Persons and Institutions Abroad (195.1), as well as the respective federal ordinances on Political Rights (161.11) and on Swiss Persons and Institutions Abroad (195.11). Details related to the organisation of elections and popular ballots are regulated at the cantonal level (OSCE/ODIHR, 2007c: 2). Remote electronic voting is regulated within this framework on political rights. In this sense, art. 34 of the Swiss Constitution enshrines the political rights, providing that this guarantee protects the free formation of opinion by citizens and the faithful expression of their will. At the federal level, the Federal Act on Political Rights authorises the testing of remote electronic voting and the Ordinance on Political Rights sets the specific requirements for its adoption[106] (Swiss Federal Council, 2013a: 105). The Act prescribes in its art. 8 a simple voting procedure, the guarantee the verification of eligibility to vote, voting secrecy and the counting of all the votes cast, and to prevent violations (Swiss Federal Council, 2002: 619). While these provisions initially only applied to postal voting, the Federal Act on Political Rights was later amended, and similar provisions were detailed for remote electronic voting in its article 8a.2[107].

In turn, arts. 27a to 27q of the Federal Ordinance on Political Rights sets the technical, legal, and practical requirements for the conduct of remote electronic voting pilots, as well as the voters eligible to vote online (Swiss Federal Council, 2013a: 26). As we will see in the next pages, the Confederation additionally developed a specific instrument for the regulation of remote electronic voting, the Federal Chancellery Ordinance on Electronic Voting (VEleS) and its technical annex[108]. According to an expert group that was set in

[104] In most cantons this task is assumed by the State Chancellery, sometimes by the interior minister or by another instance. Notwithstanding, they usually delegate some tasks (i.e., those related to new technologies) while the exploitation of the systems is trusted to other cantonal instances or to private organisations (Swiss Federal Council, 2013: 40). More specifically, they have the following key tasks: (1) request the authorisation to the Federal Council, (2) coordinate, plan, prepare and run the ballots with remote electronic voting (including the printing of the voting materials), (3) inform eligible voters ahead and during the voting operations, (4) organise a crisis group and prepare according to crisis conventions, and (5) communicate the conduct of the remote electronic voting to the electorate (Swiss Federal Council, 2013a: 40-41).

[105] Notwithstanding, communes are still responsible for the conduct of certain tasks, especially in highly decentralised cantons, such as keeping electoral registers (which are derived from the citizens registers that they keep), transmission of register data to the canton, presentation of voter cards, communication with their electorate, part of the delivery of voting materials, training of staff in polling stations (i.e., to prevent voters who have already voted online to also vote in polling stations), and tabulation of results (Swiss Federal Council, 2013: 42-43).

[106] Relevant provisions are also found in the 1992 Federal Data Protection Act. The links between data protection and remote electronic voting will be specifically addressed in section II.3 below.

[107] Art. 18.4 of the Federal Act concerning Swiss People and Institutions Abroad of 26 September 2014 refers to this article when it comes to the right to vote of Swiss citizens abroad.

[108] It is important to note that such instruments, however, only apply to federal ballots and not to cantonal and communal ones, which are regulated at the cantonal and communal level, respectively (Swiss Federal Council, 2013: 13). At the same time, however, federal approval is a condition for the validity of the cantonal legislation on political right, as established in art. 51 *et seq.* of the Swiss Federal Constitution and art. 91.2. of the Federal Act on Political Rights (Swiss Federal Council, 2013: 29).

2017[109], this hierarchy helps in setting at a higher normative level those legal provisions guaranteeing the proper conduct of the ballots and reinforcing trust in electronic voting in a significant way (Swiss expert group, 2018: 38). On the other hand, the higher the normative level, the more abstract the provisions need to be, and thus lower-level regulations are considered necessary to detail the technological aspects.

Historically, it is possible to distinguish four main phases in the introduction of remote electronic voting in Switzerland:

a) The feasibility of introducing remote electronic voting in Switzerland (2000-2002) and the first binding pilots on remote electronic voting (2003-2007)

Following the adoption of the Federal Council's strategy for an information society in 1998, the two chambers of the Swiss parliament mandated the Federal Council to study the advantages and disadvantages of electronic democracy in 2000 (Swiss National Council, 2000; Swiss Council of States, 2000). Following, the Federal Council instructed the Federal Chancellery to test the feasibility of remote electronic voting in Switzerland (Swiss Federal Chancellery, 2004: 7). The Federal Chancellery set up, in turn, a working group made up by representatives of the Confederation and the cantons (Swiss Federal Council, 2006: 5212). The Federal Council published a first report on electronic voting on January 2002, analysing its chances, risks, and feasibility (Swiss Federal Council, 2002; 2013: 2). The report identified several opportunities for voting technology, including how they eased citizen participation in elections and votes[110], raising voter turnout[111], and highlighted possibilities for Switzerland to become a pioneer on the adoption of these technologies[112], to name just a few examples. More important, the report also highlighted that with electronic voting the democratic principle "one voter, one vote" would be better protected from classical abuses (Swiss Federal Council, 2002: 614). At the same time, the report also acknowledged several risks and challenges[113].

[109] The reports and the minutes of the Expert Group on E-voting (GEVE, in French) can be found online:<https://www.bk.admin.ch/bk/fr/home/droits-politiques/groupe-experts-vote-electronique/rapports-et-etudes-concernant-le-vote-electronique.html> [retrieved: 27 May 2022]

[110] In the opinion of the Swiss federal institutions, this would be mostly the case for blind and visually impaired voters (as we will see later with more detail), as well as for voters abroad who, in the opinion of the Swiss Federal Chancellery, are often exposed to the hazards [sic] of the post (Swiss Federal Chancellery, 2004: 7).

[111] Notwithstanding, raising voter turnout was not considered a crucial argument (Swiss Federal Chancellery, 2004: 7). The rationale to introduce remote electronic voting was rather to adapt the democratic processes to the evolution of society, in particular to the computerisation of the means of communication, by allowing citizens to use the same means that they use daily to communicate to vote (Swiss Federal Council, 2002: 620).

[112] For instance, in its 2004 report, the Swiss Federal Chancellery developed this idea by arguing that "by launching its preliminary project on electronic voting, Switzerland plays a pioneering role in Europe. This advancement in terms of knowledge in the field of electronic democracy will place the country in a good position on the international market" (Swiss Federal Chancellery, 2004: 19). In a similar way, in its 2006 report the Federal Council argued that "it will allow Switzerland to extol the merits of direct democracy on the international scene and to assert itself as a market of the future by offering an additional modern service" (Federal Council, 2006: 5206).

[113] These included, among others, inequalities in access to technology and digital literacy (i.e., the "digital divide"), the federal organisation of the country, technological problems, and trust in remote electronic voting (and its lack thereof), as well as risks of abuse. Among the latter, the Federal

Balancing both advantages and disadvantages, the Federal Council suggested a step-by-step introduction of remote electronic voting. On the one hand, remote electronic voting was to be introduced in phases. The first phase would allow voters to vote online in votes[114], at all levels: federal, cantonal and in the communes (Swiss Federal Council, 2002: 642). In the opinion of the Federal Council, the lack of specific experiences on the use of remote electronic voting[115] meant that it was not possible to learn from specific processed (i.e., elections or votes) and apply the lessons learned to others. Likewise, it was expected that through a step-by-step approach, those directly concerned with the new voting channel would be more prone to accept it (Swiss Federal Council, 2002: 642). On the other hand, a principle that has guided the introduction of internet voting in Switzerland from the outset is that permanent and absolute security is "an illusion" [sic] (Swiss Federal Council, 2002: 639). More specifically, the Federal Council stated that remote electronic voting should be as secure as the other channels, which did not mean that it should be 100% secure (Swiss Federal Council, 2002: 632). The way to achieve this level of security in remote electronic voting was by means of risk management[116]. Quite interestingly, this security was not meant to be achieved in terms of the remote electronic voting systems only, but based on a combination of law, technology, and the practice by voters themselves[117].

Council specifically listed vote-tampering (i.e., computer programmes modifying the contents of the votes cast) and technological failures and errors, which in the opinion of the Council would be more difficult to identify in an electronic system than in a "normal one" [sic] . Specific attention was to be paid to secret suffrage, a principle that the report identified as key for the adoption of remote electronic voting (Swiss Federal Council, 2002: 626). The 2004 report by the Federal Chancellery echoed these exact concerns. It also considered the impact of remote electronic voting on political parties, since their means of influence could be either strengthened or weakened by the development of electronic democracy (Swiss Federal Chancellery, 2004: 8).

[114] These experiences would allow for applying the lessons learned to electronic elections in a second phase, since these were considered more complex than votes, and in particular to the elections to the National Council, which was considered especially challenging. For this reason, it was considered necessary first to test internet voting in the framework of municipal and cantonal elections (Swiss Federal Chancellery, 2004: 10). Taking this into account, it was planned to use internet voting for these elections before 2011, this is: almost ten years after the first pilots were conducted. This is another example of the "security first" approach in the introduction of remote electronic voting.

[115] At this stage, lessons could be only drawn from the experiences with postal voting (Swiss Federal Council, 2006: 5206).

[116] The Swiss Federal Council further developed this point in its third evaluation report: it is commonly agreed that risk zero does not exist. Notwithstanding, the legal framework requires that any targeted or systematic fraud is excluded. This principle is inspired in traditional voting channels, for which isolated irregularities are accepted but would allow for identifying a systematic fraud with high probability (Swiss Federal Council, 2013: 74). How are errors to be dealt with, then? The Swiss Federal Council (2013: 74) additionally detailed that if despite the measures taken (e.g., system architecture, use of current cryptographic techniques, logical and organizational separation of sensitive parts of the system, interventions on controlled authorizations, etc.) a problem is detected (thanks, in particular to the permanent monitoring of the system), "zero tolerance" is applied, which means that any problem, no matter how small, should be explained and fraud excluded. Otherwise, the result of the electronic channel would not be taken into account. In this case, it would be necessary to assess whether the results of the electronic vote are likely to modify the outcome of the ballot, in which case the ballot would have to be repeated (something that the Federal Council wished to avoid "at all costs" [sic]).

[117] Drawing from the pilot project in the canton of Zurich (that will be detailed later), the feasibility study identified three different levels of security: system security would represent 70% of overall security and it was split between technical security (30%) and the security resulting from the functional and the structural organization of the system (40%). The remaining 30% was to be

The introduction of internet voting would however require first the amendment of the Swiss legal framework of elections and votes. As it has been already mentioned, the Federal Act on Political Rights sets the formal requirements for elections, votes, referendums, and popular initiatives. The Ordinance on Political Rights further details these provisions. The political rights of Swiss abroad were regulated in the Federal Act on Political Rights of Swiss Abroad and the respective ordinance[118]. All these regulations assumed that votes and elections were to be conducted by traditional means, meaning with paper ballots. For instance, art. 5.2 of the Federal Act on Political Rights provided that "ballot papers that are not pre-printed must be completed by hand. Pre-printed ballot papers may be altered only by hand", which would exclude *a priori* the electronic casting of ballots[119]. Thus, between June and September 2001 the Swiss Federal Council launched a consultation to fill these *lacunae* and come up with a legal basis for the pilots. Following, the Swiss parliament adopted the new legal basis for the conduct of the pilots by amending the Federal Act on Political Rights of 17 December 1976 on 21 June 2002 (Swiss Federal Council, 2006: 5213). With the new regulation, the Swiss Federal Council would be able to authorise those interested cantons and communes to test remote electronic voting (by limiting its reach to a part of the territory, to certain dates and for certain contests). Following the amendment of the Act, the Federal Council amended in turn the Ordinance on Political Rights on 20 September 2002.

With the new regulatory framework in place, and based on the step-by-step approach, the Swiss Federal Council authorised[120] three cantons to run pilot projects with internet voting between 2003 and 2005: Geneva, Neuchâtel, and Zurich. The three cantons chose a different approach towards remote electronic voting, which would allow for testing and evaluating specific solutions (Swiss Federal Council, 2002: 648).

Geneva[121] run the first binding ballots with internet voting already in 2003 (on municipal matters) and 2004 (for federal ballots). Four municipalities in Geneva were able to test internet voting at the communal level, respectively: Anières (as soon as 19 January 2003),

achieved from both the protection guaranteed by the law (i.e., the criminal code) (20%) and from the security guaranteed by voters themselves (10%) (Swiss Federal Council, 2002: 640). While it is not clear how these percentages may have been established, this approach helps us understood the suite of tools available to secure the use of remote electronic voting. More importantly, it also draws our attention to the responsibility assigned to voters themselves.

[118] The law and the ordinance were abrogated on 26 September 2014, when the new Federal Act concerning Swiss People and Institutions Abroad was adopted instead (and which entered into force on 1 November 2015).

[119] At the same time, the Act also provided that "cantonal vote recording vouchers for electronic data processing shall be regarded as equivalent to official ballot papers" (art 5.1) (Swiss Federal Council, 2002: 647). In a similar vein, the Act also provided that for the elections to the Swiss National Council, the Federal Council could authorise the cantons to adopt provisions derogating from the Act with a view to adopt new technological measures to stablish the results of the ballots (art. 84).

[120] According to the amended Ordinance on Political Rights (version of 28 January 2003), the remote electronic voting trials conducted in the framework of popular votes and elections would be subject to the authorisation of the Federal Council (art. 27a.1). The Federal Council was to decide (art. 27c): (a) for which elections or federal votes authorises the use of Internet voting, (b) during which period of time, and (c) in which communes of the canton the results will have binding effects.

[121] Art. 188 of Geneva's cantonal Act on the Exercise of Political Rights of 15 October 1982 authorised the canton's Council of State to run tests with a view to adapt the exercise of political rights on cantonal and communal matters to the possibilities offered by the technique, under certain conditions (Swiss Federal Council, 2006: 5221).

Cologny (November 2003), Carouge (April 2004) and Meyrin (June 2004)[122]. Neuchâtel and Zurich followed in 2005. The project in Neuchâtel[123] was framed within a wider digitisation process, the so-called *guichet virtuel* (Swiss Federal Council, 2002: 650) or *sécurisé* (Swiss Federal Chancellery, 2004: 8) *unique* (in what follows, GSU). Thus, online voting was to be just one of the services offered by this portal. Remote electronic voting

[122] The number of eligible voters in these ballots ranged from 1.162 in Anières to 9.180 in Meyrin. In turn, the use of the remote electronic voting ranged from 22% in Meyrin to 43,6% in Anières (Swiss Federal Chancellery, 2004: 36). Two ballots at the federal level followed in 2004, during the votes on 26 September (with 20.000 eligible voters) and on 28 November (with 40.000 eligible voters). During the first of these ballots, it would have been possible to vote electronically at the three levels (communal, cantonal, and federal) simultaneously (Swiss Federal Council, 2005: 5225). Overall, between 22% and 25% of eligible voters decided to vote online. During a cantonal ballot on 17 April 2005, up to 88.000 eligible voters in 14 communes could vote electronically (Swiss Federal Council, 2005: 5224).

The pilot project in Geneva was characterised by (1) a legal framework that enabled the cantonal Council of State to introduce an electronic process on a trial basis (see footnote 121 above); (2) a widespread resort to postal voting; and (3) a centralised and digitised voter register. The principle (or keyword) that guided the development of remote electronic voting in Geneva was "simplicity" (Swiss Federal Council, 2006: 5222). The remote electronic voting process was to be as similar as possible to the one in place to vote by post (Swiss Federal Council, 2002: 649; Swiss Federal Chancellery, 2004: 8): voters would receive their credentials (a password) by post, shielded by a tamper-evident overlay. To reveal their password, they would have to scratch the area of their voting card where the password had been hidden. To authenticate themselves, they would have to introduce this password as well as their birthdate into the system. The team responsible for this pilot project thus considered that the voting card was at the core of their system (Swiss Federal Chancellery, 2004: 35). This mechanism would also prevent voters in Geneva from voting twice. Since the area in a voter card hiding the credentials would have to be scratched to reveal it, it would be possible for electoral officers in polling stations to know whether a given voter had already voted online (their card would have been scratched) or not (the card would not have been scratched) (Swiss Federal Council, 2002: 649). The system used in Geneva was developed by the *Centre des technologies de l'information de l'Etat* in partnership with Hewlett Packard (HP) and Wisekey and was owned by the canton (Swiss Federal Chancellery, 2004: 34). In Geneva, the initial development of the Internet voting system was entrusted to a consortium of private companies, following a call for tenders. The specifications, published on 20 November 2000, described the architecture of the system, and detailed the legal requirements for ballots according to Swiss and cantonal law. Since 2005, the system has been entirely in the hands of the State, including its development and maintenance (Swiss Federal Council, 2013: 54-55). Blue-infinity also contributed to the predevelopment of the system for the security aspects (Swiss Federal Council, 2006: 5221). As reported by the canton, such partnership made it possible for the necessary elements for transparency and the proper conduct of the ballots to be included in the specifications (Swiss Federal Chancellery, 2004: 34).

From a technological perspective, votes cast were encrypted to protect voters' choices. At the end of the ballot, the electronic counting would be conducted in the presence of representatives from political parties. First, they would verify that the number of electronic votes cast was the same than the number of voters having cast a vote in the electoral rolls. The votes would then be shuffled to modify the order of the votes cast (so they could not be related to the order in which the identity of the voter was registered, something that was stored in another database). To decrypt the electronic ballots, two controllers would have to introduce their passwords (decided at the beginning of the online voting period and only known to them) (Swiss Federal Council, 2006: 5223). The electronic votes would then be added to the votes cast by post and at polling stations.

[123] In October 2001, the Grand Council of Neuchâtel adopted an ordinance authorising the canton's Council of State to introduce electronic voting on an experimental basis and subject to the agreement of the Confederation, on condition that the security of the vote and the respect for the secrecy of the vote were guaranteed (Swiss Federal Council, 2006: 5226). With the amendment of the cantonal Act on Political Rights in September 2002, the setup of a new organisation of the ballots was made possible.

was offered for the first time in the context of a federal ballot on 25 September 2005[124]. 2.000 voters were offered the possibility to cast their vote remotely by electronic means, out of which 68% decided to do so. A second federal ballot followed on November 2005,

[124] In 2004 the Grand Council of Neuchâtel adopted the Act for the GSU. This law defines in particular the procedures by which access rights are issued (art. 10, 18 and 19), various aspects related to the security of the GSU (art. 13 to 17) and to personal data protection (art. 23 to 25).

The pilot project in Neuchâtel was characterised by its decentralisation, the conduct of the votes being under the responsibility of the 62 communes in the canton. The main changes were the set-up of a central voter register ahead of each ballot, the printing and distribution of voting material centrally, and the creation of a unique legitimation card per voter and per ballot, integrating the necessary information to vote by post and electronically (Swiss Federal Council, 2006: 5226). Thus, in a first phase, a specific voter register would have to be created ahead of each ballot (even if it was not yet possible to vote online). To be able to vote online, voters would have first to register and have general access rights to the GSU, which would require them to prove their identity in person. More specifically, they would have to fill a registration form, to legalise their signature with a competent authority, and to submit their request to the State Chancellery (Swiss Federal Chancellery, 2004: 8). Upon identification, they would be provided with a specific access code (*code contrat*, in French) and a password to access the GSU (Swiss Federal Council, 2002: 651). To connect to the GSU, they would have to provide both these codes, as well as a session number specific for each connection (Swiss Federal Chancellery, 2004: 8). Based on the central register, each eligible voter (namely, those registered at the GSU) would receive a unique confidential voter card together with their voting materials (Swiss Federal Council, 2002: 651). This voter card contained unique references (a barcode) and a security hologram (Swiss Federal Chancellery, 2004: 41). Just as in Geneva, the voter card became essential to vote: it had to be either returned to the municipal administration by post, with the voter's date of birth and signature, or handed at the polling station. Having such a central register would also prevent voters from casting more than one vote. The last operation concerning the new organisation of the ballots was the recording of the votes. This operation consisted in entering the date, time and means used by a voter to cast their vote, ensuring that each voter had cast just one vote, be it by post, at the polling station or, in the second phase, through the Internet (Swiss Federal Chancellery, 2004: 41). In a second phase, the voter card would contain a unique access code that they would have to use to access the voting platform within the GSU (Swiss Federal Council, 2002: 651). Ahead of the ballot on 25 September 2005, Neuchâtel had organised several tests: in January 2005, with 336 voters from the cantonal administration, the Federal Chancellery and a monitoring group. A second one followed in February, and a third one in March. In the later, 2.600 people were able to voter online.

The solution was developed in partnership with Arcantel (for the application) and Scytl (for the cryptographic protocol). The voting process worked as follows: voters would have to access the GSU first. By accessing the voting application, they would be shown the ballots for which they had voting rights. Voters would then select their choices for each ballot, and then the system would display a summary of their choices. To cast their ballot, a voter would have to type the validation code provided in their voting card. Upon casting the ballot, the application would display a confirmation code (that voters should check against the code provided in their voting card) and a second code that acknowledged the receipt of the vote. Should the confirmation code displayed be different from the one in the voter card, it would mean that the vote had not been received by the voting server. Having voted online, voters would be prevented from voting by post or in polling stations. By checking the barcode in the voting card, it would be possible to know if someone had already voted either online or by post, and prevent them from casting a second vote.

One final characteristic of this project was that it offered end-to-end encryption from the outset, meaning that votes were encrypted (using asymmetric cryptography) already in the voting device used to cast it and were kept sealed until the decryption stage. Before the start of the voting process, the electronic ballot box would be configured and a pair of keys would be generated: the public key (to encrypt the votes) and the private one (to decrypt them) (Swiss Federal Council, 2006: 5229). The later would be in turn divided into different shares, each one stored in a smartcard. Each smartcard (containing a share of the private key) was handed to a member of the electoral commission who would protect it with a password known only to each of them. All the materials would then be stored in a safe at the State Chancellery and the cantonal police. To decrypt the votes after the voting period had ended, the members of the electoral commission had to retrieve their smartcard and activate it using the password that they had chosen at the beginning of the voting process.

when 1.345 voters made use of this channel (out of 2.442 eligible voters, namely a 55,08%). All in all, votes cast online in the latter ballot represented 2,5% of all votes cast. Voters also had the possibility to vote online for a by-election to the Council of States in October, when 1.194 votes were cast online. The third pilot project was implemented in Zurich[125]. Zurich run two tests with Internet voting in 2005. The first one took place in the village of Bülach in October[126]. At the federal level, voters were able to vote online during the votes of 27 November[127].

The Swiss Federal Council evaluated these experiences in a 2006 report[128] and concluded that the tests had been a success: a survey had revealed that two thirds of

[125] This project was characterised by even more decentralisation. Thus, it was first necessary to adopt a voter register at the cantonal level as well. As a matter of fact, Geneva was the only canton that already had a digital voter register by the time they launched the remote electronic voting project (Swiss Federal Council, 2006: 5222). The adoption of such a register was challenging for two reasons: first, because of the differences in population between the 171 communes in the canton (ranging from the smallest communes, with only 200 eligible voters, to Zurich, with more than 200.000 eligible voters in the early 2000). Second, because each commune used a different information system to manage their population and/or voter registers. To accommodate this reality (and the electronic voting channel) the cantonal Act was amended in September 2003. Art. 4.2 provided that political rights could be exercised by electronic means should the technical and organisational requirements allow so. Namely, it should be possible to correctly ascertain the voters' will while ensuring the respect for secret suffrage (Swiss Federal Council, 2006: 5232). The law was complemented by the cantonal Ordinance on Political Rights of 27 October 2004. Art. 12 of the Ordinance provides that there can be derogations from its provisions for the conduct of pilots with internet voting, modalities that should be regulated by the State Council of the canton of Zurich.

The online voting system used in Zurich was developed by Unisys. The development of the electronic voting system was awarded to Unisys within the framework of a public tender procedure in 2003. The mandate concerned the development of both Internet and SMS voting. In 2007, the cantonal government entrusted its operation to the same company in its decision to develop electronic voting for the period 2008-2011 (Swiss Federal Council, 2013: 54). The system was subject to two audits (one by Swisscom solutions and another one, mandated by the Swiss Federal Chancellery, by Blue-infinity).

In practice, a specific voter register had to be created ahead of each ballot. As in the two other pilot projects, each eligible voter would then receive their credentials ahead of a vote. Voters would identify themselves by means of an access code printed on their voter card. After the voter had marked their selections, they would see displayed a summary of their choices. At this stage, they could still modify their choices or decide to cast their vote. Once the vote had been cast, the process ended. The credentials were accompanied by a barcode. This barcode allowed the election officers to verify that a voter had not already cast an electronic vote when attempting to vote in person or by post. At the end of the voting period, the communes would be responsible for decrypting the ballots. The teams responsible for the organisation of a ballot would receive the passwords necessary to decrypt the votes by email on election day.

[126] 9.943 eligible voters in the municipality were offered the possibility to vote online, and 1.006 took advantage of it (equivalent to 25,68% of all votes cast). Additionally, Zurich also piloted SMS voting. In this occasion, 455 voters used this channel (Swiss Federal Council, 2006: 5236). The piloting of SMS voting was discontinued in 2011 (Swiss Federal Council, 2013: 24)

[127] Out of 16.762 eligible voters in three communes (Bertschikon, Bülach and Schlieren), 1.397 votes were cast electronically (equivalent to 22,14% of all votes cast). Additionally, the system was also tested during the elections to the Student Council of the University of Zurich in December. There were 1.767 voters who cast their vote, and 88.55% of them did so electronically. Finally, online voting was also offered in the context of the elections of Bülach in April 2006, both to their legislative (with proportional representation) and executive (majoritarian system) representation bodies. Out of 3.522 votes cast during these elections, 700 of them (equivalent to 19,88%) were cast electronically (Swiss Federal Council, 2006: 5236-7).

[128] In the meantime, the implementation of these first pilots and the "immense echo" [sic] they received from the media aroused an important demand for information from the public and, in

people surveyed were aware of the projects, and 90% of voters involved in the tests would like to continue being able to vote electronically (Swiss Federal Council, 2006: 5275). Overall, the conduct of the pilots was thus perceived as positive (Swiss Federal Council, 2006: 5276). For example, the Federal data protection officer, who had raised concerns about the adoption of remote electronic voting in its annual reports for 2002 and 2003, no longer formulated any criticisms in connection with the implementation of electronic voting after examining the security architectures of the cantonal pilot systems (Swiss Federal Council, 2006: 5255). Additionally, the Courts systematically rejected the appeals filed against these votes[129]. In fact, already in 2004, several cantons had expressed their interest in joining the internet voting pilots, including Bern, St. Gallen and Tessin (Swiss Federal Chancellery, 2004: 9).

Furthermore, the pilots had also allowed for successfully validating the remote electronic voting systems, which did not experience any failure (Swiss Federal Council, 2006: 5240). In this sense, the close collaboration between the Confederation and the cantons of Geneva, Neuchâtel and Zurich (as well as the cooperation between them) had resulted in the availability of three internet voting systems that had been tested at the communal, cantonal and federal levels. At this stage, now the rest of the cantons could also take advantage of the three systems available (Swiss Federal Council, 2006: 5207). All in all, the first projects showed that remote electronic voting was feasible (Swiss Federal Council, 2006: 5276). Notwithstanding, the step-by-step approach in the introduction of remote electronic voting should be maintained, not to lose sight of the inherent risks of remote electronic voting (Swiss Federal Council, 2006: 5206). Therefore, the main conclusion drawn from these first pilots was that it was necessary to set up a legal framework at the federal level for the introduction of remote electronic voting (Swiss Federal Council, 2006: 5207).

Following the first pilot phase, a second intermediate phase was launched (Swiss Federal Chancellery, 2004: 9). The interested cantons could freely use most of the pilot systems developed, their components as well as the know-how on their future use gathered during the first pilot phase (Swiss Federal Council, 2006: 5276). In this new phase of extended pilots, risk management would still be placed at the core of Switzerland's Internet voting strategy (Swiss Federal Council, 2006: 5207). In this sense, cantons would be allowed to decide independently whether to introduce remote electronic voting or not, but the Confederation would assume a coordination role. In practice, it meant that Federal Council kept limited veto capabilities regarding the time frame, territorial scope, and object of these extended pilots (Swiss Federal Chancellery, 2004: 9). Likewise, and in addition to the use of remote electronic voting being subject to an authorisation by the Federal Council,

particular, from those cantons that had not been involved in the pilot projects (Swiss Federal Chancellery, 2004: 7). For these reasons, the Swiss Federal Chancellery decided to publish an intermediate evaluation report on the pilots already 2004.

[129] According to Beat Kuoni (2015: 202), in Switzerland "[l]itigaiton relating to the use of electronic voting is rare" and swiss courts have had few opportunities to consider the legal issues arising from Internet voting. Following the first tests with internet voting in the canton of Geneva in 2004 and 2005, three appeals were filed. The canton's "Administrative Court dismissed the appeals on the grounds that the authorisation decision [to authorise a trial with electronic voting] in dispute did not infringe any procedural provisions" (Kuoni, 2015: 202).

no more than 10% of eligible voters at the federal would be able to take advantage of this new voting channel[130] (Swiss Federal Council, 2006: 5207).

The publication of the second report on e-voting and the adoption of the amended legislation by the Swiss Parliament in 2007 (which entered into force in 2008), put an end to the first pilot phase and marked the beginning of a new phase of extended pilots (Swiss Federal Council, 2013a: 24).

b) Extended pilots on remote electronic voting (2008-2013)

The amended regulation that entered into force in 2008 affected the Federal Act on Political Rights, the Federal Act on Political Rights of Swiss Abroad and the Federal Ordinance on Political Rights. They allowed for the extension of the pilots to new cantons and created the conditions for Swiss voters abroad to be able to use this channel. They also came up with new requirements on accessibility for voters with disabilities, with special focus on visually impaired and blind voters (Swiss Federal Council, 2013a: 27). At the time, the proportion of the electorate that was eligible to vote online was limited to the 20% of the cantonal electorate and 10% of the overall Swiss electorate.

Therefore, this third phase in the introduction of remote electronic voting saw an increase in the number of cantons allowing votes to be cast online from three in 2007 to 13 in 2009[131], meaning that by this time half of the cantons were offering remote electronic voting (Swiss Federal Council, 2013a: 3). The three pilot cantons (Geneva, Neuchâtel, and Zurich) offered their systems to the rest of the cantons[132], and by 2013 four had already adopted it at the federal level during the 2011 elections to the Swiss National Council: Basel Stadt, Graubünden, Aargau, and St. Gallen. To extend the use of remote electronic

[130] As in the previous phase, the extension of internet voting would also require first the amendment of the Swiss legal framework of elections and votes (i.e., of the Swiss Federal Act and the Ordinance on Political Rights). An Art.8-1bis would be added allowing the Federal Council to authorise the cantons having conducted a certain number of pilots (i.e., five successful federal ballots) to pilot Internet voting for a given period, with the possibility of limiting its use to a location, a date or given contests. An additional art. 5.b. would be added to the Federal Act on the Political Rights of Swiss Citizens Abroad also allowing them to vote online. Allowing Swiss citizens abroad to vote online would also require the harmonisation of the voter's registers (Swiss Federal Council, 2006: 5277). Finally, allowing new cantons to use any of the available remote electronic voting solutions would require the Swiss Federal Council to not only define the requirements for these solutions (set out in arts. 27a et seq.), but to also verify that the systems used complied with these requirements (Swiss Federal Council, 2006: 5279-80).

[131] In its 2013 report, the Swiss Federal Council identified three main mechanisms by means of which these new cantons introduced internet voting: (1) cantonal laws allowing the resort to internet voting, provided that the technical and organisations requirements were met and the fundamental principles regulating the exercise of political rights were respected (Berne, Lucerne, Solothurn, Basel-Stadt, Schaffhausen, Thurgau, and Fribourg); cantons that regulated the possibility for Swiss voters abroad to vote online, regulated in specific executive instruments (Bern, Lucerne, Basel-Stadt, Solothurn, Schaffhausen, and Thurgau), and (3) specific aspects of remote electronic voting being dealt with in the ordinance on political rights (St. Gallen, Graubünden and Aargau).

[132] The cantons that did not have their own remote electronic voting systems benefited from the agreement reached between the three pilot countries and the Confederation, that had foreseen that the systems developed with the financial support of the Confederation would be offered for free to the confederation and the interested cantons (Swiss Federal Council, 2013: 55). The fact that some cantons offered their systems to others also resulted in a new provision on data exchanges in case that a canton hosted another canton's remote electronic voting infrastructure (Swiss Federal Council, 2013: 28).

voting, accompanying groups (*groups d'acompagnement*, in French) were set up. These accompanying groups were external agencies recognised by the Swiss Federal Chancellery and made up by representatives from the cantons and the Confederation. They were tasked with conducting a sort of peer assessment when an online voting system was designed and subsequently modified (Swiss Federal Council, 2013a: 4).

Additionally, the three initial pilot cantons and their systems also saw changes throughout this pilot phase. For instance, Geneva amended its cantonal constitution twice[133]: first, a new article was drafted introducing the principle of electronic voting in 2009 [134]. The new constitution also set up a central electoral commission. Following the use of Geneva's remote electronic voting system by another canton, Basel-Stadt, during the 2011 federal elections by Swiss abroad, the system was used for the first time for cantonal elections in November 2012. At the cantonal level, Geneva's system was also used by all the cantonal electorate in four occasions, starting in May 2011 (Swiss Federal Council, 2013a: 52; 2013: 59). On their side, Neuchâtel became the first canton to allow voters abroad to vote online in June 2008[135] (Swiss Federal Council, 2013a: 51). Lastly, the canton of Zurich extended the use of Internet voting from three communes to 13 and to a part of their Swiss voters abroad[136]. However, in 2011 the canton decided to discontinue its internet voting project pending further harmonisation of the registers kept by the municipalities and until a federal decision to expand the electorate eligible to vote online was adopted (Swiss Federal Council, 2013a: 51; Serdült et al., 2015). Following this decision, seven cantons within the consortium (Fribourg, Solothurn, Schaffhausen, St. Gallen, Graubünden, Aargau and Thurgau) resumed a cloned copy of Zurich's remote electronic voting system, in partnership with a private company that was tasked with the operation of this channel for Swiss voters abroad in these cantons (Swiss Federal Council, 2013a: 33).

Therefore, this phase focused on Swiss voters abroad and voters with disabilities (Swiss Federal Council, 2013a: 3). In line with the goals set by the Swiss Federal Council and the Swiss Parliament in 2006, the extended pilots had Swiss voters abroad as a priority target group. Notwithstanding, not all Swiss voters abroad would be given the possibility to vote online. In this sense, Swiss voters residing in a country that was not part of the EU nor a signatory state of the Wassenaar arrangement would be *a priori* excluded[137]. In September

[133] In the first pilot phase, Geneva had adopted remote electronic voting based on a derogation of its cantonal Act on the Exercise of Political Rights, established in its art. 188 (see footnote 121 above).

[134] Art. 48 Constitution of Geneva. The constitution was further amended in 2012 so it would not make specific reference to specific voting channels (Swiss Federal Council, 2013a: 29).

[135] Out of the 152 Swiss voters abroad eligible to vote online, 57 ended up doing so. Overall, the participation in the ballot was of 48,3%. Out of 4.699 voters eligible to vote online, 33,9% of them (equivalent to 1.593) voted electronically. The number of Swiss voters abroad registered at the GSU increased to 217 in 2013 (equivalent to 5,4% of the 4012 Swiss voters abroad registered in municipalities within the canton) (Swiss Federal Council, 2013: 51). Neuchâtel saw an increase in the number of users registered at the GSU from 3.800 in 2007 to 21.200 in June 2012 (Swiss Federal Council, 2013a: 56).

[136] The number of voters eligible to vote online increased from 18.000 in 2008 to around 100.000 in 2011 (representing 12,5% of the cantonal electorate). Among the 18.000 Swiss voters abroad registered in Zurich, 60% were authorised to vote online (Swiss Federal Council, 2013: 56).

[137] As an example, in the five communes of Berne that piloted remote electronic voting on 12 January 2011, out of the 3.098 eligible Swiss voters abroad that could have cast their vote electronically,

2009, Swiss voters abroad were excluded from the cantonal cap with the amendment of art. 27.c.2 of the Ordinance on Political Rights.

At the same time, voters with disabilities, and especially those with visual impairment or blind, also benefited from a priority treatment (Swiss Federal Council, 2013a: 5). While when voting with traditional means voters with disabilities needed the assistance of a third party to cast their vote, which was a breach to their right to vote in secret, remote electronic voting was a way for this group to vote independently (Swiss Federal Council, 2013a: 63). When art. 27e^{bis} of the Ordinance on Political Rights entered into force in January 2008, cantons were encouraged to take into account the special needs of voters with disabilities and to offer them a voting channel that respected their right to vote in secret (Swiss Federal Council, 2013a: 64).

In 2011, a new strategy was adopted, defined jointly by the Confederation and the cantons, in a document known as the "e-voting roadmap" (Swiss Federal Chancellery, 2011). The roadmap became a reference document for the definition of the goals and the steps needed to achieve them. The roadmap identified three main goals (Swiss Federal Council, 2013a: 97-98):

- in the short term (by 2012), allow the majority of Swiss voters abroad to vote online;
- in the medium term, allow the majority of Swiss voters abroad to vote online for the 2015 elections to the Swiss National Council; and, following,
- allow all voters to vote online.

For all resident voters to be able to vote online, it would be required to develop and put in place the so-called second-generation remote electronic voting systems, such as the one tested in the online voting pilots in Norway in 2011 (Swiss Federal Council, 2013a: 11) and 2013. Additionally, the roadmap also identified five key domains for the establishment and the extension of remote electronic voting[138]. Based on the roadmap, the legal framework was also amended during this phase. For instance, the limit of 20% of the cantonal electorate would be increased to 30% on 1 June 2012 (Swiss Federal Council, 2013a: 27).

Additionally, in 2011 the OSCE/ODIHR also deployed election observers for the first time to monitor Internet voting in Switzerland, in the context of the Swiss Federal elections of 23 October. It was the first time that the OSCE/ODIHR observed the use of remote

529 could not do so because of this requirement (Swiss Federal Council, 2013: 91). This restriction was justified on the grounds that only those states authorised the transmission of encrypted data (Swiss Federal Council, 2013a: 6), which as we will see with more detail later is key for the protection of confidentiality. Such restriction was not free from criticism. The Organisation of swiss abroad (OSE, from the French O*rganisation des Suisses de l'étranger*) argued that it was usually in the non-signatory countries of the Wassenaar arrangement where the postal services did not work properly, which in practice meant that without the option to vote online Swiss voters in those countries had no alternatives to vote at all (Swiss Federal Council, 2013: 7-8). We will get back to this issue when analysing the requirements and mechanisms to protect the confidentiality of voters' choices. When this restriction was later removed as of January 2014, the Federal Council considered necessary to raise awareness among Swiss voters living in the countries where the use of encryption was forbidden that there was a risk to their free expression of their will – and leave the decision of whether to vote online or not up to them (2013: 8).

[138] Namely: (1) a common strategy by the Confederation and the cantons; (2) security; (3) enlargement; (4) transparency; and (5) costs.

electronic voting in Switzerland, with about 22.000 Swiss voters abroad being eligible to vote online[139] (Swiss Federal Council, 2013a: 63). More specifically, two systems were tested for federal elections: the "consortium system", originally developed by the canton of Zurich, was used in Aargau, Graubünden, and St. Gallen, while the system developed by Geneva was used in Basel Stadt[140] (OSCE/ODIHR, 2011c: 7). The contest thus became an occasion for the OSCE/ODIHR to monitor the organisation and the conduct of internet voting in the four cantons that offered this channel to their voters abroad.

The OSCE/ODIHR conducted a needs assessment mission (NAM) [141] from 5 to 8 July[142]. The NAM recommended the deployment of an Election Assessment Mission (EAM)[143] (OSCE/ODIHR, 2011c: 10) and the observers were deployed in the country from 10 to 28 October[144] (OSCE/ODIHR, 2012a: 1). The final report was published in January 2012. Although it concluded that the remote electronic voting "pilot systems performed reliably and enjoyed widespread trust" (OSCE/ODIHR, 2012a: 2), 13 of the recommendations in the report were related to Internet voting (out of the 23). Overall, the OSCE/ODIHR's Election Assessment Mission pointed out that the systems would have benefited from improvements in certification, security, transparency and oversight (2012: 2).

Lastly, this phase also saw some additional rulings on the legality of e-voting[145]. All the cases were filled in the canton of Geneva (Kuoni, 2015: 2019). In a case filled in 2009, the Federal Court rejected an appeal of a voter who claimed that Internet voting would be too

[139] Out of which, about half voted via the internet (OSCE/ODIHR, 2012a: 15).

[140] In all cantons, voters accessed their internet voting systems via an internet browser and communications between the voting client and the server were protected by Secure Sockets Layer (SSL) technology (OSCE/ODIHR, 2012a: 16). Votes cast were encrypted directly on the voting device (Geneva's system) or once received by the server (consortium system) and were stored encrypted until the day before election day.

[141] A NAM is "usually deployed several months before a given election to assess the pre-election environment, including preparations for the event, to recommend whether an election-related activity is necessary and, if so, what type of activity best meets the identified needs" (OSCE/ODIHR, 2010: 26). It is not conducted by Election Observation Team, but by the staff of the ODIHR's Election Department. In the context of election technologies, it is also entrusted with "enquire about the plans for NVT-related events to help assess whether key events will take place before or after the deployment of the EOM core team" (OSCE/ODIHR, 2014: 14).

[142] The Needs Assessment Mission concluded that both systems provided for positive voter identification, as well as measures for voters to check the authenticity of the server, such as pictorial symbols and response codes (OSCE/ODIHR, 2011c: 7). The Mission also highlighted that "in principle" [sic], "the secrecy of the vote is protected by the separate storage of personal data and the unique voting number following the generation of the voting cards and before votes are cast" (OSCE/ODIHR, 2011c: 7). Notwithstanding, they also noted that certain issues applicable to both systems deserved further attention, including (but not limited to): the transparency of the source code, the access to and security of the servers, the access to voting cards to prevent anyone other than the intended voter from casting a vote, as well as the security of voters' computers.

[143] An EAM "do not comprehensively observe the whole election process, but instead follow specific issues identified by NAMs […] Such issue could include the legal framework for elections, the media environment, minority rights, campaign finance, the use of new technologies in voting and counting processes and election dispute resolution, as well as any other specific issues that may warrant some scrutiny" (OSCE/ODIHR, 2010: 31). In addition to EAM, the OSCE/ODIHR can also decide to deploy an Election Observation Mission (EOM), a Limited Election Observation Mission (LEOM) or an Election Expert Team (EET).

[144] Additionally, the New Voting Technologies Analyst appointed by the OSCE/ODIHR also had the chance to attend several planning sessions for the two remote electronic voting systems in September (OSCE/ODIHR, 2012a: 18).

[145] According to the OSCE/ODIHR those were the first rulings, but we have already mentioned the three rulings from 2004 and 2005 (see footnote 129 above).

easily falsified on the grounds that the case was unfounded. The decision is reported by Beat Kuoni (2015: 203) as follows:

> "The appellant demanded a rerun of the vote and claimed *inter alia* that it was too easy to falsify electronic voting and that voting secrecy was not guaranteed. The Federal Supreme Court took the view that these allegations were unjustified. The appellant had only claimed that there were general risks associated with voting online and had referred to the case law in other countries. The appeal did not raise any issues specifically related to the system used in the canton of Geneva. In addition, the appellant did not demonstrate how the system failed to meet the technical security requirements under federal law."

In five cases filled in 2011, one appellant called into question the system used during the votes (Hill, 2005). The appellant did not claim any damages regarding the counting nor the publication of the results of the electronic voting channel. He neither alleged the existence of an illicit influence from a third party that may have tried to interfere, modify, or turn away the e-votes. These appeals were rejected by the administrative chamber of Geneva's Court of Justice (Swiss Federal Council, 2013a: 36). Overall, the courts considered that the use of remote electronic voting was legal. In no circumstances the use of remote electronic voting resulted in the annulling, even partially, of the results of a ballot[146] (Swiss Federal Council, 2013a: 4). The Courts insisted that while it is not necessary to prove that a procedural defect decisively influenced the result of a ballot for it to be overturned[147], the annulment of a ballot based on the provisions of art. 34 of the Swiss Federal Constitution required the existence of a specific irregularity[148]. Therefore, a theoretical and abstract risk was not enough, and any such specific irregularity has had to plausibly influence the results (Swiss Federal Council, 2013a: 36).

c) A legal framework on remote electronic voting for a federal country: the Swiss ordinance on remote electronic voting (VEleS) (2014-2015)

Despite the overall satisfaction with the conduct of both the initial and the extended pilots, the Swiss Federal Council considered that several measures had to be adopted to generalise the use of remote electronic voting and for it to become the third ordinary voting channel. In this sense, the Swiss Federal Council published its third report in 2013, underlining the importance of the "security first" principle and proposing "new requirements, including for security, certification and verifiability" (OSCE/ODIHR, 2016: 4).

First, and in order to leave no room for interpretation about the scope of the provisions of the Federal Ordinance on Political Rights, their contents had to be specified (and

[146] In this sense, and even if some minor incidents had been pointed out, it was considered that such incidents in no circumstances called into question the success of the ballots in question, especially since the secrecy of the vote and the accuracy of the result had been guaranteed (Swiss Federal Council, 2013: 4).

[147] Such a proof would be difficult, if not impossible, to provide (Swiss Federal Council, 2013: 36).

[148] According to Beat Kuoni (2015: 200),

> "[i]f the Federal Supreme Court established a procedural problem, it only annuls the election or vote if the irregularities are substantial and it seems possible that. They have influenced the result. The complaint made must relate to a specific irregularity; a mere abstract theoretical risk is not sufficient for the result of a ballot to be declared invalid. Under the regulations relating to electronic voting, if irregularities are proven, it must be possible to measure the number of defective votes or to assess the extent of their effects on the results of the count."

especially those provisions related to personal data protection, the secrecy of the vote and the accuracy of the results) (Swiss Federal Council, 2013a: 6). In the opinion of the Swiss Federal Council, the definition of more specific requirements would bring two kinds of benefits: on the one hand, it would make it compulsory for remote electronic voting systems to comply with high security standards. On the other hand, it would ease the control of the security properties claimed by the systems. In turn, such controls would also have to become more professional and independent.

In this sense, it was considered necessary to amend the Ordinance and to adopt a specific regulation on the technological aspects, so the legal bases of electronic voting would describe more precisely the common basis of the requirements imposed on all systems. Standardisation work was carried out at three levels: (1) on requirements for federal votes and elections and for printing electronic voter cards, by the Federal Chancellery in collaboration with the federal working group on remote electronic voting; (2) on the systems, such as the standardisation of documents and internal procedures; and (3) by eCH, an association that promotes, develops and adopts standards in the field of e-government for efficient electronic collaboration between authorities, companies and individuals (Swiss Federal Council, 2013a: 35). Additionally, the Swiss Federal Council also considered other technical standards that related directly or indirectly to remote electronic voting, such as those of the Federal Statistical Office on record-keeping, of the Federal Department of Foreign Affairs' on the register of Swiss Abroad, or the work of the Federal Office of Justice on a future eID or SuisseID (Swiss Federal Council, 2013a: 35).

Another advantage of having this additional layer would be that it could be possible to lighten and refine the content of the regulation (Act an Ordinance) and that it would become easier to proceed with the frequent changes in line with technological developments[149] (Swiss Federal Council, 2013a: 125). Accordingly, the Federal Chancellery[150] adopted in 2013 a specific Ordinance for Electronic Voting (VEleS), which contained the security requirements for remote electronic voting. VEleS translated the principles anchored in the Ordinance on Political Rights into technical requirements for the systems and their operation. The new ordinance included "provisions in respect of voting and tabulation procedures, voter education, responsibilities for electoral administration staff, security and risk management, certification and requirements for verifiability, audit and testing" (OSCE/ODIHR, 2016: 5). Overall, VEleS put the accent on verifiability and the different verification mechanisms (i.e., the audits) (Swiss Federal Chancellery, 2013: 3)

Moreover, it was considered that the existing requirements were sufficient as long as there were limits in the number of voters who could vote electronically (i.e., 30% of the cantonal electorate). In order to increase those limits, it would be necessary to adopt new security requirements beyond the so-called first-generation remote electronic voting systems. Which would be the new security requirements for these second-generation

[149] As argued by the Swiss Federal Council, « [l]e vote électronique est un projet techniquement très complexe. Il fait appel à des technologies en constante évolution et nécessite à cet égard un règlement strict, pour lequel le niveau normatif de l'ODP ne convient pas » (2013a: 124). As a matter of fact, the Swiss Federal Council pointed out, there is nothing exceptional about regulating technical aspects in an executive regulation and it is common in other areas, such as those depending on the Federal Office of Communication (Swiss Federal Council, 2013a: 125). As a matter of fact, the OSCE/ODIHR election observation mission actually recommended the drafting of such a document (2012: 16).

[150] Since the Swiss Federal Chancellery was the body responsible for the project, it was trusted with the drafting and the update of VEleS (Swiss Federal Council, 2013: 125).

Internet voting systems? From this point on, complete verifiability and the certification of remote electronic voting systems would become the bedrocks for internet voting adoption in the country (Swiss expert group, 2018: 6). On the one hand, these requirements would focus on the verifiability properties of online voting systems (Swiss Federal Council, 2013a: 11). Such properties would allow for identifying any malfunctions in the conduct of the ballots, of any sort (i.e., software or human errors, as well as tampering attempts), while observing the requirements of secret suffrage (Swiss Federal Council, 2013a: 107).

Along these lines, the Swiss Federal Chancellery entrusted the Berne University of Applied Sciences with an analysis of the feasibility of developing a verifiable remote electronic voting system. Verifiability would also contribute to help reduce the trust assumptions for both the client-side and the server-side components of remote electronic voting systems. For the former, individual verifiability (cast-as-intended and recorded-as-cast) would suffice. For the latter, in addition to universal verifiability (counted-as-recorded) it would be necessary to split the tasks conducted by the servers between different control components[151] (Puiggalí and Rodríguez-Pérez, 2018: 89). In the annexes of the 2013 report by the Federal Council, a proposal for the implementation of these security requirements was described (Swiss Federal Council, 2013c: 2). Additionally, the role of the verifier was introduced, and they were trusted to recalculate the proofs generated by the control components to ascertain the integrity of the process.

On the other hand, it was also considered necessary to review the authorisation process to lower the administrative burden and to make it more efficient, and to professionalise the certification of the internet voting systems. In the opinion of the Swiss Federal Council, the number and complexity of the cooperation venues between the cantons, together with the frequency and complexity of the ballots, required a simplification of the procedures[152]. It would be now the responsibility of the Federal Chancellery to verify that the cantons (still) met the requirements (Swiss Federal Council, 2013a: 12). Thus, a new two-step procedure was envisaged in which the Swiss Federal Council would grant an authorisation and the Swiss Federal Chancellery would observe whether the cantons complied with the federal requirements (Swiss expert group, 2018: 15). Additionally, and taking into account the definition of the new security requirements, it would be of paramount importance to develop new mechanisms for their control. This task, which to date had been conducted by the Swiss Federal Chancellery, would be now the responsibility of external specialised services accredited by the Confederation[153]. While it would be up to the Chancellery to

[151] The control components would have the following characteristics: (1) they would contain a share of the private key; (2) they would be involved in the generation of the control code for individual verifiability printed in the voting cards; (3) they would be involved in the mixing of the ballot box; (4) they would be involved in the decryption of the votes; and (5) they would generate cryptographic proofs.

[152] At the time, the Federal Council could grant a general authorisation only as long as the canton had proven that it had conducted a series of successful ballots using online voting. Two main changes would be introduced: (1) the possibility for the Federal Council to grant general authorisations; and (2) the adoption of a new agreement process by the Federal Chancellery.

[153] As we have explained elsewhere (Puiggalí and Rodríguez-Pérez, 2018: 83),

> "Beyond the participation of the applicant canton, the Federal Council, the Federal Chancellery, and several agents are involved in the licensing and authorisation processes. On the one side, the regulation requires an independent, external agency to (a) confirm that the Federal Chancellery's security standards are met; and (b) to review whether the safety precautions and the electronic vote casting system complies with the state of the art (Art. 27l.1 OPR). This independent external agency has taken the shape, on many occasion, of what has been called as *groupes*

agree on whether the requirements had been met, this decision would be based on the analysis and reports by external services[154] (in whose preparation the Chancellery would not be directly involved).

Building on a step-by-step approach, it was suggested to set up different caps based on the systems' degree of advancement. Thus, Switzerland would shift towards a new paradigm where not all cantons would have necessarily the same limit in the number of Swiss residents eligible to vote online (Swiss Federal Council, 2013a: 9). More specifically, three different caps were envisaged[155]:

- The cap at 30% of the cantonal electorate (and 10% of the Swiss federal electorate) would be maintained for the cantons using the already existing systems.
- A second cap at 50% of the cantonal electorate (and 30% of the federal one[156]) would be envisaged for partial implementations of second-generation remote electronic voting systems, namely: those providing individual verifiability.
- Only when integral second-generation (i.e., with complete verifiability) were used, such cap would be set at the 100% of the cantonal electorate. At this level there would be no limit on the number of Swiss eligible voters being able to vote online at the federal level.

The new legal framework entered into force in January 2014. According to Jordi Puiggalí and Adrià Rodríguez-Pérez, the framework became "the first regulation for online voting systems that included advanced security requirements such as verifiability and

> *d'accompagnement* (which could translate from French as steering, support or advisory groups). In practice, *groupes d'accompagnement* are made up by representatives from four different cantons using a different voting system […] In case that the licence concerns more than the 30% of the cantonal electorate limit (i.e. up to 50% or the whole cantonal electorate), more specific examinations are set (Annex 5 to the VEleS). In this second scenario, the participation of specialized institutions is required, including the participation of institutions accredited by the Swiss Accreditation Service (SAS) or certification agencies, among others. These specialized institutions (i.e. certification laboratories), should first pass an accreditation process through the Swiss Chancellery to get the seal of certification authorities of the VEleS regulation."

[154] To that end, the Swiss Federal Chancellery would set up accompanying groups, thrusted to confirm whether those cantons introducing or making substantial changes to their remote electronic voting systems complied with the security requirements and the security measures were up to date. Accompanying groups were generally made up by four representatives of a canton that was using o had used another online voting system than the one being introduced or modified (Swiss expert group, 2018: 19). The advantage of those groups was that in addition to conduct technical verifications, they would also enable their participants to gather experience and information and draw lessons from what other cantons were doing. VEleS also provides that if more than 30% of the cantonal electorate is authorised to vote via the Internet, the system must be certified by an independent institution accredited by the Swiss Accreditation Services and appointed by the canton (OSCE/ODIHR, 2016: 9).

[155] As we have explained elsewhere (Puiggalí and Rodríguez-Pérez, 2018: 83),

> "[t]he amendment of the OPR also established that it should be the Federal Chancellery who stipulates the requirements that an electronic vote casting system and its operation must meet at each level. As a result, the Federal Chancellery published an Ordinance on Electronic Voting (VEleS), specifying the requirements for authorizing electronic voting for each of the new limits."

[156] If in 2013 there were 5.1 million eligible voters in Switzerland, raising the federal cap to 30% would mean that up to 1.5 million voters could be offered the possibility to vote online (Swiss Federal Council, 2013: 10).

mechanisms for certifying them (e.g., cryptographic and formal proofs)"[157] (2018: 83). In the paper we describe the consequences of adopting such framework. While we have also explained the immediate consequences of the new legal framework[158] (Puiggalí and Rodríguez-Pérez, 2018: 91-92), it must be stressed that

> "Neuchâtel and Geneva go7 authorised with the evolution of their previous voting systems. However, because of the increase in security requirements in the new regulation, the voting system of the Consortium lost its previous authorisation since it failed to address the security issues detected by the experts of the Chancellery."

The introduction of individual verifiability in 2015 represented an intermediate step towards the achievement of complete verifiability (Swiss expert group, 2018: 6). Following the adoption of the new legal framework, 14 cantons applied for an authorisation to the Federal Council and all of them tested their systems in the context of federal popular votes on 8 March and 15 June 2015 (most of them for their registered voters abroad, while Geneva and Neuchâtel also conducted pilots for registered voters residing in the cantons) (OSCE/ODIHR, 2016: 6). In 2015 as well, Swiss voters were able to individually verify for the first time that their vote had been cast-as-intended as well as recorded-as-cast[159] in the context of a federal election (OSCE/ODIHR, 2015c: 6). In this occasion, up to 130.000 Swiss voters[160] from four cantons were authorised to enable the remote electronic voting channel (i.e., those using Neuchâtel's and Geneva's systems): Based-Stadt and Luzern for

[157] At the time, and "[u]nlike other countries were [sic] internet voting is being used or has been piloted, Switzerland is the only country that has developed an overarching certification and authorisation framework suitable to evaluate different internet voting systems, both from an operational and technical perspective" (Puiggalí and Rodríguez-Pérez, 2018: 83). As we will see later, France's CNIL has adopted a similar approach in 2019. We argue that this approach is beneficial since it "allows to certify more than one voting system technologies if they achieve the security requirements, so each canton [or electoral administration] can choose which one they prefer based on this certification" (Puiggalí and Rodríguez-Pérez, 2018: 83).

[158] As we have explained (Puiggalí and Rodríguez-Pérez, 2018: 91),

> "[w]hen the new regulation came into force in January 2014, all the pre-existing voting systems were called for certification once again, to allow their use in the 2015 elections. Thus, all cantons using internet voting started the process to be authorised against the basic level (level 1) to keep at least the same status. Geneva and Neuchâtel also took advantage of this opportunity to improve their voting systems and prepared them for achieving higher levels of certification. In parallel, the Federal Chancellery started the accreditation process for external entities required for the certification levels 2 and 3."

[159] In their final report, the OSCE/ODIHR's Election Expert team stated that "further steps of verification such as confirming that a voter [sic] was recorded as cast have not yet been implemented" (2016: 8). Notwithstanding, since return codes are calculated between the server and the voting client, and the voting portal displays a confirmation code, they also provide recorded-as-cast verification (i.e., they allow voters to ascertain that their vote has reached the voting server unmodified). For a detailed explanation how the return codes worked in Neuchâtel, see Galindo, Guasch and Puiggalí (2015).

[160] Out of 5.2 million eligible voters (OSCE/ODIHR, 2015c: 2), that is slightly above the 3% of all eligible voters. Initially, this number was higher, since 13 cantons requested an authorisation to the Federal Council that would have enabled up to 85.000 voters abroad to vote online (i.e., those of Aargau, Basel-Stadt, Fribourg, Geneva, Graubünden, Luzern, Neuchâtel, Schaffhausen, Solothurn, St. Gallen, Thurgau, and Zurich). That would have represented about 11% out of the 746.00 citizens estimated to be living abroad. However, since the "Consortium" system did not receive an authorisation for these elections, 35.000 voters abroad and 95.000 resident voters in the cantons of Geneva and Neuchâtel, were finally eligible to vote online (OSCE/ODIHR, 2016: 3).

voters abroad and Geneva and Neuchâtel for both voters abroad and resident voters[161]. Based on the testing and administration pilots held in March and June, "the nine cantons that used the Consortium system were declined authorisation for security reasons" (OSCE/ODIHR, 2016: 7). Following the decision, members of the Consortium system postponed the development of their system due to cost considerations (OSCE/ODIHR, 2016: 7). Out of the 132,134 voters eligible to vote electronically, 13.370 did so (10%) (OSCE/ODIHR, 2016: 9)

The OSCE/ODIHR deployed a second election observation mission ahead of the federal assembly elections of 18 October, this time in the form of an Election Expert Team. A NAM was conducted between 9 and 11 June[162]. the OSCE/OIDHR deployed an Election Expert Team between 8 to 21 October (OSCE/ODIHR, 2016: 2). The Team concluded that the pilots had been "professionally and impartially administered and enjoyed widespread trust" (OSCE/ODIHR, 2016: 1). Notwithstanding, they also concluded that additional measures could have been taken to enhance the transparency and accountability of the process.

d) Making remote electronic voting an ordinary voting channel? Operation, dematerialisation, and a Public Intrusion Test (since 2016)

On 14 March 2016, the steering committee on electronic voting[163] of the Swiss Federal Chancellery decided that they would adopt a new framework with a view to make internet voting available for everyone (both Swiss voters abroad and those living in Switzerland) (Swiss Federal Chancellery, 2017a: 10). The new framework was meant to replace the e-voting roadmap (Swiss Federal Chancellery, 2017a: 3). On 5 April 2017, the Swiss Federal Council decided to put an end to the pilot phase and to launch a partial revision of the Federal Act on Political Rights to make online voting an ordinary voting channel (Swiss Federal Chancellery, 2017c: 1). Also in April, the Swiss Federal Chancellery and the Swiss Conference of State Chancelleries adopted a Declaration of intent for the introduction of electronic voting (Swiss Federal Chancellery, 2017b). The Confederation and the cantons also agreed that the first use of a remote electronic voting system offering complete verifiability would be subject to a Public Intrusion Test (PIT) (Swiss Federal Chancellery, 2020c: 5). During the PIT everyone would be invited to try to hack those systems claiming complete verifiability (Swiss expert group, 2018: 20).

[161] Therefore, this was also the first federal election in which Swiss resident voters would be eligible to vote online (OSCE/ODIHR, 2015c: 2; 2016: 1).

[162] The NAM noted that the legal update had addressed a number of prior recommendations (OSCE/ODIHR, 2015c: 1). Notwithstanding, they also concluded that "the revised legal framework for Internet voting and its implementation could benefit from a more in-depth assessment, particularly in light of the authorities' stated intention to extend its usage in future federal elections" (OSCE/ODIHR, 2015c: 2).

[163] The steering committee on electronic voting (*Comité de pilotage vote électronique*, in French) was set in the framework of the Swiss Federal Chancellery's e-voting roadmap of 2011. It comprised two policymakers from two pilot cantons, another policymaker from a different canton having introduced internet voting, and two representatives from the Confederation (Swiss Federal Chancellery, 2011: 2).

In August, the Swiss Federal Chancellor set up an expert group[164] and entrusted them with the examination of the questions related to the adoption of internet voting as an ordinary voting channel, including the amendment of the Federal Act and the Federal Ordinance on political rights[165]. The expert group concluded that the country had gathered enough know-how and achieved the necessary operational conditions to fully adopt internet voting as an additional ordinary voting channel (Swiss expert group, 2018: 4).

In practice, making remote electronic voting the third ordinary voting channel in Switzerland meant that each and every voter[166] (and not only voters abroad, voters with disabilities and a percentage of resident voters) would be able to choose whether to vote in polling stations, by post or online (Swiss expert group, 2018: 4). In the opinion of the Swiss expert group on electronic voting, the knowledge and the procedural prerequisites to establish online voting as a third ordinary voting channel were present (OSCE/ODIHR, 2019c: 8) and no additional security requirements would be required. In this sense, verifiability (i.e., the traceability of the vote and the establishment of the results, in compliance with secret suffrage), accessibility, and transparency would remain the fundamental characteristics of remote electronic voting. Therefore they should be detailed in the Federal Act of Political Rights. More specifically, the expert group suggested the following amendments:

- The important aspects of remote electronic voting (i.e., verifiability and traceability, accessibility, certification, authorisation, and transparency) would have to be regulated at the level of the Act.
- To remove the cap on the percentage of resident voters eligible to vote online, remote electronic voting systems with complete verifiability would have to become available.
- The administrative requirements would have to be reviewed and simplified, and the authorisation process by the Confederation would have to be reduced to one single stage.

By 2018, 10 cantons were conducting pilots with remote electronic voting, out of which five offered it both to Swiss voters abroad as well as to resident voters: Fribourg, Basel-Stadt, St. Gallen, Neuchâtel, and Geneva (Swiss expert group, 2018: 6). The other five cantons (Bern, Lucerne, Aargau, Thurgau, and Vaud) only allowed Swiss voters abroad to

[164] The group was made up by 13 representatives: three from the Confederation (not including the Swiss Federal Chancellery), five from the cantons, four from academia, and a representative from Swiss Post (as the provider of an internet voting system) (Swiss Federal Chancellery, 2017c: 1). The group met in five occasions between the months of August of 2017 and March of 2018 and published its final report in April 2018.

[165] More specifically, the group was asked to address the following subjects: the legal principles regulating internet voting (such as transparency, verifiability, and certification); implement provisions and technical standards (normative level and density); the future of the authorisation process; and monitoring functions of the Swiss Federal Council and the Swiss Federal Chancellery (Swiss Federal Chancellery, 2017c: 2). The group was also asked to provide a framework the dematerialisation of the vote. By dematerialisation it is understood the abandonment (in part or in full) of the sending of printed voting materials (e.g., information materials, voter card, etc.) by post.

[166] In those cantons where remote electronic voting had been adopted. While it was envisaged to offer remote electronic voting as the third ordinary voting channel, cantons would still retain the decision on both whether and when they would introduce this technology (Swiss expert group, 2018: 4).

vote online (Swiss Federal Chancellery, 2018c: 3; Swiss Federal Chancellery, 2019c: 3). In May 2018, the Swiss Federal Chancellery took an additional step towards transparency and, with the amendment of VEleS, mandated the publication of the source code for those solutions claiming complete verifiability (2018a). In November, the Chancellery of Geneva decided that it would not continue the development of their system and that it would no longer offer it from 2020 onwards (Swiss Federal Chancellery, 2018c: 3).

Later that year, the Swiss Federal Chancellery published a draft proposal to amend the Federal Act on Political Rights. The draft proposed amending art. 5 of the Federal Act on Political Rights to regulate the option to vote electronically (at the same level than voting in polling stations and by post) (Swiss Federal Chancellery, 2018b: 1). Additionally, new provisions requiring individual verifiability (Art. 8b 1) as well as universal verifiability (Art. 8b 2), which should be compliant with the principle of secret suffrage, were also drafted. The draft proposal also enshrined the publication of the source code (Art. 8c). A consultation process with the cantons, political parties and other interested stakeholders was then launched, encouraging a political debate on electronic voting at the federal level (Swiss Federal Chancellery, 2018c: 6). The consultation process was open between 19 December 2018 and 30 April 2019[167] (Swiss Federal Chancellery, 2019c: 3).

In parallel, Swiss Post decided to certify their online voting system for its use by 100% of the electorate. In February 2019, the source code of Swiss Post's system was published and between 25 February and 24 March it was subject to a PIT (Swiss Federal Chancellery, 2019c: 3). A total of 3.200 people from 137 countries took part in the PIT (Swiss Federal Chancellery, 2019d: 7) and although "16 violations [sic] were identified" (OSCE/ODIHR, 2019c: 8), the PIT did not allow for identifying any intrusion in the infrastructure nor any manipulation of the votes, neither any breaches of the secrecy of the vote (Swiss Federal Chancellery, 2020c: 5). During the publication of the source code, "two serious issues were discovered that affect[ed] universal verifiability, […] while no irregularities were observed with the integrity of the casting and counting of votes" (OSCE/ODIHR, 2019c: 8). A third flaw was found that affected individual verifiability of Swiss Post's system already being use and on 19 May this system was not approved to be used in federal referendums (Swiss Federal Chancellery, 2019c: 4). The Federal Chancellery thus mandated additional analysis on the system[168] (Swiss Federal Chancellery, 2020c: 5).

[167] On 18 June, the Swiss Federal Chancellery published the results on their consultation on amending the Federal Act on Political Rights. The report showed that most of the cantons supported the partial revision of the Federal Act on Political Rights, some of them even after the flaws in Swiss Post's voting system (Swiss Federal Chancellery, 2019c: 6). Aargau, Appenzell Innerrhoden, Appenzell Ausserrhoden, Berne, Basel-Landschaft, Basel-Stadt, Fribourg, Glarus, Grisons, Jura, Lucerne, Neuchâtel, Obwalden, Schaffhausen, Thurgau, Ticino, Uri, Zug, and Zürich supported the Swiss Federal Chancellery's project (Swiss Federal Chancellery, 2019c: 5). Basel-Stadt, Glarus, Grisons, Neuchâtel, St. Gallen, Schaffhausen, Ticino, and Zürich did so even after the flaws were found (Swiss Federal Chancellery, 2019c: 6). Four cantons supported internet voting, but not the project, and three neither supported the project nor online voting (Swiss Federal Chancellery, 2019c: 5). Interestingly, none of the 10 political parties that answered the questionnaire supported the project, while seven still supported the use of online voting (Swiss Federal Chancellery, 2019c: 5).

[168] According to the Swiss Federal Chancellery (2020c: 5),

> "Plusieurs membres du groupe Vote électronique de la Haute école spécialisée bernoise (BFH) ont étudié la mise en oeuvre du protocole cryptographique dans la spécification du système et dans le code source, et les chercheurs Olivier Pereira (Université de Louvain) und Vanessa Teague (Université de Melbourne) ont examiné la mise en œuvre du protocole sur la base de la spécification du système. L'entreprise Oneconsult a par ailleurs contrôlé la mise en œuvre des mesures de sécurité techniques et organisationnelles en se fondant sur les évaluations des risques des cantons."

Shortly after, on 19 June, the canton of Geneva decided to advance the withdrawal of its internet voting system, since the Federal Council would not decide on whether to approve the cantons' use of internet voting until August and they argued that it would adversely impact their ability to prepare effectively (OSCE/ODIHR, 2019c: 7). More important, on 26 June the Federal Council, "taking into account recent developments with the Swiss Post and Geneva systems, decided to delay introducing internet voting as a regular voting channel and to amend the general conditions for future pilots" (OSCE/ODIHR, 2019c: 8). On 5 July, Swiss Post decided to no longer continue offering their internet voting system (which had been certified for its use by 50% of the cantonal electorate) for the 2019 Federal Assembly elections and "to continue working exclusively on its new system with universal verifiability, with a plan to make it available to the cantons from 2020" (OSCE/ODIHR, 2019c: 8).

In the meantime, the OSCE/ODIHR had conducted a NAM ahead of the federal assembly elections of 20 October. The Mission took place between 21 to 23 May, when only the Chancellery of Geneva had decided to withdraw their internet voting system. However, the final report was issued by July 5, when it was known that internet voting would not be offered in the 2019 federal assembly elections. Initially, it was expected that up to 286,000 citizens from nine cantons would be eligible to vote via the internet in the 2019 elections[169] (OSCE/ODIHR, 2019c: 7), but by the time the mission took place that number had been reduced to 51.000 voters in four cantons[170]. The Mission concluded that "some of the [legislative changes since the 2015 Federal Assembly elections] address[ed] prior ODIHR recommendations, including those related to the transparency of New Voting Technologies" (OSCE/ODIHR, 2019c: 4). These included "transparency requirements for publishing the source code, increased voter information, and allowing voters to familiarize with and to test internet voting outside of an election" (OSCE/ODIHR, 2019c: 7).

In follow-up to these events, the Swiss Federal Council's mandate of 26 June 2019 entrusted the Swiss Federal Chancellery with the restructuring of the trial phase[171] (Swiss Federal Chancellery, 2020c: 7). Under this mandate, the Swiss Federal Chancellery conducted an expert dialogue in collaboration with various cantons (Swiss Federal Chancellery, 2020a: 1). In the framework of this dialogue, the Swiss Federal Chancellery "discussed various issues concerning internet voting with 23 experts from the academic research community and the industrial sector" (Swiss Federal Chancellery, 2020a: 1). The dialogue last between February and July 2020[172]. Most of the issues discussed during the expert dialogue revolved around security standards and risk management, standardisation

[169] Including 86.000 voters abroad from the cantons of Aargau, Bern, Basel-Stadt, Fribourg, Geneva, Luzern, Neuchâtel, St. Gallen, and Thurgau, as well as 120.000 resident voters in the cantons of Basel-Stadt, Fribourg, Geneva, Neuchâtel, and St. Gallen (OSCE/ODIHR, 2019c: 7).

[170] Some 19.000 voters abroad and 21.500 resident voters in Basel-Stadt, Fribourg, Neuchâtel and Thurgau (OSCE/ODIHR, 2019c: 8). The canton of St. Gallen had announced that it would not apply to use internet voting on 19 June (OSCE/ODIHR, 2019c: 7).

[171] The restructuring is aimed at achieving the following goals: (1) pursue the development of the systems; (2) effective monitoring and control; (3) enhancing of transparency and trust; and (4) strengthening the links with the scientific community (Swiss Federal Chancellery, 2020c: 7).

[172] It was split into two phases: first, based on a questionnaire that was sent out on 14 February 2020. Second, and based on the answers to this questionnaire, the Swiss Federal Chancellery conducted a moderated discussion in writing from 5 May to 17 July (Swiss Federal Chancellery, 2020a: 1).

of cryptographic blocks, transparency, and publication of the source code (including disclosures of vulnerabilities), certification and independent examination by cryptographers, public scrutiny, as well as verifiability. For the experts, the dialogue marked a milestone. And while they identified several areas in which improvements were possible (such as security, verifiability, transparency and scrutiny[173]), they concluded that "there is no need to abandon all future plans with internet voting" (Swiss Federal Chancellery, 2020b: 73).

Based in the dialogue, the Swiss steering committee on electronic voting adopted, a report with a catalogue of measures to restructure and resume the internet voting pilots on 30 November 2020 (Swiss Federal Chancellery, 2020b: 73). The report suggested the implementation of a first set of improvement with a view to resume the pilots in the short term, as well as a series of goals for the mid and long term (Swiss Federal Chancellery, 2020b: 37). Among the former, they included: guaranteeing the efficacy of the audits, come up with a procedure for the processing of non-conformities, and a limitation of the electorate eligible to vote online at 30% of the cantonal electorate and 10% of the Swiss one, to name just a few examples.

The Swiss Federal Chancellery has come up with a series of amendments for both the Ordinance on Political Rights and on Remote Electronic Voting. However, at the time of writing neither have the pilots resumed nor there is a clear calendar of when it will happen.

2. France

Internet voting[174] in France dates back to 2003, when the first law was passed allowing the use of remote electronic voting for the elections to the High Council of French Citizens Abroad[175] (Anziani and Lefèvre[176], 2014: 38; Rambaud, 2019: 38). Subsequently, the

[173] While the conclusions of the report also speak about "privacy" (Swiss Federal Chancellery, 2020b: 73), after a thorough analysis of the report we have only identified some concerns related to long-term privacy which, within the wider discussions, only occupy a residual space.

[174] In addition to internet voting, French legislation also foresees the use of voting machines since 1969, which are used in some municipalities (*communes*). Because of important criticism about the functioning of these voting machines during the 2007 presidential elections, the government imposed a *moratorium* on the number of municipalities that could use this technology and limited them to the municipalities where they were already being used (Anziani and Lefèvre, 2014: 11). Additional alternative voting channels for voters in France and in overseas communities and departments include voting by proxy (OSCE/ODIHR, 2012c: 4). The option to vote by post was reintroduced, at experimental level, for prisoners during the 2019 elections to the parliament of the EU (Rambaud, 2019: 38).

[175] The High Council of French Citizens Abroad (*Conseil supérieur des Français de l'étranger*) became the Assembly of French Citizens Abroad (*Assemblée des Français de l'étranger*) in 2004 (Anziani and Lefèvre, 2014: 37). This is a representative instance specific to French citizens abroad, created under the mandate of art. 24 of the French Constitution.

[176] Alain Anziani and Antoine Lefèvre are two Senators who authored a report on the use of (remote) electronic in France in 2014. Similar reports have been authored by Senators Jacky Deromedi and Yves Détraigne in 2018 and by Jacky Deromedi, Christophe-André Frassa, and Jean-Yves Leconte in 2020. Also in 2020, François-Noël Buffet presented an interesting report on remote voting at the Senate. In turn, we also resort to a report prepared by Marie-Christine Haritcalde for the Assembly of French citizens abroad in 2020.

French Ministry of Foreign Affairs[177] carried out three pilot projects during the 2003, 2006 and 2009 elections[178] (OSCE/ODIHR, 2012c: 9). Nowadays, remote electronic voting is foreseen as an additional voting channel for French voters abroad[179]. They can cast a remote electronic vote for the elections to the National Assembly (the directly elected lower house of the French parliament, with 577 seats) and for the election of the advisers of French abroad and consular delegates[180].

For the elections to the National Assembly, a constitutional amendment of 2008 introduced 11 seats to be elected by voters residing abroad (OSCE/ODIHR, 2012b: 3; Rambaud, 2019: 38[181]). In 2012, voters had the possibility to vote online for these seats (Anziani and Lefèvre, 2014: 37) for the first time[182] (OSCE/ODIHR, 2012b: 1). However, in 2017 this possibility was halted due to concerns of foreign cyber threats as well as over certain technical issues (OSCE/ODIHR, 2017: 6; Deromedi and Détraigne, 2018: 35-36). On their side, advisers of French abroad and consular delegates are based at each embassy with a consular district and at each consular post. They are elected for a six-year mandate during the month of May, their first elections taking place in 2014 (Anziani and Lefèvre, 2014: 37). The next elections were scheduled for May 2020. Yet, the French Ministry of Foreign Affairs decided to postpone these elections due the Covid-19 pandemic and were finally held in 2021[183].

France is a semi-presidential republic with a parliament comprising two chambers: a directly elected lower House, the National Assembly, and an upper house, the Senate, composed of 348 indirectly elected senators (OSCE/ODIHR, 2012b: 2). Elections are regulated by the 1958 Constitution[184], the Electoral Code, other laws and regulations, as well as well as information materials issued by the different administrations. According to

[177] Throughout the period analysed here, the official name of the French Ministry of Foreign Affairs has changed on several occasions. For example, it is currently called Ministry for Europe and Foreign Affairs (*ministère de l'Europe et des Affaires étrangères*, MEAE) but it was called Ministry for Foreign Affairs and International Development (*ministère des Affaires étrangères et du Développement international*, MAEDI) between 2012 and 2017 and Ministry for Foreign and European Affairs (*ministère des Affaires étrangères et européennes*, MAEE) between 2007 and 2012. For this reason, we will simply refer to this institution as Ministry of Foreign Affairs.

[178] In addition to these three elections, different by-elections were held in 2010. It is also important to note that for the 2011 to the Assembly of French Citizens Abroad internet voting was not used (Barrat, 2015: 146), even if the new institutional framework for the representation of French citizens abroad were not set up until 2013

[179] French voters abroad can also cast their votes in-person at embassies and consulates, vote by post (for elections to the National Assembly only) or appoint a proxy to vote on their behalf.

[180] Voting online is not an option for the elections to the President of the Republic, for the elections to the European Parliament, and for referendums (Anziani and Lefèvre, 2014: 40).

[181] According to Romain Rambaud, this amendment introduced the representation of French citizens abroad at the National Assembly, given that until that moment they were only represented at the Senate (2019: 212).

[182] By-elections were held as well in 2013.

[183] Scytl –where the author works since 2015– has been the technology provider for these elections since 2012. It signed their last contract with the French Ministry of Foreign Affairs for a four-year period in May 2016 (Deromedi and Détraigne, 2018: 38) which was extended until 2021 due to the postponed Consular elections.

[184] Electoral aspects regulated already in the Constitution include the exercise of sovereignty and the characteristics of the suffrage (art. 3), the rules for presidential elections (art. 6 and 7), the rules for parliamentary elections (art. 24 and 25), the natura of the mandates (art. 27), the role of the Constitutional Council in resolving electoral disputes (art. 60) as well as the rules for elections in certain territorial communities (art. 72) (Rambaud, 2019: 40).

Romain Rambaud (2019: 157), these include different guides and *mémentos* that have become essential tools for understanding and implementing electoral law. Lastly, and as in the previous cases, one has to take into account as well the case-law and the actual practices, which may draw and specific interpretations or even deviate from the letter of the law[185] (Rambaud, 2019: 157).

On remote electronic voting, the Electoral Code regulates the functioning of the electoral commission for electronic means (in French, *bureau de vote électronique*), the period for internet voting, and voter authentication (OSCE/ODIHR, 2012c: 10). However, while the Electoral Code establishes the main features of the procedure, there are other subordinate legal documents that also have great importance (Barrat, 2015: 131). Secondary legislation includes regulations, decrees, court decisions and deliberations, and instructions on different aspects of the electoral process (OSCE/ODIHR, 2017: 4). More specifically, sources at this level include the *circularies* on electoral operations of the electoral department at the Ministry of the Interior, sometimes issued jointly with other Ministries, as well as the *mémentos du candidat*[186] prepared for the election candidates and that detail the dates of the election, rules for the candidates, the voting operations, etc. (Rambaud, 2019: 167-168). Additionally, internet voting has to meet the conditions laid out both by the *Commission nationale de l'informatique et des libertés* (CNIL), as a consultative body (Barrat, 2015: 131).

Elections are administered by a range of executive and judicial institutions that are mandated to deal with electoral matters (OSCE/ODIHR, 2012b: 3). The Ministry of the Interior is responsible for the technical and logistical administration of the elections[187] (OSCE/ODIHR, 2012b: 4). It issues operational instructions on legal and organisational matters to the state's representatives in the departments and the regions, the prefectures (in French, *préfectures*), which are responsible for candidate registration, the tabulation of results and their transmission (OSCE/ODIHR, 2012c: 5). However, it is the Ministry of Foreign Affairs who organises the voting for voters registered abroad (OSCE/ODIHR, 2012b: 4) and thus remote electronic voting. Consulates are tasked to inform French citizens registered abroad about the voting procedures, the candidates, and location of the polling stations (OSCE/ODIHR, 2012c: 6). The responsibility for general oversight of the election is vested with the Constitutional Council[188] (OSCE/ODIHR, 2017: 2; Rambaud, 2019: 41).

[185] For example, when it comes to paper-based voting in polling stations, Romain Rambaud mentions Cauchois and Savignac (2017: 121) who identify certain deviations in the actual practice of voting. For example, the authors stress that in certain villages and towns voters are handed an envelope when they enter the polling station, when in the Electoral Code it is states that electors take the envelope themselves since otherwise it could breach the secrecy of the vote.

[186] While these may not seem a legal source at first, Romain Rambaud (2019: 169) notes that the Council of State has not hesitated to accept appeals against the *mémentos*, often because they add to the legal sources by containing mandatory provisions.

[187] For presidential elections, this responsibility is shared with the Constitutional Court. However, we have already mentioned that remote electronic voting is not offered for presidential elections (see footnote 180 above).

[188] The Constitutional Council is composed of nine members who serve for non-renewable nine-year terms. During elections, the Council reviews, advises on, and validates election-related legislation, and adjudicates election-related complaints and appeals (OSCE/ODIHR). While in presidential elections the Council is responsible for registering presidential candidates and announce final presidential election results, it has less responsibility in parliamentary elections. For legislative

Furthermore, and since internet voting requires the set-up of a register with the citizens enrolled on consular lists (Anziani and Lefèvre, 2014: 43; Deromedi and Détraigne, 2018: 29), this technology is under the legal supervision of the *Commission Nationale de l'Informatique et des Libertés* (CNIL). The CNIL first adopted a Recommendation on the security of e-voting systems in 2003 and then updated it in 2010[189] (CNIL, 2010). The Recommendation provides general guidelines regarding minimal privacy, secrecy, and security requirements for any internet voting (OSCE/ODIHR, 2012c: 12). In the Recommendation, the CNIL prescribed both physical measures (such as access controls to the servers or rules for the clearance of authorized employees), as well as software-related ones (i.e., firewalls) (Anziani and Lefèvre, 2014: 37). The CNIL has further updated their Recommendation on 2019 to take stock of the new requirements introduced by the EU's General Data Protection Regulation (GDPR) after it entered into force (CNIL, 2019c). The goal of the update was to apply to future developments in internet voting, with a view to better respect the principles of personal data protection, and to inform data controllers on their choice for an online voting system (CNIL, 2019a). Furthermore, the *Agence nationale de la sécurité des systèmes d'information* (ANSSI) has established a General Security regulatory Framework (RGS) to regulate minimal requirements on electronic certificates, encryption levels, and authentication mechanisms (OSCE/ODIHR, 2012c: 12).

Historically, it is possible to distinguish three main phases in the deployment of remote electronic voting in France:

a) Introducing remote electronic voting: pilot phase (2003-2009)

Remote electronic voting in France was introduced as a mean to tackle some of the obstacles faced by French voters abroad (i.e., dispersion all over the world, distancing from polling stations within one country, reluctance if not direct opposition by some states to the organisation of French elections in their territory, etc.)[190]. In the early 2000, the option offered to these voters to cast their vote by post steadily became an electronic alternative *(*Anziani and Lefèvre, 2014: 37). Taking into account the different circumstances of those voters located in the national territory and those abroad, the legislators considered necessary to adopt additional voting channels for voters abroad[191] (Anziani and Lefèvre, 2014: 52). In this context, the legislator noted that the network of polling station abroad

elections, art. 59 of the French Constitution entrusts the Constitutional Council to rule on the proper conduct of the election in disputed cases (Rambaud, 2019: 124). Since internet voting cannot be used in presidential elections, our focus in the following pages will be on the latter role.

[189] In addition to the Recommendation, the CNIL also issued an assessment of the remote electronic voting system used in the 2006 elections (CNIL, 2006).

[190] These limitations justify, in the opinion of Anziani and Lefèvre (2014: 37), certain derogations from the general rules of electoral law, including an increased number of proxy voting, the organisation of elections in a different day in the American continent, the maintenance of postal voting for French abroad (suppressed in France for political elections in 1975) as well as enabling the remote electronic voting channel for this group. For the authors, it is the need to address the challenges of electoral participation by voters abroad that justified the introduction of remote electronic voting in French law (Anziani and Lefèvre, 2014: 10). Régis Dandoy and Tudi Kernalegenn also agree that "Internet voting is meant to make the voting process easier for citizens, [and] in turn, it presents an opportunity to increase participation (2021: 1-2).

[191] This is the same reason why postal voting was kept as an option for voters abroad when it was suppressed in France following the electoral reform of 1975 (Rambaud, 2019: 38). For an overview of the vulnerabilities of postal voting in France between 1946 and 1976, an excellent summary is offered in the Senate report submitted by François-Noël Buffet (2020: 22).

did not satisfy the requirements set for mainland France, and that voting for French citizens abroad also carried additional financial cost. In some circumstances, Alain Anziani and Antoine Lefèvre note (2014: 52), material or geopolitical circumstances made it directly impossible for French citizens abroad to exercise their voting rights. In view of this constraints, it would be claimed that internet voting for French voters abroad constitutes a "democratic imperative" (Deromedi and Détraigne, 2018: 8).

According to Alain Anziani and Antoine Lefèvre (2014: 37), from the fact that art. 3 of the Constitution recognises the right to vote to all French nationals followed that it was necessary to organise voting channels compatible with the situation faced by French citizens abroad. The French parliament adopted in 2003 the law num. 2003-277, of 28 March, authorising remote electronic voting for French citizens established abroad for the elections to the Assembly of French Citizens Abroad[192]. The Assembly of French Citizens Abroad, until 2004 known as High Council of French Citizens Abroad[193], is the French government's interlocutor on the situation of French people living abroad and the policies conducted in their regard. The government consults the Assembly, which meets twice per year in Paris, on all consular affairs and matters of general interest. Each year the government submits a report on the situation of French citizens abroad to the National Assembly (Deromedi and Détraigne, 2018: 73).

At that time, the Assembly was composed of 190 members, 155 of them directly elected by French citizens abroad, 11 members by the National Assembly, 12 senators and 12 qualified individuals[194]. By allowing voters abroad to vote online, it was expected that their turnout, which overall tended to be lower than the national average, would increase (Anziani and Lefèvre, 2014: 43). At the time, remote electronic was considered an experimental voting channel (Anziani and Lefèvre*,* 2014: 38). From the outset, internet voting has been considered a remote and advanced voting channel, something that, according to Alain Anziani and Antoine Lefèvre, had no equivalent in French electoral law (2014: 38) and supposed thus a limited derogation from the legal framework (Anziani and Lefèvre, 2014: 38). In practice, however, postal voting was already being offered to French citizens abroad (Rambaud, 2019: 229) and therefore remote electronic voting was not the only derogation to the standard of voting in polling station that existed for voters in mainland France.

The voting period started the second Wednesday preceding election day, at 12h00 pm in Paris, and ended the Tuesday preceding election day at the same time (Anziani and Lefèvre*,* 2014: 39). The system worked as follows: voters identified themselves against the platform using a pair of credentials (i.e., username and password) that they had received from their consular administration (Anziani and Lefèvre*,* 2014: 39). A voter could cast a vote for a candidate or an explicit blank vote, but not an invalid one (Anziani and Lefèvre*,* 2014: 39). Not being the only voting channel available for voters abroad, conducting remote electronic voting in advance prevented a voter from casting multiple

[192] In French, Loi n° 2003-277 du 28 mars 2003 tendant à autoriser le vote par correspondance électronique des Français établis hors de France pour les élections de l'Assemblée des Français de l'étranger.

[193] The change in the institution came as a result of the adoption of *Loi n° 2004-805 du 9 août 2004 relative au Conseil supérieur des Français a l'étranger.* For the sake of simplicity, throughout these pages we will be referring to this institution as Assembly of French Citizens Abroad.

[194] Since the setup of the institutions for the representation of French citizens abroad in 2013 (see section II.3.b below), the Assembly is made up of 90 Consular Advisers, chosen among their peers (Deromedi and Détraigne, 2018: 73).

votes: before e-day, consular administrators could identify who had already voted online and marked them on the electoral rolls used at the polling stations abroad (i.e., what in French is referred to as *liste d'émargement*[195]).

France implemented remote electronic voting for the first time in the 2003 elections to the Assembly of French citizens abroad, in a pilot project in two electoral districts for the United States of America (Pellegrini, 2006: 4). Notwithstanding, it was only in the 2006 elections that is use was generalised. According to Régis Dandoy and Tudi Kernalegenn, 10,201 voters used this channel in 2006 (2021: 5). Some concerns were raised following the election: "reports by the ADFE (*Association démocratique des Français de l'étranger* - the so-called Pellegrini report) and UFE (*Union des Français de l'Etranger* -the so-called Lang report) both expressed serious doubts about the verifiability, transparency, and sincerity of Internet voting" (Dandoy and Kernalegenn, 2021: 5).

Alain Anziani and Antoine Lefèvre (2014: 46) have summarised three experts' contributions who came up with outspoken criticism regarding the use of internet voting around the idea that this channel failed to meet the two basic requirements of any democratic election, namely: that elections need to be both honest and secret. According to François Pellegrini (2006), one of the experts, internet voting actually failed at achieving any of them. On the one hand, regarding the genuine nature of elections, he claimed that it was not possible to guarantee that the person voting online was the eligible voter and voters could not know whether their ballot actually contained their choices. On the other hand, on secret suffrage, Alain Anziani and Antoine Lefèvre argued that the lack of a formal framework, such as entering the voting booth, did not guarantee the conditions ensuring the non-public nature of the vote (2014: 47). In this context, a voter could cast their vote while being monitored by, and thus under the influence of, a third person. In the opinion of these experts, there had been cases in which people gathered together in order to vote online. This would be specially concerning for those voters who are not used to digital technologies, since they may need to resort to someone else's assistance in order to cast their remote electronic vote (Anziani and Lefèvre, 2014: 47).

In addition to the issues related to the genuine and secret nature of elections[196], Alain Anziani and Antoine Lefèvre also raise the issue of observation of e-enabled elections. Because internet voting incorporates a technical intermediary in the voting process, voters can no longer control by themselves the correct conduct of the electoral operations (Anziani

[195] Jordi Barrat, on the other hand, refers to this process as the registration of voters who have exercised their right to vote (2015: 133).

[196] in line with some of the criticism already analysed in chapter 2, some concerns were also raised regarding the social act of voting. As highlighted by Gilles Toulemonde (in Anziani and Lefèvre, 2014: 47): . In some of the most recent reports and discussions in the French Senate we can find similar claims. For example, François Bonhomme argued that the act of voting is sacred in a democracy (Deromedi at Détraigne, 2018: 57). More specifically, this senator adds that mechanisms such as ballot boxes and principles such as the secret nature of the vote represent immense progress and fears a desacralization of the act of voting because of the introduction of remote electronic voting (Deromedi at Détraigne, 2018: 57). This concerns have been echoed elsewhere. For example, in relation to voting via the Internet, Josep Maria Reniu Vilamala has noted that "the physical gathering of citizens at polling stations is a link that is difficult to abandon in both the process of political socialization and the articulation of an appropriate democratic consciousness (2008: 68). While this is a valid criticism, it is not necessarily related to secret suffrage and thus we will not address them further. Likewise, we have also seen in chapter 2 that this criticism is not unique to remote electronic voting.

and Lefèvre, 2014: 47). The Council of State[197] (*Conseil d'État*) was also called to examine the grievances related to the impossibility encountered by a part of the electorate to vote online in those elections. The Council dismissed this and other concerns. Succinctly, it concluded that it could not be stablished that these grievances could have influenced the results of the election, given that voters had alternative voting channels to cast their vote (by post and in person at polling stations) (Anziani and Lefèvre, 2014: 50).

b) The generalisation of remote electronic voting for French voters abroad and the development of technological standards (2010-2017)

Following the first experiences with remote electronic voting, the institutions representing French citizens abroad were substantially overhauled. A 2008 Constitutional amendment[198] introduced 11 members of the National Assembly[199] to be elected by French voters abroad (OSCE/ODIHR, 2012b: 3). In 2009, remote electronic voting provisions were adopted in art. L. 330-13 of the French Electoral Code for the election of the members of the National Assembly that were elected by French voters abroad (Barrat, 2015: 134).

Following, the law num. 2013-659, of 22 July 2013, on the representation of French citizens abroad[200] set up a new institution representing the interests for French citizens abroad, the Consular Councils, for whose election voters could vote online. Consular Councils are advisory bodies representing French citizens abroad[201]. There is a Consular

[197] The country's legal framework envisages a system for adjudicating electoral disputes, including disputes related to remote electronic voting, that the OSCE/ODIHR (2012b: 7) has deemed complex. Prior to election day, complaints are submitted to the Administrative Court (*Tribunal Administratif*). After the proclamation of the results, any registered voter or candidate standing in that constituency can file a complaint contesting the results of the election, within a 10-day period (OSCE/ODIHR, 2012c: 20). Based on such complaints or appeals challenging the announces results, the Council is empowered to take a decision to invalidate results at individual polling stations and to proclaim a 'rightfully' elected candidates (OSCE/ODIHR, 2012b: 7). On complaints and appeals, see the national framework in *Ordonnance No. 58-1067 of 7 novembre 1958*

[198] The French Constitution is not much detailed regarding the country's legislative elections. For instance, art. 24 only details that only the lower house, the National Assembly, is directly elected. The Constitution also established that the National Assembly shall not have more than 577 members and that those French nationals living abroad shall be represented in both chambers of the Parliament. On the other hand, art. 25 sets that an Institutional Act (in French, *loi organique*) sets the term for which each House is elected, the number of its members, their allowances, the conditions of eligibility and the terms of disqualification and of incompatibility with membership (Rambaud, 2019: 122).

[199] The electoral system of legislative elections dates back to the *Loi nº 86-825, of 11 July 1986, relative à l'élection des députés et autorisant le gouvernement à délimiter par ordonnance les circonscriptions électorales*. According to art. L 123, the 577 members of the National Assembly are elected in single-member constituencies using a two-round system (Rambaud, 2019: 219-220). If no candidate obtains an absolute majority of votes cast by at least a quarter of the registered voters, a second round is held between the candidates who received at least 12.5% of the number of registered voters (OSCE/ODIHR, 2012b: 3). If only one or none of the candidates reaches this quota in the first round, the second round is held between the two leading candidates in the first round.

[200] In French, Loi n° 2013-659 du 22 juillet 2013 relative à la représentation des Français établis hors de France.

[201] Régis Dandoy and Tudi Kernalegenn offered a detailed account of this institution:

> "the consular council if 'responsible for formulating opinions on consular matters or matters of general interest, in particular cultural, educational, economic and social, concerning the French

Council at each embassy that has a consular district assigned and at each consular post. Nowadays, there are 130 Consular Councils. Each consular council is made up of Consular Advisers, chosen by universal direct suffrage during the consular elections (Deromedi and Détraigne, 2018: 73). There are currently 443 Consular Advisers, who are elected for a six-year mandate.

In the meantime, the CNIL updated its recommendation on the security of e-voting systems[202] (CNIL, 2010). Remote electronic voting required the creation of an automatic register of voters registered on the consular electoral lists (Deromedi and Détraigne, 2018: 28), and was thus subject to the control of the Commission. The Recommendation provided general guidelines regarding minimal privacy, secrecy and security requirements for any internet voting (OSCE/ODIHR, 2012c: 12), including both physical measures (such as access controls to the servers or rules for the clearance of authorized employees), as well as software-related ones (i.e., firewalls) (Deromedi and Détraigne, 2018: 29). The recommendation also provided that votes must be encrypted end-to-end to protect their confidentiality throughout the process, and that voters must receive their identification codes by two different channels (such as email and SMS) to confirm their identity[203]. Lastly, updates of these guidelines in 2010 included input from an independent third-party audit company[204], who was engaged following public tender proceedings.

More important, this period includes the first –and, at the time of writing, only[205]– elections to the French National Assembly in which voters abroad could cast a remote electronic vote, namely: those of 2012. The voting period lasted for six days, between the second Friday and the Wednesday before election day (Deromedi and Détraigne, 2018: 28): voters were able to cast their ballots via the internet from 23 to 29 May, for the first round (held in France on 10 June), and from 6 to 12 June for the second round (held in France on 17 June)[206] (OSCE/ODIHR, 2012b: 5).

A specific body was set up to monitor the proper functioning of the remote electronic voting channel and its operations, the *bureau de vote par voie électronique* (Deromedi and Détraigne, 2018: 28). The commission is made up of a judge of the Council of State, who

> [citizens] established in the district' (art. 3). Their most concrete tasks are allocating scholarships to French students throughout the network of French school abroad, providing social assistance to French people in need, supporting the volunteer sector, and attending to security issues (Lequesne, 2020)."

[202] In French, délibération nº 2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique. In 2003 the CNIL had already provided general guidelines regarding minimal privacy, secrecy and security requirements for any internet voting (OSCE/ODIHR, 2012c: 12). Until 2010, however, this entity had basically focused on internal online elections within non-political bodies (Barrat, 2015: 146). The increasing use of internet voting to all types of elections (CNIL, 2010), including the constitutional amendments already mentioned, led to the adoption of an updated recommendation

[203] Something that, in the opinion of (Deromedi and Détraigne, 2018: 30), adds complexity to the process for voting online.

[204] The same company was then also selected as a third-party independent auditor for the 2012 elections (OSCE/ODIHR, 2012c: 12).

[205] With the exception of two partial elections (in the first and eight electoral districts for French voters abroad) held in 2013. These partial elections were held after the Constitutional Court cancelled the results of the 2012 elections because the elected members' campaign finances were rejected and, thus, they had been declared ineligibles (Constitutional Council, 2013: 2).

[206] An interval between internet and in-person voting was intended to make it possible for voters to cast their ballots in person at the diplomatic representations if substantial problems were encountered with internet voting (OSCE/ODIHR, 2012c: 10).

acts as the president of the commission, two representatives from the Ministry of Foreign Affairs, one from the Ministry of the Interior, one representative from the ANSSI[207] and three representatives from the Assembly of French Citizens Abroad. Among others, the *bureau* registers all the operations in a written record and can order the temporary halting of voting operations in case of hacking attempt[208] (in French, *procès-verbal*) (Deromedi and Détraigne, 2018: 28). All operations of internet voting are conducted from Paris (OSCE/ODIHR, 2012b: 4). Prior to the election, the internet voting system's source code was audited by a private company hired by the CNIL and it was tested with the participation of more than 5.000 users.

On 18 May, the cryptographic keys used for encrypting and decrypting the votes were generated and the shares of the decryption key were handed over to the members of the *bureau de vote par voie électronique*. The key generation ceremony was public, with some party delegates (mainly from the Pirate Party) present (OSCE/ODIHR, 2012c: 10). The OSCE/ODIHR (2012c: 10) describes the voting process as follows:

> "Some 210,000 citizens residing abroad fulfilled the criteria for this option by submitted [sic] their e-mail address and mobile phone number to consulates. They then received instructions on how to vote via the internet and the login to use during the first and second rounds by regular mail two weeks before the first round. This enabled voters' authentication during the internet voting. Additionally, each of them received two different passwords via e-mail, one for each round. […] Once a secure connection was established to the voting portal through a browser, a Java-based internet voting application was loaded on the user's computer. The user was able to authenticate him or herself with the login and password provided. The application listed all the candidates in the corresponding constituency. Once the voter cast his/her vote, it could not be changed even if cast by mistake or under pressure […] A 'receipt' with a validation code was displayed on the screen in a printable format, enabling the voter to confirm the correct casting of his/her vote."

Following this election, a legal proposal was presented in 2013 aimed at allowing the use of Internet voting for French voters abroad for the elections to the European Parliament[209]. The draft, however, was not adopted by the competent commission of the Senate (*commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale, sous réserve de la constitution éventuelle d'une commission spéciale dans les conditions prévues par le Règlement*) and was therefore not discussed any further.

In 2014, the first elections to the advisers of French abroad and consular delegates were held. The French Consular elections have been defined by Jacky Deromedi, Christophe-André Frassa and Jean-Yves Leconte as "particularly complex to organize" (2020: 9). 443 Councillors of French citizens abroad and 68 Consular Delegates are chosen by French citizens abroad by universal, secret, and direct suffrage in 130 electoral districts all over

[207] Therefore, in addition to the CNIL, the ANSSI also plays an important role regarding the security of remote electronic voting. Besides having a seat at the *bureau de vote électronique,* the ANSSI also contributed to the development of a security matrix during the procurement of the remote electronic voting system for the period 2016-2020, which details 419 recommendations and requirements (Deromedi and Détraigne, 2018: 34)

[208] However, as we will see later, for the 2017 parliamentary elections it was the Ministry of Foreign Affairs who decided to cancel the use of online voting.

[209] In French, *Proposition de Loi nº 48 (2013-2014) tendant à autoriser le vote par Internet pour les Français établis hors de France pour l'élection des représentants au Parlement européen*.

the world. In 2014, 43,21% of the votes were cast by electronic means (Dandoy and Kernalegenn, 2021: 1).

The assessments of the contests show some dissatisfaction with remote electronic voting. Regarding the legislative elections, the OSCE/ODIHR interlocutors voiced concerns about the security and secrecy of Internet voting and on the limited public debate prior to its introduction (OSCE/ODIHR, 201a: 2). Among others, the OSCE/ODIHR EAM concluded that various aspects of internet voting, including preparation, certification, and audits, lacked detail in the legal framework (OSCE/ODIHR, 2012c: 2). For instance, they argued that key information related to the procurement and audits was not publicly disclosed[210], which negatively affected the transparency of the election and raised some concerns (OSCE/ODIHR, 2012c: 2).

Additionally, two technological issues also arose during the 2012 legislative election (OSCE/ODIHR, 2012c: 11). First, the Java Virtual Machine used for the casting of the vote was updated around the time that the internet voting was available for the first round of the election and made it incompatible with the voting application[211]. This update resulted in several voters being unable to cast their vote. The second issue was observed during the counting off the results for the second round, when a one-vote disparity in one constituency was found. The vote's digital certificate had been corrupted during the casting and thus the solution had not counted it.

Similar issues can be identified for the 2014 elections. According to Régis Dandoy and Tudi Kernalegenn (2021: 5) "[m]any critiques were expressed about Internet voting after the 2014 consular elections". Some of these critiques were related to the authentication system used, which carried several problems linked to the delivery of the SMS abroad on time. The authors add (Dandoy and Kernalegenn, 2021: 5):

> "First, it had been difficult to send logins and passwords to voters since around 25% of registered voters had failed to provide an e-mail address, whereas others in several countries never received the information sent by post and SMS. Second, 6% of Internet voters (i.e., around 4,630 citizens) contacted support services because they encountered connection problems. In addition to these two issues, an uptick in those

[210] For instance, all relevant actions and decisions taken by the electoral commission for electronic means were recorded in minutes, to which voters and proxies gained access only after a lengthy process (OSCE/ODIHR, 2012c: 11). At the same time, the OSCE/ODIHR's report also acknowledges that a Steering Committee comprised of representatives of all parties involved in internet voting implementation was responsible for the risk assessment study of the project before the procurement.

[211] The Senate rapporteurs has offered a detailed account of this issue (Anziani and Lefevre, 2014: 56):

> « Le problème technique lié au logiciel Java lors du scrutin de 2012 L'essentiel des problèmes recensés lors des élections législatives à l'étranger est lié au passage du logiciel Java 1.6 à une nouvelle version 1.7 en mai 2012, soit quelques jours seulement avant le premier tour. Il semblerait que le comité de pilotage n'ait pas considéré ce changement de version comme un problème technique mais plutôt comme une mesure de sécurité. Seuls les ordinateurs munis d'une version du logiciel Java préalablement testée étaient autorisés à voter. Oracle, l'éditeur du logiciel, avait publié une version 1.7 en juillet 2011, qui avait ensuite été retirée en raison de dysfonctionnements. Une nouvelle version 1.6_032 avait été proposée sur le marché et recommandée aux électeurs en lieu et place de la version 1.7. En juin 2012, c'est-à-dire au moment des élections législatives, Oracle a lui-même recommandé la désinstallation de la version 1.7 au profit de la version 1.6 pour certaines de ses suites logicielles. Sur 244 623 votants sur l'ensemble des deux tours, seuls 12 893 électeurs ont tenté de se connecter au site de vote sans toutefois déposer de bulletin dans l'urne électronique, soit un taux d'accès réussi égal à 95 %. »

> connecting within the last few hours before Internet voting ended saturated the voting platform, rendering it inaccessible for about two hours."

Taking these issues into consideration, it should not come as a surprise that internet voting also raised some concerns in this period, if not outward criticism, regarding its compliance with the French constitutional principles. Following the first elections to the National Assembly in which internet voting was an option, the Constitutional Council was called to decide upon the constitutionality of the law[212]. Yet, the Council was not called to pronounce itself on the constitutionality of article I.22, which authorised the remote electronic voting channel for the election to the Consular Councillors (Anziani and Lefèvre*,* 2014: 46).

Notwithstanding, some appeals logged at the Council contained one or several irregularities directly linked to votes cast online[213] (Anziani and Lefèvre*,* 2014: 49). In all cases the judges applied their traditional case-law to electronic voting[214], attempting to contextualise any irregularities and concluding that the shortcomings did not affect the validity or reliability of the results (Barrat, 2015: 145). When the Constitutional Council had to position itself regarding allegations of fraud, it systematically rejected them (Anziani and Lefèvre, 2014: 39). On this matter, the Council argued that anyone filing a complaint should provide proof of the alleged fraud or error for the election and circumscription in question. Since this requirement places the burden of the proof on the applicants, it should not come as a surprise that the majority of complaints were rejected.

For example, the Constitutional Council rejected a complaint by the Pirate Party that highlighted several drawbacks in the operations of remote electronic voting. They ranged from technical weaknesses to chronological contradictions, like approving the legal framework having already sent the personal data to the supplier, or procedural faults, like not inviting the party representatives to the meetings of the *bureau de vote par voie électronique* (Barrat, 2015: 146). The Court also rejected a request to cancel the results of the 2012 parliamentary elections for the fourth district of French voters abroad[215], where several voters had not managed to cast their vote because of the update in the Java Virtual Machine. The reasoning of the Court was that the number of voters affected was not significant (Deromedi and Détraigne, 2018: 30).

The Constitutional Council followed the Council of State's reasoning in 2007 and subordinated the annulment of the e-enabled elections to the evidence provided by the claimant. They should proof that a significant number of electors in the circumscription had been affected by eventual malfunctioning, and that those events were of such a nature that the integrity of the election could be compromised (Anziani and Lefèvre, 2014: 50). Lastly, Alain Anziani and Antoine Lefèvre (2014: 50) also highlight the decision[216] by the Constitutional Court about the vote whose certificate had been corrupted. Where, in the

[212] The Constitutional Court ruled that any voting method should guarantee the sincerity of the election and the secrecy of the vote. *Conseil Constitutionnel, 18 juikket 2013, Loi relative à la representation des Français établis hors de France, decision nº 2013-673 DC du 18 juillet 2013*.

[213] All in all, following the legislative elections of June 2012, the Council received 108 complaints filled either by candidates or by voters (Constitutional Council, 2013: 1).

[214] According to Alain Anziani and Antoine Lefèvre, showing caution – if not reluctance – to accept a mean based on a computer malfunction (2014: 49).

[215] Décision nº 2012-4597/4626 AN, of 15 February 2013.

[216] Décision nº 2012-4580/4624 AN, of 15 February 2013.

opinion of the rapporteurs from the Senate, this instance clearly highlighted some sort of error –if not a voluntary manoeuvre–, the Constitutional Court declared that such vote had been declared spoiled according to the applicable law. In the opinion of the Court, the fact that the vote was declared invalid proved that electoral operations were properly conducted.

c) The election without internet voting (2017), the CNIL's updated standards (2019), and the resumption of remote electronic voting

The next elections were planned for 2017. However, only two months before the contest the resort to internet voting was abandoned for that year's elections[217] (Deromedi and Détraigne, 2018: 8). The OSCE/ODIHR reported that, while some interlocutors voiced concerns with regards to limited information and public debate prior to suspending internet voting, all underlined the importance of preventing foreign interference and minimising the risk of jeopardising the integrity of election results (OSCE/ODIHR, 2017: 2). At the time, four main concerns were highlighted, three of which had already been raised previously:

- The difficulties in guaranteeing the personal and secret nature of the vote;
- Issues with the social act of voting and the loss of solemnity of the vote;
- The impossibility to check the ballot box and the counting of the votes; and
- A new concern related to the increasing risks of hacking.

In the opinion of Jacky Deromedi and Yves Détraigne (2018: 34), this concern is what actually motivated the decision not to allow the use of remote electronic voting for the 2017 elections. This position is consistent with Romain Rambaud's assessment as well (2019: 38). Notwithstanding, that decision was made for the legislative elections only. France has not abandoned its plans to offer remote electronic voting to its voters abroad[218]. Proof of that are the most recent elections to the advisers of French abroad and the consular delegates in May 2021[219]. French voters could vote online during the advance

[217] Arrêté du 17 mars 2017 relatif au vote par correspondance électronique pour l'élection de députés par les Français établis hors de France.

[218] In fact, 2022, the Government has been working since 2018 to overhaul the dedicated voting platform ahead of the legislative elections scheduled for June 2022 (Buffet, 2020: 42). In this occasion, the provision of the voting platform has been entrusted to Voxaly, a subsidiary of the *La Poste*. More recently, the Senate even studied whether remote electronic voting could have been introduced for the regional and departmental elections scheduled in 2021 (Buffet, 2020). The report, submitted in December 2020, concluded that it would not be possible to meet the necessary requirements in such a short period of time. Notwithstanding, it encouraged further consideration on the technical developments to secure Internet voting and guarantee the sincerity of the vote in order to explore, its use beyond the elections of French people living abroad in the mid-term (Buffet, 2020: 10).

[219] Initially planned for May 2020, the health crisis caused by the Covid-19 pandemic forced the French government to postpone the elections. The elections were postponed first to June 2020 and afterwards to May 2021 (Deromedi, Frassa and Leconte, 2020: 10). Consequently, the candidates registered and the authorisations to vote by proxy were cancelled out. In turn, the elections of the members of the Assembly of French Citizens Abroad and the elections to the French Senate were postponed until June and September, respectively (Deromedi, Frassa and Leconte, 2020: 10). On 23 February 2021, a scientific committee confirmed that the elections could be held on 29 and 30 May 2021. Following, the government informed the Parliament of their intentions to pursue the organisation of the elections and published the decree calling for the election.

voting period (21-26 May) or vote at a polling station on election day, Sunday 30 May (except for America and the Caribbean where the election took place on Saturday, 29 May). Alternatively, voters could also appoint a proxy to vote on their behalf on election day. Postal voting was not offered, since this channel is no longer envisaged following the reform of the institutions representing French citizens abroad of 22 July 2013 (Haritcalde, 2020: 2).

In terms of participation, the results published by the Ministry of Foreign Affairs show a clear support for the online voting channel: out of the 205,865 votes cast (representing 15% of all eligible voters), more than 85% were cast electronically (176,734 votes). This proportion represents a sharp increase when compared to the 2014 elections (when only 43.26% of all votes were cast online) and confirms the trend of increased online participation observed since the introduction of online voting in 2006.

In the meantime, the CNIL has further updated their Recommendation to take stock of the new requirements introduced by the EU's GDPR (CNIL, 2019c). The goal of the update is to apply to future developments in internet voting, with a view to better respect the principles of personal data protection, and to inform data controllers on their choice for an online voting system (CNIL, 2019a). The Recommendation identifies a set or requirements for remote electronic voting systems in three different levels, depending on the risks each contest may face. Therefore, the new Recommendation first identifies three security levels. The three levels are described as follows[220] (CNIL, 2019a: 2):

Ahead of the election, the Ministry of Foreign Affairs organised two User Acceptance Tests (in French, *Test Grandeur Nature* or TGN). More than 12.000 eligible voters volunteered to participate in the TGN. In the end, 3.408 eligible voters took part in the first TGN of July 2019 and 4.302 in the second one in November (Deromedi, Frassa and Leconte, 2020: 21). The second TGN was conducted between 22 and 26 November 2019. According to Marie-Christine Haritcalde (2020: 6) 12.943 voters (out of the 1.257.767 registered) were involved in the test, out of which 12.640 has provided their email address and 12.222 their mobile phone number. Overall participation was of 33% (six points higher than in the previous TGN) (Haritcalde, 2020: 6). According to Jacky Deromedi, Christophe-André Frassa and Jean-Yves Leconte, At the end of the second TGN, 84.2% of the participants declared that they had not encountered any difficulties to vote (2020:21).

[220] The description of the levels is actually more detailed. The standards by the CNIL (2019a: 2) provide the following description:

« - Niveau 1 : Les sources de menace, parmi les votants, les organisateurs du scrutin ou les personnes extérieures, ont peu de ressources et peu de motivations. L'administrateur (ou les administrateurs) du système d'information n'est ni électeur, ni candidat. Il est considéré comme neutre par toutes les parties. Ce niveau s'applique pour les scrutins impliquant peu d'électeurs, se déroulant dans un cadre non conflictuel, à l'issue duquel les personnes élues auront peu de pouvoirs, comme par exemple l'élection d'un représentant de classe. Le scrutin ne présente pas de risques importants.

- Niveau 2 : Les sources de menace, parmi les votants, les organisateurs du scrutin, les personnes extérieures, au sein du prestataire ou du personnel interne, peuvent présenter des ressources moyennes ou des motivations moyennes. Ce niveau s'applique à des scrutins impliquant un nombre important d'électeurs et présentant un enjeu élevé pour les personnes mais dans un contexte dépourvu de conflictualité particulière. Il s'agit par exemple des élections de représentants du personnel au sein d'organismes ou encore au sein d'un ordre professionnel. Le scrutin présente un risque modéré.

- Niveau 3 : Les sources de menace, parmi les votants, les organisateurs du scrutin, les personnes extérieures, au sein du prestataire ou du personnel interne, peuvent présenter des ressources importantes ou de fortes motivations. Ce niveau concerne les scrutins impliquant un nombre important d'électeurs et présentant un enjeu très élevé, dans un climat potentiellement conflictuel. Il s'agit par exemple d'élections de représentants du personnel au sein d'organisations importantes, à grande échelle et dans un cadre conflictuel. Le scrutin présente un risque important. »

- Level 1: no significant risks.
- Level 2: moderate risk.
- Level 3: significant risk.

Second, each of these levels[221] has some security objectives associated to them, which are incremental. Therefore, at level 2 both the objectives for level 1 and level 2 must be achieved. It is not specified how to achieve these objectives. According to the CNIL, "data controllers or their service providers are free to use any solution that allows them to achieve the security objectives" (2019a: 3). However, some solutions are already suggested (CNIL, 2019c).

To assess which is the specific level of a given election, the CNIL then offers an evaluation grid based on 10 questions. Each of the questions must be answered as either true or false (CNIL, 2019c). At the end of the questionnaire, a specific level is assigned to that election based on the number of questions for which the answer is "true": level 1 in case there are two or less questions whose answer is "true"; level 2 when there are between three and six "true" answers; and level 2 when the "true" answers are seven or more.

In addition to the security objectives, the Recommendation also prescribes certain obligations. For example, at all levels voters should be informed about the voting operations and the general functioning of the system (CNIL, 2019a: 3). It also requires that remote electronic voting systems are evaluated by an independent expert, at all three levels. In the context of elections at the levels 2 and 3, such appraisals become audits based on intrusion tests. Furthermore, at level 3 such audits must be conducted *ad hoc*, despite the fact that at levels 1 and 2 previous evaluation reports may be used instead (as long as they do not have more than 24 and 12 months, respectively) (CNIL, 2019a: 4)

3. Estonia

"In 2005 Estonia became the first country in the world to have nation-wide local elections where people could cast binding votes over the internet"[222] (Vassil, 2016: 2). Successive local, national, and European elections followed. Today, Estonia remains the only country in Europe that has offered the possibility to vote online to all its electorate. Following a first experience in the framework of the local elections in 2005, Internet voting was used as an additional advanced voting channel for the 2007 elections to the Estonian parliament (the *Rigikogu*) between the sixth and the fourth days preceding election day. "The share of e-voters in the first e-enabled elections was very low, i.e. only less than 2% of all votes were cast online" (Vassil, 2016: 3) but this number has increased and in 2014 every third vote was cast online (Vassil, 2016: 3).

"[S]ince 2011, there have been more electronic advance voters compared to paper advance voters" (Vinkel and Krimmer, 2016: 184-185). "By 2019, this option has grown

[221] The CNIL does not recommend using remote electronic voting systems in those other circumstances where the source of threat is considered to have both significant resources and strong motivations (CNIL, 2019a: 2).

[222] It is interesting to see how different authors argue that Estonia was "leading a kind of 'race' at the beginning of the 2000s for introducing remote electronic methods in elections" (Vinkel and Krimmer, 2016: 184) or highlight "Estonia's function as a trailblazer [sic] in this respect" (Madise, 2007: 5).

to be the second most favourite for Estonian voters, with about 44% of votes being cast this way during the 2019 Parliamentary elections" (Buldas et al., 2020: 6). It is important to note that "Internet voting is an additional voting method and is not obligatory" (OSCE/ODIHR, 2007b: 8). The Estonian case is of interest to us for two main reasons. On the one hand, because it is the only example in Europe of a country allowing its entire electorate to vote online. On the other hand, because in Estonia "it has been possible to get out of the apparent trap of the legal principles of voting secrecy and equality on a rather practical level" (Madise, 2007: 15).

After regaining its independence from the Soviet Union in 1991, Estonia became a "parliamentary democracy with a President, Prime Minister, and a 101-seat unicameral Parliament, the *Riigikogu*" (Drechsler and Madise, 2002: 235). "Members [of the *Riigikogu*] are elected from 12 multi-seat constituencies for four-year terms through a proportional, open-list system" (OSCE/ODIHR, 2007a: 1). "The municipal level with around 205 units has a certain degree of autonomy and also enjoys democratic elections; there is no level, other than purely administrative ones, in-between the local one and the central government" (Drechsler and Madise, 2002: 235). More importantly, Estonia also became a referent of e-governance and of digitisation. "Estonia's success making their public services available online is first and foremost based on the widespread use of electronic identification cards" (Vassil, 2016: 16). "After passing the Identity Document Act in 1999 and the Digital Signature Act in 2000, the first ID cards were issued in January 2002" (OSCE/ODIHR, 2007b: 9). Between 2002 and 2014, "about 1.2 million of these credit-card size personal identification documents have been issued, allowing citizens to digitally identify themselves and sign documents or perform actions" (Vassil, 2016: 16). According to Ülle Madise, the reason for launching Internet voting in Estonia was precisely this "e-fascination and the aspiration to find 'innovative', i.e. new, solutions" (2007: 16).

According to the OSCE/ODIHR, elections in Estonia are managed by the Estonian National Electoral Committee "and a network of election managers and polling staff, led by the [Estonian State Electoral Office]" (OSCE/ODIHR, 2019b: 4)[223]. The Estonian National Electoral Committee "is an autonomous body responsible for overall electoral management, including to issue decisions and to supplement the legal framework, manage candidate registration, consider complaints, and validate election results" (OSCE/ODIHR, 2019b: 4). It "is composed of […] a judge of a court of first instance, a judge of a court of appeal, an advisor to the Chancellor of Justice, an official of the State Audit Office, a public prosecutor, an official of the Chancellery of the *Riigikogu*, and an official of the State Chancellery" (OSCE/ODIHR, 2007a: 4). On the other hand, the State Electoral Office "lead the executive branch of the election administration and is in charge of all operational preparations and the conduct of elections" (OSCE/ODIHR, 2019b: 4), including "the organization of Internet voting" (OSCE/ODIHR, 2019b: 4). Below the level of the State Electoral Office, the preparation for elections is co-ordinated by city and rural municipality secretaries at the

[223] Until 2017, [e]lection administration was carried out by a three-tiered election commission structure (OSCE/ODIHR, 2007a: 3). For example, "[t]he *Riigikogu* Elections Act establishes a three-tiered election administration structure that is responsible for the preparation and conduct of the elections to the *Riigikogu*. The National Election Committee (NEC) is at the top of the structure, with 15 County Electoral Committees and two City Electoral Committees (CEC) at the second level and 657 Division Committees (DC) at the third level. Regulations issued by the NEC and decisions and instructions of superior electoral committees are binding for the lower level committees" (OSCE/ODIHR, 2007b: 7)

municipal level, and Voting District Committees[224] at the polling station-level [225] (OSCE/ODIHR, 2019b: 4). For the latest *Riigikogu* elections of 2019, there were 79 city and rural municipality secretaries, some of them with "additional responsibilities related to county-level co-ordination and material delivery" (OSCE/ODIHR, 2019b: 4), and 451 Voting District committees.

Estonia's Constitution states that elections must be general, uniform, and direct. It "also provides for the secret ballot" (Meagher, 2009: 360). "According to article 60 of the Estonian Constitution, 'Members of the *Riigikogu* shall be elected in free elections on the principle of proportionality. Elections shall be general, uniform, and direct. Voting shall be secret'" (Drechsler and Madise, 2002: 239). Elections are regulated in three different acts: [p]arliamentary elections are primarily regulated by the *Riigikogu* Election Act (OSCE/ODIHR, 2007a: 3), while election for local government units are regulated by the Municipal Council Election Act and elections to the European Parliament at the European Parliament Election Act. Additionally, the Referendum Act deals with referendums, which according to the provisions in Chapter 7 shall provide also for the option to vote electronically[226].

In addition to electoral regulations, "the Estonian e-government ecosystem is strongly regulated by legal instruments that provide a framework for security and protection of the personal data" (Vassil, 2016: 18). This framework includes, among others, Estonia's Personal Data Protection Act (1996), the Public Information Act (2000), the Population

[224] Previously, these tasks had been assumed by county and city election committees (CEC) and division committees (DC) (OSCE/ODIHR, 2007a: 3). On the one hand, the CEC consisted "of up to 13 members. The County Secretary serves as CEC chairman, and the county Governor appoints the remaining members on the proposal of the Secretary. For the cities of Tallin and Tartu, the CEC Chairman is the corresponding City Secretary, and the other members are nominated by the political parties participating in the elections and half are nominated by the municipal or city secretary" (OSCE/ODIHR, 2007a: 4). On the other hand, "[t]he division committees and responsible for the administration of the election at polling station level. [They] are multi-party commissions. DCs may have up to nine members; the chairman and members are appointed by resolution of the local government council. Half of the members are nominated by the political parties participating in the elections and half are nominated by the municipal or city secretary" (OSCE/ODIHR, 2007a: 4).

[225] Additionally, the Final Report by the OSCE/ODIHR's 2007 Election Assessment Mission also identified the following actors responsible for remote electronic voting (2007b: 11): the Ministry of the Interior's Population Registry, responsible for providing the list of eligible voters and issuing the national ID cards; the Estonian Informatic Center, responsible for government IT infrastructure and for the hosting of the servers; Sertifitseerimiskesus AS, a private company contracted as certification authority and able to issue legally accepted digital certificates: Cybernetica AS, the private company that developed the software for internet voting; and KPMG Baltics AS, as the private company entrusted to audit the internet voting system. Since 2017, when the NEC decided to outsource the management of the collecting and securing Internet voting, the Estonian state Information System Authority (RIA) is also involved in the electoral processes. Since them, the Registration Service [is] outsourced as well and operated by a private company (OSCE/ODIHR, 2019b: 8).

[226] Additionally, Sutton Meagher has noted (2009: 360-361) that

> "[t]he Estonian Penal Code has a set of criminal provisions relating to elections. The Penal Code prohibits interfering with voting and utilizing violence or taking advantage of a relationship to influence how another person votes. Criminal laws also prohibit anyone from violating the confidentiality of the secret ballot or employing bribery to induce someone to vote, not vote, or vote in a certain way".

Register Act[227] (2000), the Digital Signatures Act (2000), and the Electronic Communications Act (2004) (Vassil, 2016: 19-20).

In what follows, we provide an overview of the evolution of remote electronic voting in Estonia. The analysis is based on Priit Vinkel's three periods (2016: 41). However, they have been slightly modified and an additional fourth period has been added that describes the current landscape.

a) The setup, implementation, and constitutionality of Internet voting (2001-2005)

Early in 2001, the then Estonian Minister of Justice publicly announced a plan to introduce internet voting in Estonia (Drechsler and Madise, 2002: 236). The then Prime Minister, Mart Laar, proposed the idea to test e-voting already in 2001 "and to decide then whether to introduce it already for the 2002 local elections" (Drechsler and Madise, 2002: 237). However, the Ministry of Justice commissioned an analysis to two cryptographers that "recommended to prepare some experiments or pilot-projects first and not to introduce e-voting before 2007" (Drechsler and Madise, 2002: 238). A second analysis was commissioned in fall focusing on technical question and costs (Drechsler and Madise, 2002: 238).

Despite these recommendations, the Ministry of Justice started drafting Internet voting provisions as part of four different elections laws (the Local Communities Election Act, the *Riigikogu* Election Act, the European Parliament Election Act, and the Referendum Act) and sent them to the parliament (Drechsler and Madise, 2002: 238). On 30 April 2001, the draft of the Local Government Councils Election Act was initiated at the *Riigikogu* (Madise, Vinkel and Maaten, 2006: 13). "Parliamentary debate on e-voting was nevertheless long and lively. The problems most discussed were the equality of citizens in political life, privacy and secrecy of voting, security of electronic voting systems, and how to avoid fraud" [emphasis added] (Drechsler and Madise, 2002: 240). Wolfgang Drechsler (2003: 5) lists the following main concerns put forward by those Members of Parliament opposing e-voting: equality of citizens in political life (i.e., the digital gap or divide); detriment to democracy (i.e., going to the polling station would be a valuable action by itself); unconstitutionality of e-voting (secrecy, generality, and uniformity); the privacy and secrecy of voting not being guaranteed; the security of electronic voting systems and the proneness to fraud (including the "problem" of hackers); as well as the negative or absent experiences in other countries[228]. According to Ülle Madise, "the controversial or absent experience in other countries and security of electronic voting systems belonged to the most discussed issues in the Estonian parliament" (2007: 16).

On the discussion about remote electronic voting's compliance with Constitutional principles, the Minister and the Ministry based themselves on a *teleological* approach, as we will see in more detail in the next chapter. They stated that "that Constitutional problems should be understood through the problems the given principles were meant to

[227] According to Vassil (2016: 20), in Estonia "when new public e-services are developed, it is legally not permitted to design system that store the same data in different repositories. In practical terms this means that if a citizen's age is stored in the Population Register, it will be retrieved automatically for checking their eligibility for e.g. voting or driving, but not collected additionally by the system of internet voting."

[228] For a more detailed description of these concerns see also Wolfgang Drechsler and Ülle Madise (2014: 103)

solve" (Drechsler and Madise, 2002: 239). In the case of the principle of secrecy, it was said, it would be actually achieved "if all those who ha[d] voted via the Internet ha[d] the right (which was proposed) to go to the polling station on election day and replace their electronically recorded, transferred and counted [sic] vote by a new paper-ballot" (Drechsler and Madise, 2002: 239). "[A] large majority of Members shared the Ministry's attitude towards teleological interpretation of the Constitution" (Drechsler and Madise, 2002: 240) and thus the initial provisions on e-voting were adopted on 27 March 2002. The new laws entered into force on 6 May 2002 (Madise, Vinkel and Maaten, 2006: 13).

Therefore, "[t]he year 2002 marked the start of the setup phase, when a very general principle for remote electronic voting was stipulated under electoral law (LGCEA, 2002), allowing the election authorities to start with the project preparations, find a vendor for the system and prepare for the 2005 local elections" (Vinkel, 2016: 44). However, and while it was expected that Estonia would be "the leading country for e-voting, introducing it already for the national elections of 2003, the Estonian parliament voted for delaying the implementation of e-voting until 2005" (Drechsler and Madise, 2002: 234). In this sense, "probably genuine worries that technical problems would not be solved by the Fall of that year, as well as the scepticism of individual members of parties generally in favour of e-voting, all of them reasonable and appropriate, were among the reasons that prevented such an outcome" (Drechsler and Madise, 2002: 243). Likewise, and as a result of the parliamentary debate, the principle that "the voter shall vote himself or herself" was added to all laws or drafts[229] (Drechsler and Madise, 2004: 104).

[229] The main requirements of the first regulation of remote electronic voting in Estonia have been described by Wolfgang Drechsler and Ülle Madise (2002: 241) as follows: (1) voting would be possible on advance polling days (the sixth to the fourth day before election day) on the website of the National Electoral Committee; (2) voters would have to certify their identity by giving their digital signature via the ID Card (as of 1 January 2002, it became compulsory to hold and ID card); (3) following identification, the list of candidates would be displayed, and voters would have to mark the candidate in favour of whom they voted; and (4) voters would then receive a message on the website stating that their vote had been calculated. Since multiple voting would be possible, to prevent that more than one vote per voter would be included in the final tally the NEC would prepare a list of voters having cast their vote electronically at the end of the advance voting period. Following, and based on this list, each division committee would check whether a voter had voted more than once, including using electronic means, and "send a corresponding notice to the National Electoral Committee immediately. On the basis of such notice, the National Electoral Committee must not tally the voter's vote cast using electronic means" (Drechsler and Madise, 2002: 240)

The electronic voting project started in August 2003 with the appointment of "a project manager and a six member steering committee. The group finalized its General Concept paper in January 2004, after a security analysis in December 2003 of an expert group with IT specialists from the private sector and academics" (OSCE/ODIHR, 2007b: 10). There were three preconditions for the implementation of the e-voting project (Madise, Vinkel and Maaten, 2006: 20): (1) the existence of a legal basis, (2) widespread use of ID cards guaranteeing the electronic identification of persons and digital signature, necessary for e-voting, and (3) the existence of electronic polling lists. "On the basis of the General Concept Paper, the NEC published a tender in March 2004" (OSCE/ODIHR, 2007b: 10). "[t]hree tenders were submitted to the public procurement of e-voting software. The Government of the Republic declared the offer of AS Cybernetica winner" (Madise, Vinkel and Maaten, 2006: 20). By autumn "the software was ready and preparations were made for the first public pilot project, which was offering the possibility of e-voting in the polling of the residents of Tallin" (Madise, Vinkel and Maaten, 2006: 20) "about the location of the Freedom Monument to be erected in Tallin" (Madise, Vinkel and Maaten, 2006: 25). The goal of this limited pilot was to test the features of the system (Vinkel, 2016: 44). "The system was implemented as a whole, including the possibility to change one's vote, giving priority to ballot paper and public opening of votes with the e-voting system keys divided between the members of the committee" (Madise, Vinkel and

In 2005, "[l]egal debates on the topic were restarted […] to broaden the regulations in the law" (Vinkel, 2016: 44). According to Ülle Madise, Priit Vinkel and Epp Maaten (2006: 17), the

> "[d]escription of the e-voting procedure in the Act adopted in 2002, among other things, [had] left it open whether it is allowed to change the e-vote or not, also there was no description of how the e-votes are to be calculated [sic]. Upon completion of the technical solution the National Electoral Committee presented the detailed description of e-voting procedure to the Riigikogu Constitutional Committee and the Constitutional Committee initiated a relevant amendment to the Act"

The *Riigikogu* adopted the amendments on 12 May 2005, but the "President of the Republic refused to proclaim the Local Government Election Act on 25 May 2005, referring in the reasons for his decision to contradiction with the principle of uniformity of local government councils elections stipulated in subsection 256 of the Constitution" (Madise, Vinkel and Maaten, 2006: 19). In this sense, "[t]he Estonian President, Arnold Rüütel, opposed […] the inequality between e-voters and traditional voters in the sense that e-voters could apply reversible voting during the three days (i.e. re-cast their e-votes) while this was not possible for traditional voters" (Breuer and Trechsel, 2006: 7). According to the President of the Republic, "not all voters were guaranteed equal opportunities for voting: the voter who can vote electronically has the right to change his or her electronically given vote by voting again electronically or with ballot paper, whereas the voters using other means of voting do not have such possibility to vote again" (Madise, Vinkel and Maaten, 2006: 19). The *Riigikogu* further amended the Act, acknowledging that the possibility to change an e-vote during election day could influence some voters, but the President of the Republic again refused to proclaim it.

As a result of the Estonian President's opposition to proclaim the Act, "[t]his period also held the discussions about the constitutionality of the system in the constitutional Chamber of the Estonian Supreme Court" (Vinkel, 2016: 44). On 12 July 2005, after the *Riigikogu* again adopted the unamended Act, the President of the Republic turned to the Supreme Court to declare it unconstitutional. However, "[t]he Constitutional Review Chamber of the supreme Court refused to satisfy the application of the President of the Republic", who pursuant to the Constitution was obliged to proclaim the Act (Madise, Vinkel and Maaten, 2006: 20). The Supreme Court of Estonia justified the constitutionality of e-voting and of multiple voting ruling that (2005):

> "[d]espite the repeated electronic voting a voter has no possibility to affect the voting results to a greater degree than those voters who use other voting methods. A vote given by electronic means shall be counted as one vote and from the point of view of voting results this vote is in no manner more influential that the votes given by voters using other voting channel."

As a matter of fact, it noted that "[t]he introduction of electronic voting without allowing to change the vote given by electronic means may endanger the principles of free voting

Maaten, 2006: 25). The pilot took place between 24 and 30 January 2005 and 703 voters took part in it, out of which 697 votes were counted (Madise, Vinkel and Maaten, 2006: 20). "13,7% of all those who participated in the poll used the possibility of e-voting" (Madise, Vinkel and Maaten, 2006: 25).

and secret voting" (Supreme Court of Estonia, 2005). The Supreme Court of Estonia (2005) also observed that

> "[t]rough legislation concerning suffrage, the legislator has guaranteed all voters the legal possibility to vote in a similar manner. In the legal sense the system of electronic voting is equally accessible to all voters at local government council elections […] [T]he identity card (ID card) necessary for electronic voting is mandatory for both an Estonian citizen staying permanently in Estonia and an alien staying permanently in Estonia on the basis of a valid residence permit. Thus, the state has created no legal obstacles to anyone to electronic voting, including to changing one vote during the time prescribed for advance polls".

The Supreme Court of Estonia also upheld the *teleological* approach to secret suffrage in their ruling when observing that "[t]he secrecy of voting as a subprinciple [sic] of freedom of elections is a prerequisite of free elections. Pursuant to the principle of free elections both the participation in elections as well as the choice to be made are voluntary" (Supreme Court of Estonia, 2005). Interestingly enough, the Court also ruled that the principle of free elections gives rise to the obligation for the state to guarantee the protection of voters against persons trying to influence their choices. In this context, the possibility offered to cast multiple electronic votes, or to cancel any electronic vote by casting a paper ballot, would be thus the most effective measure "to guarantee the freedom of election and secrecy of voting upon electronic voting in an uncontrolled medium" (Supreme Court of Estonia, 2005). After the Constitutional Court decided "that the proposed system did not violate the Constitution and electoral principles, the President ultimately signed the amendment on 5 September 2005 and the Act finally entered into force on 18 September 2005" (Trechsel et al., 2006: 12).

"The first e-enabled elections (for local government councils) were held in October 2005" (Vinkel, 2016: 44). The 2005 "local elections in Estonia were the first time that an electorate of an entire country could cast its vote over the Internet in a public election" (Breuer and Trechsel, 2006: 3). "In Estonia local government councils are elected for four years on the basis of proportional electoral system" (Madise, Vinkel and Maaten, 2006: 12). For the 2005 local government council elections there were 240 electoral districts in 227 cities and rural municipalities (Madise, Vinkel and Maaten, 2006: 12). Ahead of the election, the National Electoral Committee organised a campaign to inform about e-voting and "[b]etween 26 September and 2 October 2005 all persons eligible to vote were given the possibility to test e-voting in order to encourage people to solve the problems that might emerge (acquisition of necessary software, updating expired ID card certificates, renewal of PIN codes etc.) before the days of real e-voting" (Madise, Vinkel, and Maaten, 2006: 25). "In August 2005 all larger political parties were called to take part in a training course on observing e-voting. As e-voting was new way of voting that could not be observed according to the same principles as traditional voting, special approach to the observing of e-voting was necessary"[230] (Madise, Vinkel, and Maaten, 2006: 20).

[230] Madise and Martens (2006: 17) further developed this idea as follows: "[e]-voting results cannot be verified by people themselves and people need to have an absolute faith [sic] in the accuracy, honesty and security of the whole electoral apparatus (people, software, hardware). Thus, for people who didn't program the system, the operations of the computers can truly be verified only

Voters were eligible to vote online "throughout three days of advance voting (6-4 days before the actual Election Day)" (Breuer and Trechsel, 2006: 9), meaning that "Internet voting in the elections took place from Monday, October 10 to Wednesday, October 12" (Breuer and Trechsel, 2006: 7). In order to vote, voters had to have a digital ID card[231]. The voting interface was provided through a Voter Application accessible "via an internet browser. Voters using Microsoft Windows open[ed] the internet web address www.valimised.ee with their browser, while for voters who use Mac OS or Linux the voting interface is a stand alone program"[232] (OSCE/ODIHR, 2007b: 13). "The encrypted [sic] system was based on the so-called digital envelope method and used public key cryptography, which ensures the maintenance of the privacy of e-voters" (f: 9).

As already mentioned, "e-voters had the possibility of electronic re-vote: they could vote more than once and only the last vote was counted. This measure was supposed to avoid the possibility of vote-buying" (Breuer and Trechsel, 2006: 9). To ensure that only one vote per voter is counted, after the end of advance poll and before election day on Sunday all polling stations were informed of the e-voters on their list of voters. If it was found that a voter had voted both electronically and with paper ballot, the polling division would inform the National Electoral Committee, who would cancel that voter's e-vote (Madise, Vinkel and Maaten, 2006: 23). "Before the verification of voting results in the evening of the election day, the encrypted votes and the digital signatures with personal data or inner and outer envelopes are separated. Then the e-votes are opened and

by knowing the input and comparing the expected output with the actual outcome. Under a secret ballot system, there is no known input, nor is there any expected output with which to compare electoral results". As we will see in the following pages, while the transparency and auditability of remote electronic voting systems has evolved and today may no longer be necessary to have "an absolute faith" in the electoral apparatus, it is still common to oppose the principles of free (include with references to accuracy and integrity) and secret suffrage.

[231] "Upon the issue of ID card a person is given two PIN codes. PIN 1 is meant for digital identification of a person and PIN 2 for digital signing […] The PIN codes and PUK code necessary for the electronic use of the ID card are known only to the owner of the card, the codes are issues in a safety envelope together with the ID card" (Madise, Vinkel and Maaten, 2006: 9). According to Ülle Madise, Priit Vinkel and Epp Maaten (2006: 9), one of

> "[t]he problems that had to be solved before the implementation of e-voting was the updating of ID card certificates and restoring PIN codes […] part of the certificates had expired immediately before the election in 2005. On the other hand, most of the ID card holders do not use the card electronically and they have no need for PIN codes, so they have been lost or destroyed in the course of time."

Therefore, "[a] campaign was organised before the election to inform the cardholders of the need to update the certificates and a possibility to get new PIN codes free was created. The purpose was to establish conditions for the use of ID card at e-elections for as many people as possible" (Madise, Vinkel and Maaten, 2006: 10)

[232] According to Fabian Breuer and Alexander H. Trechsel (2006: 9):

> "the voters got access to the online ballot with the[…] ID-cards, which allow electronic personal authentication and digital signatures. The voters had to access a particular website and to introduce their electronic ID-card in a card reader, which is connected to the computer. Once identified through the ID-card and authenticated with a PIN code, a relevant candidate list of voter's constituency was displayed according to the voter's identification number. Subsequently, the voter made his or her voting decision"

The voting process continued with the following steps (Madise, Vinkel and Maaten, 2006: 23):

> "[t]he application downloaded in the voter's computer during e-voting encrypts the vote before it is sent to the voting server through web connection. The encrypted vote can be regarded as the inner, anonymous envelope. After that, the voter gives a digital signature to confirm his or her choice. By digitally signing, the voter's personal data or outer envelope are added to the encrypted vote."

counted. The system opens the votes only if they are not connected to personal data"[233] (Madise, Vinkel and Maaten, 2006: 23).

In this first experience, "about 2% of the voters, i.e. 9317 persons with the right to vote used the possibility of internet voting, giving a total number of 9681 e-votes. 9287 e-votes were taken into account in the verification of election results: during the changing of e-votes, 364 e-votes were given and the e-voters also voted with 30 ballot papers" (Madise, Vinkel and Maaten, 2006: 28). "The overall turnout at these elections was 47,4 percent" (Breuer and Trechsel, 2006: 7). Overall, Ülle Madise, Priit Vinkel and Epp Maaten (2006: 27) point out that:

> "General conclusion is that the implementation of e-voting at the local government councils elections of 2005 was successful. The auditors confirmed that the e-voting system worked correctly, also there were no failures of problems that could have shattered people's trust in the honesty of e-voting and the reliability of the system. No complaints connected with e-voting were submitted to the National Electoral Committee or the Supreme Court."

According to the OSCE/ODIHR, who did not observe these elections but referred to them in later reports, however, "[t]here were no reports of significant disruptions in the functioning of the system, although voting was interrupted for a brief period" (2007a: 5). Interestingly, "[t]here were no court cases and we do not have any information about purchase of e-votes (on the contrary to the votes on paper-ballot)" [emphasis added] (Madise and Martens, 2006: 26). "[A]s the elections passed off without any problems, they paved the way to using e-voting during the legislative elections of 2007" (Trechsel et al., 2007: 13).

b) The years of increasing participatory numbers and additional legal debates (2006-2013)

The second phase of remote electronic voting in Estonia "entailed a steady rise in user numbers and diffusion of the solution to the wider electorate"[234] (Vinkel, 2016: 44). After the 2005 Local Council Government elections, "[t]he *Riigikogu* Election Act was subsequently amended to enable the use of remote internet voting for the 4 March 2007 parliamentary elections. The legislation provides that voters may vote by internet from six to four days before election day if they have an Estonian identity document permitting

[233] As we will see with more detail in the next chapter, to guarantee the secrecy of the votes the system used asymmetric cryptography: "[a] pair of keys is generated for the system in a special safety module so that its private component never leaves it. Public component of the pair of keys is integrated into the voter application and it is used for encrypting the votes" (Madise, Vinkel and Maaten, 2006: 24). the digital signatures with personal data are removed from the encrypted votes are transferred on a CD and afterwards the private key of the system is used, votes are summed up and the e-voting results are issued (Madise, Vinkel and Maaten, 2006: 24). More specifically, "[p]rivate component of the pair of keys is used in the Vote Counting Application for opening the votes on election day evening. The National Electoral Committee can open the votes, i.e. uses the private component, only collegially. After the end of the period of dealing with the complaints the private key is destroyed" (Madise, Vinkel and Maaten, 2006: 24)

[234] For instance, in the 2007 *Riigikogu* elections, 30.243 voters cast ballots via the Internet, compared to 9.317 in the 2005 local elections, and this number increased to 58.614 in the 2009 European Parliament elections (OSCE/ODIHR, 2011b: 8). "During the 2009 Local Government Council elections, 104.413 votes, or 15.8 per cent of all valid votes, were cast via the Internet" (OSCE/ODIHR, 2011a: 5)

digital authentification" (OSCE/ODIHR, 2007a: 6). In this sense, the use of remote electronic voting in the 2007 *Riigikogu* elections was "a remarkable *world-premiere*: for the first time an electorate could vote over the Internet in elections of a national parliament[235]" (Trechsel et al., 2007: 3). "Internet voting in the elections took place from 26 to 28 February (six to four days prior to Election Day)" (Trechsel et al., 2007: 11). "Overall, 30.275 voters […] used the possibility of e-voting, which corresponds to 5.4 percent of the participating voters" (Trechsel et al., 2007: 3) and more than three times the number of voters who cast their votes electronically in 2005. "The overall turnout of the elections was 61 percent (58% percent in the parliamentary elections of 2003)" (Trechsel et al., 2007: 11).

In their pre-election review of Estonia's parliamentary elections, the OSCE/ODIHR's Needs Assessment Mission concluded that "[t]he legal framework of Estonia overall provides for the conduct of democratic elections"[236] (2007a: 2). After the election, "media reports were positive about the election and in particular the success of Internet voting" (Meagher, 2009: 355). The Final Report of the OSCE/ODIHR's Election Assessment Mission noted that "[t]he election administration implemented the system in a fully transparent manner, and appeared to take measures to safeguard the conducted of internet voting to the extent possible" (OSCE/ODIHR, 2007b: 1). Notwithstanding, the OSCE/ODIHR's Mission also acknowledged that "[a]lthough the National Election Committee made considerable efforts to minimize the inherent risks, t testing and auditing of the system could have been more comprehensive" (2007b: 2). According to the Mission, internet voting "poses real risks to the integrity of elections due to the potential of external attacks or internal malfeasance" (OSCE/ODIHR, 2007b: 1) and "the organization of voting outside the supervised and controlled environment of a polling station always raises the potential that the fundamental right to a secret ballot could be compromised" (OSCE/ODIHR, 2007b: 2).

[235] As we have already seen, until then remote electronic voting had "so far been used in local elections, in consultative decision-making processes, in private elections and in a number of formally binding referendums, the parliamentary elections in Estonia were the first time that the electorate of an entire country had the possibility of electronically cast its vote for electing a national parliament" (Trechsel et al., 2006: 7). The OSCE/ODIHR's Needs Assessment Mission also noted that "the planned used of remote internet voting in the *Riigikogu* election would be the first countrywide use of the internet as a voting method in a parliamentary election in an OSCE participating State" (2007a: 1).

[236] In this sense, it was noted that (OSCE/ODIHR, 2007b: 9)

> "[t]he legislation introduced for the 2007 Riigikogu elections, similar to the legislation for local elections, provides that eligible voters with the digitally-enabled ID card may cast their ballot via internet during the advance voting period, from six to four days before election day. The law also permits voters to change their votes during the advance voting period, either by voting through the internet or by casting a ballot paper at a polling station. The law established the primacy of paper balloting. The voter can change his/her vote an unlimited number of times electronically, with the last ballot cast being the only one counted, but a vote cast by paper is final and annuls all internet votes cast by the voter".

The Needs Assessment Mission (OSCE/OIDHR, 2007a: 2) also noted that [emphasis added]:

> "[t]wo political parties represented in the current Riigikogu opposed the introduction of remote internet voting. Their concerns included the limitation on transparency due to the inherent difficulties of observing voting in an uncontrolled environment, the potential for violations of the secrecy of the vote, and the potential for coercion of voters or buying of votes" Notwithstanding, the Final Report of the Election Assessment Mission noted that "[n]evertheless, some improvements to the legislation could be made in relation to internet voting. The Riigikogu Election Act does not contain provisions regulating the security of the internet voting system. It does not foresee the responsibility of any institution, nor does it provide for specific grounds for application of sanctions in case of failures of the system" (OSCE/ODIHR, 2007b: 10).

The OSCE/ODIHR also observed the 2011 *Riigikogu* elections. A Needs Assessment Mission was deployed from 10 to 13 January 2011 and concluded that "[t]he authorities have followed up a limited number of previous OSCE/ODIHR recommendations, including those addressing the security of the internet voting system" (OSCE/ODIHR, 2011a: 1). The Needs Assessment Mission acknowledged certain changes, including an extended online voting period from three to seven days as well as the use of "mobile phones with specially enabled SIM cards for electronic identification and authentication" (OSCE/ODIHR, 2011a: 5). At the same time, they also noted that "no provisions for responsibilities or sanctions in case of failure or misuse of the system have been established" (OSCE/ODIHR, 2011a: 6). In this sense, they concluded that "[w]hile some modifications were introduced with regard to security of the Internet voting system, substantial changes in this area are still pending" (OSCE/ODIHR, 2011a: 10).

An Election Assessment Mission was then deployed from 21 February to 8 March 2011. The Election Assessment Mission's Final Report concluded that "there is scope for further improvement of the legal framework, oversight and accountability, and some technical aspects of the Internet voting system" (OSCE/ODIHR, 2011b: 1). Regarding the legal framework, the Mission noted that "generally provides an adequate legal basis for the conduct of democratic elections in accordance with OSCE commitments and other international standards, although the regulation of the Internet voting remains insufficient" (OSCE/ODIHR, 2011b: 3) and noted that "it is of concern that large parts of the Internet voting remain unregulated"[237] (OSCE/ODIHR, 2011b: 1).

The Final Report also accounts that "[d]uring the counting[238], one vote was determined invalid by the vote counting application since it was cast for a candidate who was not on the list in the corresponding constituency" (OSCE/ODIHR, 2011b: 11). "The project manager could not explain how this occurred", the same report follows (OSCE/ODIHR, 2011b: 11). Lastly, the Mission also observed that a "[f]ew formal complaints[239] were filed before the NEC or the Supreme Court [and] concerned, *inter alia*, […] lack of reliability, secrecy and security of the Internet voting"[240] (OSCE/ODIHR, 2011b: 2). For instance, "a citizen asked the NEC to cancel all the votes cast via the Internet due to alleged lack of secrecy, security and reliability of the Internet voting system in light of the program he developed to change the content of the vote without the voter noticing" (OSCE/ODIHR,

[237] According to the Mission (OSCE/ODIHR, 2011b: 9),

> "[t]he Internet voting process consists of five key stages: testing, set-up of the system, conduct of voting, counting, and destruction of data. The NEC organized the Internet voting process in a professional and timely manner. It maintained security of the system and ensured that voters wishing to cast their vote via the Internet could do so as easily as possible."

[238] Regarding the counting stage, the OSCE/ODIHR (2011b: 11) reports that,

> "[c]ounting of internet votes took place on 6 March in the presence of the NEC members and domestic and international observers. Before the decryption of the votes, the Internet votes superseded either by another Internet vote or by an advance paper ballot were cancelled. Four members of the NEC then used their keys to start the decryption of the votes, after which the votes were counted, uploaded into the Election Information System and displayed."

[239] According to Vinkel (2016: 40), [c]omplaints in Estonian elections (both on paper and on e-voting) can be issues via a fast-track appeal system, where institutions only have a limited period within which to reach a verdict (for electoral committees five working days, for the Supreme Court seven working days). In addition to the Supreme Court, appeals have to be scrutinised first by two lower tiers (county- and national-level) of electoral committees. Altogether, there are three tiers, so the maximum duration of dealing with an electoral complaint in all instances is about one month."

[240] According to their report, "[a]ll complaints were rejected as being ungrounded or for not being filed within the deadline" (OSCE/ODIHR, 2011b: 2).

2011b: 22) which the NEC did not consider to be a formal complaint "due to their lack of evidentiary basis" (OSCE/ODIHR, 2011b: 22). Additionally, "two complaints were filled to the Supreme Court by the Center Party with regard to the Internet voting" (OSCE/ODIHR, 2011b: 22). One of them challenged the decision by the NEC to dismiss the already mentioned complain. The second one "requested the Supreme court to cancel the results of the *Riigikogu* elections for the same reason of alleged lack of secrecy, security and reliability of the Internet voting" (OSCE/ODIHR, 2011b: 22) as well.

According to Priit Vinkel (2016: 44), "[t]he legal stipulations had not been changed between the year 2005 and 2011[241]. However, the technical solution was constantly updated for every election" and "the Mobile-ID support system and a new voter-application interface were developed for the 2011 general elections" (Vinkel, 2016: 44). Regarding the voter application, "[a]s of 2009 e-voters needed to download a voting program instead of voting via a web-embedded application"[242] (Vassil, 2016: 8). In this sense, "the voter applications were reprogrammed by Cybernetica AS in a way in which the application is downloaded from the NEC website as stand-alone program and is not run in the user's browser" (OSCE/ODIHR, 2011b: 11). Secondly, "[a]s of 2011, citizens can also electronically identify themselves with a so called 'Mobile-ID', which requires special mobile phone SIM card with security certificates and two pin codes" (Vassil, 2016: 5). Thus, "voters were given the possibility to use a mobile phone with a specially enabled SIM card to identify him/herself and digitally sign the vote. It was used by less than two per cent of Internet voters" (OSCE/ODIHR, 2011b: 11).

Even if we accept that the legal provisions did not change substantially, it does not mean that the period is free from legal debate. As pointed out by Priit Vinkel, during this period "[a] second broader category of discussions on e-voting have taken place in the Constitutional Chamber of the Supreme Court, following on from specific electoral complaints" (2016: 40). The author points out that "the complaints issued after the 2011 parliamentary elections had a strong influence on the parliamentary debates of 2012" (Vinkel, 2016: 41). In this sense, Vinkel (2016: 41) notes that

> "The principles of equality, secrecy, technical uniformity, procedural soundness and the security of e-voting have been raised in various different complaints […] By 2015, all of the complaints concerning e-voting had been dismissed. However, the complaints issues after the 2011 parliamentary elections had a strong influence on the parliamentary debates of 2012"

Likewise, the OSCE/ODIHR's 2011 report also marked the end of this phase. According to Vinkel, "several key features of the Estonian e-voting system and the regulations were revised as a result of recommendations made" (2016: 41). All in all, both the complaints

[241] Additionally, we have also seen that for the 2011 elections the period of Internet voting was extended from three to seven days.

[242] With this new system, the voting process worked as follows: "[w]hen voting online, citizens download a voting app to their computer and upon request from the system have to first identify themselves using the ID-card and the first pin-code. Next, the system checks whether the voter is eligible to vote in these elections and if the answer is affirmative, displays a list of candidates in their district. No digital signature has thus far been required. However, in order to cast an e-vote, the second pin-code – the signing function – is used to confirm the voter's choice. The latter is the transactional part of the citizen-state communication. When performed correctly, the electronic vote is sent to the server and will be counted at the appropriate time prescribed by the procedures for online voting" (Vassil, 2016: 17).

filled and the OSCE/ODIHR's report seem to have been "the main engine to launch renewed discussions in parliament to review the e-voting regulations and amend the procedures to bring more transparency and introduce additional steps regarding the ability of a citizen to verify their vote was counted correctly" (Vinkel, 2016: 41).

c) The introduction of verifiability and a stabilised used of the method (2012-2015)

As we have seen, the follow-up to the 2011 *Riigikogu* elections started a new phase on the use of remote electronic voting in Estonia. "Until 2011, the electronic voting procedures had only very brief legislative regulations (despite the discussions in 2005)" (Vinkel, 2016: 44). This scenario changed after the 2011 *Riigikogu* elections. As described by Priit Vinkel (2016: 44)

> "After the 2011 general elections, where almost a quarter of all votes were cast electronically, parliament decided to specify the norms of e-voting under electoral law in order to improve the legitimacy and transparency of e-voting […] The parliament established a special working group (Constitutional Committee, 2011) which in addition to detailing procedures, had to propose a solution for raising levels of transparency and accountability with the e-voting system."

One of the changes was related to the organisation of the remote electronic voting. In this sense, "[i]n 2012, the parliament adopted several amendments to the electoral law, stating that a new electoral committee – the Electronic Voting Committee – was to be created for the technical organization of I-voting" (Vinkel and Krimmer, 2016: 182). "The first elections where this committee was in charge were the 2013 local elections" (Vinkel, 2016: 45). Another change was related to the technology used. In this sense, "[t]he most significant change of the law was the statement that, from 2015 onwards, voters had to have the possibility to verify that their vote was received, stored at the central server of the elections and reflected the choice of the voter correctly" (Vinkel, 2016: 45). According to Priit Vinkel (2016: 44-45), "the technical community involved by the Estonian National Electoral Committee (NEC) in the discussions about the security and transparency of e-voting, came to the conclusion that a mechanism for the voter to verify their vote was counted correctly was needed".

For Mihkel Solvak, "the main aim of introducing verifiability in Estonia was to detect possible large scale attacks on the system […] by encouraging individual voters to verify their e-vote with a separate smart device from the device used to cast their e-vote" (2016: 127-128). Thus, "[a]dditional changes in 2012 introduced the first steps for individual vote verification with the Estonian system […] and therefore opened new possibilities to minimize the threats to personal computers" (Vinkel, 2016: 42). With this new system, "[v]erification is done using a separate smart device (mobile phone or tablet), which reads a code displayed on the screen upon the completion of voting and temporarily displays the voter's choice" (OSCE/ODIHR, 2015a: 6). Lastly, "[o]ne new chapter describes the general principles and procedures for Internet voting" (OSCE/ODIHR, 2015a: 6). Additionally, "[a]mendments in 2014 prescribe obligatory testing and more stringent requirements for auditing of the Internet voting system" (OSCE/ODIHR, 2015a: 7).

Thus, starting with the local elections of 2013, "Estonia introduced the feature of individual vote verification to the e-voting. This gave individual voters the ability to verify whether their e-vote was: 1) cast-as-intended; [and] 2) recorded-as-cast" (Solvak, 2016: 127). According to Mihkel Solvak (2016: 127),

> "Vote verifiability is a crucial element in ensuring a so called end-to-end (E2E) verifiable voting system. E2E verifiable systems add another layer of security and should ensure higher integrity of the voting process. The definition of an E2E verifiable voting system is quite strict […] and the verification procedure introduced in Estonia as of 2013 does not yet meet that of a fully implemented E2E system; it does however cover a central element of it, namely giving individual voters the possibility to check if their vote was cast and counted as intended."

Indeed, the verifiability mechanisms first introduced in 2013 allowed "voters to voter to confirm that their online vote was cast as intended and recorded on the ballot storage server as cast […] However, the system does not allow for end-to-end verification" (OSCE/ODIHR, 2015b: 1). Individual verifiability was "[p]iloted during the local elections of 2013 and fully implemented from the 2014 European elections onward" (Vassil, 2016: 10). According to this author,

> "vote verification enables Estonian e-voters to verify whether their vote was cast as intended. Effectively, vote verification makes it possible to detect whether the computer is infected with malware that changes the e-vote of has blocked an e-vote. The process of vote verification involves the usage of a smart device (a smartphone or a tablet) equipped with a camera and internet connection. After the voting process a QR-code id displayed in the voting application and using a smartphone with a QR-code reader a vote verification app allows the voter to verify their vote."

During the elections to the European Parliament of 2014, about 4% of all e-voters verified their vote (Vassil, 2016: 10). "The number of e-voters who verified their vote has grown throughout the years, reaching 4,7% for the 2015 elections"[243] (Vinkel, 2016: 46).

Since the introduction of individual verifiability, "[t]he discussion about transparency and verifiability in a remote electronic voting system has clearly defined the general discussions on e-voting" (Vinkel, 2016: 46). In this sense, the OSCE/ODIHR first observed this new feature during the 2015 *Rigiikogu* elections[244]. The Needs Assessment Mission acknowledged the amendments to the Election Act "to further detail provisions pertaining to Internet voting" (OSCE/ODIHR, 2015a: 1) and concluded that "these changes partly addressed previous OSCE/ODIHR recommendations" (OSCE/ODIHR, 2015a: 1). Notwithstanding, they also recommended the deployment of an Election Expert Team, which observed the 1 March 2015 parliamentary elections from 15 February to 5 March (OSCE/ODIHR, 2015b: 2). Their Final Report provides a detailed description of the decryption and counting process that we reproduce here as it will serves us to analyse how the principle of secret suffrage is observed (OSCE/ODIHR, 2015b. 6)):

> "Internet votes were counted in a public counting ceremony on the evening of election day. First, encrypted votes were transferred to an offline counting server. Votes were then sorted by constituency and voters' digital signatures were removed and stored separately to preserve vote secrecy. Subsequently, encrypted votes were decrypted

[243] According to Heiberg, Krips, and Willemson (2020: 89), this number of voters who verify their vote has not changed substantially in recent elections, and "[c]urrently, the rate of verifiers is about 4,5%."

[244] For the 2015 *Riigikogu* elections, "a total of 176,329 voters (10.6 per cent of all registered voters) cast their ballots via the Internet, which amounted to 30.5 per [cent] of all votes cast" (OSCE/ODIHR, 2015b: 4). It is also important to highlight that "[b]y June 2015, digital ID-cards had been used about 353 million times for personal identification and 222 million times for digital signatures" (Vassil, 2016: 21).

> using the decryption key and counted […] The next day, the EVC performed successful checks of the server logs files in order to verify the consistency of the counting process."

According to the Election Expert Team, "[t]hese logs files contain information about which electronic ballots were excluded as required and which were counted. This process can be compared to reconciliation of ballots cast with those counted in different categories" (OSCE/ODIHR, 2015b: 6). The report also noted that "[t]he system does not allow for verification that all electronic ballots were counted exactly as recorded in the ballot storage server without jeopardizing vote secrecy" [emphasis added] (OSCE/ODIHR, 2015b: 6), but also noticed that "[t]he EVC is aware of possible technical solutions to this problem, including end-to-end verifiability, which would not jeopardize the secrecy of the vote, and states publicly that it is considering such improvements of the system" [emphasis added] (OSCE/ODIHR, 2015b: 6). Those plans would be put in place already for the 2017 local municipal elections (Vinkel and Krimmer, 2016: 184)

"The OSCE/ODIHR election specialists' report […] emphasises the need for added verifiability, and the electronic voting committee is actively seeking contributions from the ICT community (Electronic Voting Committee, 2015) to suggest new solutions" (Vinkel, 2016: 46). According to Vinkel (2016: 45),

> "The main lesson that can be learnt from this period is that together with the development of the technical environment, legal regulations also had to kept up. As Drechsler and Kostakis (2015) argue, technology is constantly evolving, but the law is generally not updated immediately. This allows for a process of consideration as to which technologies are desirable and sustainable for implementation. Verifiability was not implemented when it was available (years before the actual introduction), but only when there was a concrete need owing to the recent discussion that took place in the country."

d) Remote electronic voting in Estonia: current landscape (2016-today)

"In 2017, the Internet voting system underwent considerable structural and managerial modifications" (OSCE/ODIHR, 2019a: 6). For example, "the authorities have introduced universal verifiability through mathematical checks of the process, including vote decryption and results tabulation, by an appointed data auditor" (OSCE/ODIHR, 2019a: 7). At the organisational level, the election administration was restructured, the Electronic Voting Committee was also eliminated and those "[t]hose responsibilities that were not outsourced were transferred to an e-voting unit in the SEO" (OSCE/ODIHR, 2019a:)

The OSCE/ODIHR observed, for the fourth time, the use of remote electronic voting during the 2019 *Riigikogu* elections. For these elections, "[i]n total, 247,232 Internet votes were collected[245]" (OSCE/ODIDHR, 2019b: 9) meaning that "43.8 per cent of all votes cast were online, marking a significant increase from 31.7 per cent in the 2017 local elections" (OSCE/ODIDHR, 2019b: 7). The NAM deployed from 13 to 15 November 2018 noted that "[t]he legal framework has not changed substantially since the last parliamentary elections, but was since amended on several occasions to facilitate structural changes within the election administration and to further detail provisions on Internet voting" (OSCE/ODIHR, 2019a: 1). The Mission noted additional amendments to the *Riigikogu*

[245] According to the OSCE/ODIHR's Election Expert Team, "704 voters (0.28 per cent of all voters) cast more than one vote [and] Internet votes of 191 voters, who invalidated their e-votes by casting a paper vote during advance voting, were removes during the ballot decryption procedure" (OSCE/ODIHR, 2019b: 9)

Election Act, "to facilitate structural changes within the election administration and to further detail provisions pertaining to Internet voting" (OSCE/ODIHR, 2019a: 4). The Mission also highlighted that the management of the vote collection process had been "outsourced [sic] by the NEC [to the state Information System Authority (RIA)] owing to enhanced integrity and audit components" (OSCE/ODIHR, 2019a: 4) and acknowledged that "[t]his change represents a shift in the role of the election administration from one of direct and technical towards more process management"[246] (OSCE/ODIHR, 2019a: 4).

In view of the amendments, the OSCE/ODIHR Needs Assessment Mission recommended the deployment of an Election Expert Team. The Team noted that "the system's integrity and secrecy properties were strengthened"[247] (OSCE/ODIHR, 2019b: 1). At the same time, they also noted that "Internet voting is no longer considered an experiment by the authorities, but as part of a regular framework" (OSCE/ODIHR, 2019b: 7) Notwithstanding, the Team also highlighted that "the system is not software independent, meaning that errors in its components may cause undetected errors in the election results, and it is potentially vulnerable to internal attacks and to allegations of cyber attacks, which may affect public confidence" (OSCE/ODIHR, 2019b: 1).

The observers also found out that an internal attacked could break the vote secrecy of any voter who published an image of their QR code for individual verifiability online and that "updates to the source code were made as recently as three days before election day and well after Internet voting commenced"[248] (OSCE/ODIHR, 2019b: 8). Additionally, and while the OSCE/ODIHR did not "audit other critical operations, most notably the correct transmission of the final aggregation of the decrypted Internet votes" (OSCE/ODIHR, 2019b: 8), they noted that "[t]he Supreme Court considered two post-election appeals against NEC decisions related to Internet voting. While the appeals were rejected, the Court recognized the need for more clear procedures and called for a legal clarification of rules on the implementation of Internet voting, in particular regarding counting and mixing of electronic ballots" (OSCE/ODIHR, 2019b: 9).

Following the elections, "the debate about Internet voting security intensified again in Estonia after a new political coalition was formed. The Minister of Foreign Trade and Information Technology called together a committee that produced a list of open action items to potentially work on" (Heiberg, Kris and Willemson, 2020: 82). According to Arne Koitmäe, Jan Willemson, and Priit Vinkel "the popularity of i-voting in Estonia has initiated debate over 1) how freedom of vote and vote secrecy are guaranteed for Internet voting,

[246] Lastly, the NAM also reports that "[p]otential security vulnerabilities [were] identified with digital ID cards in 2017" (OSCE/ODIHR, 2019a: 6). At the same time, is stresses the "[s]wift response by the authorities to implement a solution and the continued trust in the use of e-services, including internet voting" (OSCE/ODIHR, 2019a: 6).

[247] The same sentence continues "and individual vote verification was introduced" (OSCE/ODIHR, 2019b: 1). This may be a typo since, as we have already seen, individual verifiability had already been available in the previous parliamentary elections and the new verifiability features to be assessed in this election were the ones related to universal verifiability.

[248] It is important to highlight that the risks of such an attack are mitigated by the option to cancel a vote cast electronically casting a last vote by paper. This can be done even if the last electronic vote is cast at the last minute, because "the i-voting period currently ends two hours before the advance paper voting period" (Heiberg, Krips and Willemson, 2020: 91). As of 2021, voters will be also able to cancel any vote cast electronically by voting on paper on election day, making this attack even more unfeasible.

and 2) what measures would increase general trust in the system" (2021: 142). Another recent debate is whether voters should be able to vote from their smartphones as well[249]. On this issue, "a separate analysis effort was initiated by the State Information System Authority and State Electoral Office" (Heiberg, Krips and Willemson, 2020: 83). The authors of the report advised against a browser-based voting application, which could be supported in smartphone[250].

II. INTERNATIONAL AND EUROPEAN STANDARDS ON REMOTE ELECTRONIC VOTING

As rightly pointed out by Sutton Meagher (2009: 361) "[t]here are no binding international laws governing Internet elections". Of course, it does not mean that there are no international standards on the use of remote electronic voting. First, "Internet elections must adhere to the same requirements of secret ballot, equal suffrage, and auditability that are provided in the ICCPR for normal [sic] ballot elections"[251] (Meagher, 2009: 361) To these, we should add the principles of free and universal suffrage as well, which Meagher does not seem to acknowledge. Therefore, even if general standards on the conduct of democratic elections may have been developed with paper-based elections in mind, their principles should also apply to e-enabled elections.

Second, there exist indeed international standards that, while may be non-binding, offer importance guidance on the democratic conduct of e-enabled elections. Such standards include, first and foremost, the Council of Europe's Recommendations on e-voting, first adopted in 2004 and later updated in 2017. Additionally, the OSCE/ODIHR has also developed a methodology for the observation of new voting technologies[252] that helps in understanding how the introduction of digital technology for the casting and the counting of votes can comply with electoral commitments. In contrast to the Council of Europe's Recommendations, however, the work of the OSCE/ODIHR is not aimed at providing an e-voting regulation[253] (Driza Maurer, 2014: 112). Lastly, there are a whole set of

[249] As we have seen, to date it is only possible to vote from personal computers, since voters need to install a specific programme which only runs on Windows, macOS or and Linux in order to vote (Buldas et al., 2020: 6.).

[250] And which is, precisely, the voting application used in the two other case studies we have analyse: both for Scytl's solution in Switzerland and France as well as in Geneva's remote electronic voting system.

[251] It is important to notice that, regardless of this acknowledgement, Meagher herself pointed out that "[a]s states venture into the new territory of Internet elections, it will become increasingly more important for the international community to establish procedural and technical standard for Internet elections" and called for "[t]he creation of an ICCPR Optional Protocol containing standards for Internet voting [that] could resolve this problem" (2008: 381). In her opinion "[a]n Optional Protocol would assist election observers and governments by outlining criteria with which a state must abide" (Meagher, 2008: 381).

[252] In addition to the OSCE/ODIHR, International IDEA, the Carter Center, the Organisation of American States, and the National Democratic Institute for International Affairs have as well "approached the issue of standards for electronic voting and counting technologies from the perspective of election observers" (Driza Maurer, 2014: 112). Driza Maurer also notes that "IFES proposes a step-by-step approach to the introduction of e-voting, including legal considerations. IFES, IDEA, or the EU discuss key principles that should inform the introduction of e-voting more generally of technology in elections" (2014: 112).

[253] According to Essex and Goodman (2020: 168), the Recommendations of the Council of Europe "are the only intergovernmental documents that focus on regulation and standardization of voting

technological standards that may either define what a remote electronic voting system is supposed to do or how some of its building blocks (such as encryption, digital signatures or key-sharing mechanisms) are to be implemented. While the later standards have not been developed having remote electronic voting as one of their applications in mind, they are key to ensure that these systems comply with the principles for democratic elections.

In this section we explore some of these standards. First, we focus on the Council of Europe's recommendations on e-voting, which remain to date the only legal standard on the matter. Following, we delve into the opinions of the Venice Commission and the OSCE/ODIHR handbook on the observation of new voting technologies, which may also detail important aspects on the introduction of (remote) electronic voting technologies. Lastly, we explore some technological standards, as well as data protection regulations, as they are also considered when introducing remote electronic voting.

1. Remote electronic voting: international standards

At the international level, two key organisations in the field of electoral rights have committed to the development of standards in the field of electronic voting and provided a platform for the exchange of experiences between states: the Council of Europe, and the OSCE/ODIHR. While their standards are not binding for the states, most have decided to follow them when regulating internet voting at the domestic level. For instance, Switzerland considered that they should draw inspirations from them as widely as possible for the reorganisation of their legal bases or justify any departure from them (Swiss Federal Council, 2013a: 127).

a) The Council of Europe's recommendations on e-voting

To date, the Council of Europe's standards on electronic voting remain the only intergovernmental source in the field. While not binding, the Recommendation has been voluntarily adopted by several member States of the Council of Europe, including Switzerland (Swiss Federal Council, 2013a: 46) and Norway[254] (Barrat, Goldsmith and Turner, 2012; Stein and Wenda, 2014: 106). Several national high courts have also referred to it. That is the case, as we have seen, of the Supreme Court of Estonia, which in its Constitutional Judgement 3-4-1-13-05 acknowledged that (2005):

> "[a]lthough the Recommendation of the Council of Europe is not a legally binding document, it summarises the understanding of the democratic states of Europe of the conformity of electronic voting with the election principles inherent to democratic states, and is thus an appropriate tool for interpreting the [Estonian] Constitution."

technologies. All other international documents can be characterized as guidelines, efforts to formalize procedures, or provide advice regarding good practices". More importantly, these authors highlight that "[e]ven compared to domestic documents, the recommendations are unique because of the broad framework they present" (Essex and Goodman, 2020: 168

[254] Driza Maurer concludes that as of 2014 Norway had been "the only country to have given Rec(2004)11 recommendations (with few exceptions however) the status of legal basis regulating both 2011 and 2013 internet voting trials. However some of the recommendations were excluded and Norway also introduced verification mechanisms which are not deal with in the Rec(2004)11 such as the return codes" (2014: 112).

In other cases, such as in Belgium, the Recommendations of the Council of Europe have been used as a benchmark when evaluating e-voting (Stein and Wenda, 2014: 106). Some authors thus argue that the Recommendation "has been the most relevant international document and reference regarding e-voting"[255] (Stein and Wenda, 2014: 105).

The origins of the Recommendation date back to the early 2000. At the initiative of some member states, the Committee of Ministers set up a group of experts and adopted, on 30 September 2004, a recommendation on legal, operational and technical requirements for electronic voting, Rec(2004)11. According to Robert Stein and Gregor Wenda (2014: 105),

> "[a] number of international institutions and fora could have dealt with the new phenomenon of electronic voting but it was the Council of Europe which apparently developed the strongest interest and formed a 'multidisciplinary Ad Hoc Group of Specialists on legal, operational and technical standards for e-enabled voting' within the framework of its 2002-2004 Integrated Project 'Making democratic institutions work' (IP1)."

The Council of Europe thus became the first international organisation to adopt a recommendation on the fundamental principles governing the resort to electronic voting (Swiss Federal Council, 2006: 5239; 2013a: 45). Drawing from various regulations governing elections and voting in the Council of Europe's member States[256], the recommendation only set minimum standards. The 2004 recommendation stressed that "e-voting shall respect all the principles for democratic elections and referendums" (Council of Europe, 2004: i) and "shall be as reliable and secure as democratic elections and referendums which do not involve the use of electronic means" (Council of Europe, 2004: i). On the opinion of the Swiss Federal Council (2006: 5239; 2013: 46), the recommendation attached particular importance to a high level of security for electronic voting, to the fact that electronic voting is an additional and complementary voting channel, and to the neutrality of the technological tools.

Paragraph v. of the recommendation contained follow-up provisions, stipulating "a first review after two years in order to provide the Council of Europe with a basis for possible further action on e-voting" (Council of Europe, 2004: v). The first of these review meetings took place in Strasbourg on 23 and 24 November 2006 (Stein and Wenda, 2014: 105). Two more meeting followed in 2008 and 2010. Therefore, this provision meant in practice that the recommendation would be reviewed periodically after its adoption to assess its impact on member States and potentially be updated. Following the third review meeting, additional guidelines[257] were adopted regarding the certification of remote electronic voting systems (Council of Europe, 2010a) and the transparency of e-enabled elections (Council of Europe, 2010b), as well as an E-voting handbook on the "key steps in the implementation of e-enabled elections" (Stein and Wenda, 2014: 105). "A fourth review

[255] While others, more cautiously, just refer to it as "one of the first regulatory efforts in this area and so far the only one at the international level" (Driza Maurer, 2014: 111). Three years later, Driza Maurer noted that "[t]he Council of Europe is [still] the only international organization to have issued recommendations on the regulation of the use of e-voting" (2017: 146).

[256] For instance, articles 27a to 27q of the Swiss Ordinance on Political Rights, according to the Swiss Federal Council (2006: 5241).

[257] According to Ardita Driza Maurer (2014: 111) the guidelines have lower status "and are meant to complete the recommendation on these issues", that is: certification and transparency, which were dealt with as well in the 2004 Recommendation.

meeting took place in Lochau near Bregenz, Austria, on 11 July 2012" (Stein and Wenda, 2014: 105).

Ten years after its adoption, however, "voices in favour of a formal updated […] gained strength"[258] (Stein and Wenda, 2014: 105). Therefore, "[f]ollowing an informal experts' meeting in Vienna on 19 December 2013, the Committee of Ministers was confronted with the suggestion to formally update the Recommendation in order to keep up with the latest technical, legal and political developments" (Stein and Wenda, 2014: 105). It was argued that "[n]ew technological developments and concepts such as in the context of the verifiability of votes, and conclusions from studies and reports, for instance regarding certification, called for addenda or adaptations" (Stein and Wenda, 2014: 107).

A study commissioned to Ardita Driza Maurer[259] (2015) which was based on a survey among election administrations in the member states of the Council of Europe identified the following items within the scope of the update: the definition of e-voting, the responsibilities of Electoral Management Bodies, the notion of risk, the structure of the Recommendation, and the categories of requirements. New standards were drafted and approved by an Ad hoc Committee of Experts on Legal, Operational and Technical Standards for e-voting (CAHVE) in November 2016 (Driza Maurer, 2017: 147). The Committee of Ministers of the Council of Europe finally adopted the updated standards as Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting on 14 June 2017.

Regarding the definition of e-voting, the Recommendations (2004)11 "defined e-voting as an e-election or e-referendum that involves the use of electronic means at least in the casting of the vote, covering both e-voting in controlled (e.g. voting machines in polling stations) and in uncontrolled environments (e.g. internet voting from a private computer)" (Driza Maurer, 2004: 111). The current definition has been broadened to include counting machines as well. In principle, all standards would apply to the three technologies[260].

[258] For instance, in their evaluation of the Norwegian experience against the 2004 Recommendation, Jordi Barrat i Esteve and Ben Goldsmith (2012: 8) concluded that:

> "The recommendations [sic] do not build on existing public international law […] say little on the legal basis, trying, on the contrary, to cover every possible situation in a technically neutral way. The consequence is sometime vague wording that makes the enforcement of the recommendation more difficult than it should be."

Additionally, Ardita Driza Maurer (2014: 113) also takes notes of criticism coming from Douglas Jones (2004), from Margaret McGaley and J. Paul Gibson (2006), and from Andreas Ehringfeld et al. (2010). In the case of Douglas Jones, the author warned that the draft Recommendation "suffer from some serious deficiencies" (2004: 1), with special focus on how it compared the security and reliability of electronic and non-electronic voting systems.

[259] In 2014 and 2015, the author of this PhD had the opportunity to be directly involved in the update of the Council of Europe's Recommendation and in the drafting of this report as an employee of the organisation.

[260] According to Ardita Driza Maurer (2017: 152), "[u]nless specific mention, standards apply to all forms of e-voting. Standards which are specific only to one or to some form mention this". However, this is not always the case. For instance, standard No. 5 on the display of official information "across and within and across voting channels" (Council of Europe, 2017a) in principle would not apply to e-counting, since in "the electronic scanning and counting of paper ballots" (Driza Maurer, 2017: 153) no voting information is displayed across channels (there is only one channel, which is paper based). Yet, this is not mentioned in the Appendix I, neither in the Explanatory Memorandum nor in the Guidelines (although the examples in the Guidelines are focused on e-voting only). Therefore, and while Ardita Driza Maurer had previously pointed out that "[r]equirements and standards in the

Regarding its structure, the current Recommendation consists of three documents[261]: "the Recommendation, which outlines central aspects of e-voting; an Explanatory Memorandum; and guidelines to inform the implementation of provisions in the Recommendation" (Essex and Goodman, 2020: 169). It is also important to highlight that the Recommendation is, in turn, divided into the recommendation *as such*, and two Appendixes: one detailing 49 standards on universal, equal, free, and secret suffrage, regulatory and organisational requirements, transparency and observation, etc. and a second one with a glossary of terms. In terms of structure and principles, the updated Recommendation follows the Venice Commission's *Code of Good Practice in Electoral Matters* (see chapter 2 *supra*), but "address[es] only those matters (principles and conditions for implementing them) that require specific measures to be taken when e-voting is introduced" (Driza Maurer, 2017: 152).

Notwithstanding, possibly the most important change in the updated recommendation refers to its approach towards e-voting. While the 2004 Recommendation stated that "[e]-voting shall be as reliable and secure as democratic elections and referendums which do not involve the use of electronic means" [emphasis added] (Council of Europe, 2004a: i), the updated recommendation has dropped this previous comparison (Driza Maurer, 2017: 154). The benchmark in Rec(2017)5 "is [the] respect for all principles of democratic elections and referendums"[262] (Driza Maurer, 2017: 154). In practice, it means that

Recommendation should clearly indicate to which of the two types of e-voting they apply" (2014: 214), the updated recommendation still not offers such indication and it is thus still up to the national authorities to make such assessment in most cases (with the added complexity that the current Recommendation also includes provisions that should apply to electronic counting, even when votes are cast on paper).

[261] This three-tiered structure allows for distinguishing between principles, recommendations, standards, and requirements. Principles come from various international legal instruments and not from the Recommendation as such (see chapter 2 *supra*). Recommendations are contained in the Recommendation (paragraphs i. to vi.). Standard are included in the Appendix I to the Rec(2017)5 (Driza Maurer, 2017: 150) and can be distinguished between "legal standards" and "technical standards" (Driza Maurer, 2017: 152). Legal standards "set objectives that e-voting shall fulfil to conform to the principles of democratic elections" (Driza Maurer, 2017: 152), while technical standards "refer to a technical norm, usually in the form of a formal document that established uniform engineering or technical criteria, methods, processes and practices" (Driza Maurer, 2017: 152). According to Ardita Driza Maurer, "the Guidelines […] offer instructions on the implementation of the standards" (2017: 152). Lastly, requirements "are defined […] as a singular, documented need of what a particular product or service should be performed" (Driza Maurer, 2017: 152). According to Standard No. 36, it is member States who "shall developed technical, evaluation and certification requirements" (Council of Europe, 2017a). According to Ardita Driza Maurer, "[r]equirements for a specific e-voting solution to be used in a given context, must be defined with respect to that specific solution and context […] by definition, e-voting detailed requirements cannot be decided in an international document like the Recommendation" (2017: 152). Since they come from different legal sources (principles from international conventions and treaties, national constitutions and formal law; standards from international recommendations and soft-law, and from national material law; and requirements from lower level regulations), there is in principle a "hierarchy between principles (top), standards (middle) and requirements (bottom of the pyramid)" (Driza Maurer, 2017: 152-153).

[262] More specifically, the Preamble to the Recommendation reads that "the right to vote lies at the foundations of democracy, and […] consequently, all voting channels, including e-voting, shall comply with the principles of democratic elections and referendums" (Council of Europe, 2017a). Following, recommendation i. stresses that "domestic legislation and practice in the field of e-voting […] respect all the principles of democratic elections and referendums" (Council of Europe, 2017a). The Explanatory Memorandum is much more detailed when it comes to specify how (remote)

"standards should be derived directly from the applicable principles" (Driza Maurer, 2017: 154). It goes without saying that it includes the principle of secret suffrage. However, we are of the opinion that not sufficient effort has been put into directly deriving the standards in Appendix I.IV of the Recommendation from the principle of secret suffrage. This aspect will be further addressed (and justified) in the next chapter.

Another important innovation is that the Recommendation also introduces the notion of risk. In this sense, "Recommendation ii. stresses the need to assess risks, namely those specific to e-voting and to adopt appropriate measure to counter them"[263] (Driza Maurer, 2017: 154). These two aspects are of utmost importance for our research because, in what follows, we will be basing our analysis of secret suffrage and remote electronic voting on them[264].

The new standards have been welcomed both by members and non-Members states of the Council of Europe. For example, in the explanatory report to the draft law amending the Federal Act on Political Rights, the Swiss Federal Chancellery referenced the updated Recommendation of the Council of Europe on e-voting (Swiss Federal Chancellery, 2018c: 22). They argued that the draft legislation was in line with the provisions of the updated Recommendation on verifiability, certification, and risk management. Elsewhere, Essex and Goodman (2020) have been quick to assess to what extent the Council of Europe's approach to regulation could work in Canada[265]. More importantly, this experience shows that, as noted by Ardita Driza Maurer, international "[s]tandards [one e-voting] have both

electronic voting channels are expected to comply with the principles of the European Electoral Heritage (Council of Europe, 2017b: para. 16-17):

> "16. E-voting, as any other voting method, must respect the principles for democratic elections and referendums. The rapid changes in its underlying technology present a challenge to such conformity as they introduce new opportunities and threats in an on-going manner. These must be managed appropriately. At the end, it is essential that the principles are not undermined by the introduction of electronically backed solutions in vote casting and/or counting procedures or by their evolution.
>
> 17. Accordingly, e-voting systems must be designed and operated in order to ensure constantly that the principles are respected."

[263] Risks are dealt with in Recommendation ii. This recommendation reads that "domestic legislation and practice in the field of e-voting […] assess and counter risks by appropriate measures, in particular as regards those risks which are specific to the e-voting channel" [emphasis added] (Council of Europe, 2017a). Likewise, the Explanatory Memorandum to the Recommendation further details that (Council of Europe, 2017b: para. 17)

> "Member States should dedicate special attention to the risks inherent to the e-voting method chosen. E-voting specific risks need to be monitored permanently and appropriate countermeasures introduced whenever necessary. Given the rapid pace of change in the field of new technologies, member States are advised to introduce a risk management policy framework."

[264] First, in chapter 4 we will assess the standards on secret suffrage in the Recommendation against the definition of secret suffrage offered in chapter 2 *supra* (chapter 4.I) and evaluate compliance both in international standards and in the national experiences (chapter 4.II). Second, in chapter 5 we will be identifying specifics risks to secret suffrage in remote electronic voting, including both computer and human threats. To do so, we will first challenge on-going approaches based on analogies to paper-based voting channels (that is, the comparison that e-voting should be "as reliable and secure as" paper-based options) (chapter 5.I). Following, we will consider the need to balance and for trade-offs between different principles, with special focus on free suffrage and for transparency and observation (chapter 5, sections II to IV).

[265] However, these authors conclude that "[w]hile the breadth of this approach makes it widely applicable, that same leeway makes it more challenging to hold technology vendors accountable. It also lacks the specific guidance […] needed for vetting vendors or managing issues associated with unsupervised voting" [emphasis added] (Essex and Goodman, 2020: 170).

influenced developments in member States and have been influenced by them" (2017: 147).

b) The opinions of the Venice Commission on electronic voting

The Venice Commission has also studied the legality of remote electronic voting. In the framework of the *Code of Good Practice in Electoral Matters*, the Venice Commission has analysed electronic voting in the light of the way it preserves fundamental democratic rights[266]. The Code notes that electronic voting should not be adopted unless it can be organised with safety and reliably (Venice Commission, 2002a: 3.2.iii). More specifically, voters should specifically be able to obtain confirmation of their vote and to correct it (Venice Commission, 2002b: para. 42) and the transparency of the system must be guaranteed (Venice Commission, 2002b: para. 44).

In 2004, the Venice Commission adopted a report on the compatibility of remote electronic voting with the standards of the Council of Europe (also known as Greenwares report) (Venice Commission, 2004). The report addresses whether remote electronic voting is in line with the provisions of the European Convention on Human Rights (art. 3 to the additional Protocol) and the Code of Good Practice on Electoral Matters). After analysing the practices in some member States, the report concludes that (Venice Commission, 2004: para. 69-70):

> "69. In conclusion, remote voting is compatible with the Council of Europe's standards, provided that certain preventative measures are observed in the procedures for either non-supervised postal voting or electronic voting.
>
> 70. In addition, for non-supervised e-enabled voting, technical standards must overcome different threats to those which exist for postal voting. This form of voting must only be accepted if it is secure and reliable. In particular, the elector must be able to obtain confirmation of his or her vote and, if necessary, correct it without the secrecy of the ballot being in any way violated. The system's transparency must be guaranteed. Insofar as an e-enabled voting system meets these conditions, it is compatible with the European standards on electoral matters, and in particular with Article 3 of Protocol 1 to the European Convention on Human Rights."

c) From the Helsinki Final Act and the OSCE Human Dimension Commitments to the OSCE/ODIHR's handbook on the observation of new voting technologies

As it has been seen already, the OSCE/ODIHR have a leading role in electoral observation and evaluation in the organisation's 57 participating States (Swiss Federal Council, 2013a: 46). The organisation has observed the resort to internet voting in our three case studies on the occasion of legislative elections: in Estonia (for the parliamentary elections in 2007, 2011, 2015 and 2019), in Switzerland (in 2011 and 2015) and in France (for the legislative elections of 2012). Additionally, the organisation also conducted NAM ahead of the 2017 legislative elections in France and the 2019 federal elections in Switzerland (even if the possibility to vote online was finally not offered in these contests). They have also observed

[266] According to the Swiss Federal Council, the Venice Commission seems to assess positively the contribution of online voting towards the fulfilment of the right to vote, and especially for those voters who are abroad (2013a: 46).

the resort to internet voting in Norway in 2011, in the Netherlands in 2006, as well as the plans for introducing it in Lithuania in 2020, to name just a few examples. Since we use them as a reference, it is important to understand their methodology. At the same time, by identifying the aspects that need to be observed when electoral technologies are used, the OSCE/ODIHR also shows which are the values that a democratic election must meet (i.e., the electoral principles) and the mechanisms that may help contribute to complying with those values.

In July 2004 and April 2005, the OSCE/ODIHR organised two meeting in Vienna on the adoption and the observation of election technologies (Swiss Federal Council, 2006: 5239). According to the OSCE/ODIHR, (remote) electronic voting has to respect the fundamental principles for the organisation of democratic elections, as well as the international norms on this subject. It should offer the same guarantees in terms of transparency, responsibility and public trust than the traditional voting methods (OSCE/ODIHR, 2010). Some of the key aspects observed by the OSCE/ODIHR are related to (Swiss Federal Council, 2013a: 47):

- It is recommended that the legal framework takes into account in a detailed manner all the phases of Internet voting;
- The responsibility to certify the systems, to digitally sign the final version of the software and to publish an evaluation report must be assigned to an independent public body. The certification criteria must be clear, agreed upon in written format, and testable. They should over the following aspects: security, transparency, robustness, user friendliness and the protection of the secrecy of the vote;
- The bodies responsible for the organisation of the elections must reinforces their internal capabilities in the domain to be able to better monitor Internet voting;
- The reports about the tests of the system should be published online to enhance transparency and the verifiability of the process; and
- A mechanism allowing voters to detect whether they vote has been modified by malware should be envisaged.

In 2010, the OSCE/ODIHR "appointed and expert for the observation of New Voting Technologies for the first time […] and developed a 'Handbook for the Observation of New Voting Technologies' in 2013" (Stein and Wenda, 2014: 105). The handbook acknowledges that the use of election technologies "poses certain challenges to election technologies [and] are often implemented in a manner that makes direct physical observation of some important procedures difficult" (OSCE/ODIHR, 2014: 1). In this context, the handbook aims to "provide basic guidance to all ODIHR Election Observation Missions (EOMs) on how to observe the use of NVT [New Voting Technologies] in electoral processes" (OSCE/ODIHR, 2014: 1). It is worth mentioning that the scope of his handbook is quite broad, since by NVT the OSCE/ODIHR understand electronic voting machines, ballot scanners, as well as internet voting[267] (OSCE/ODIHR, 2014: 1).

[267] The actual definition of NVT is "the use of information and communications technologies (ICT) applied to the casting and the counting of votes" (OSCE/ODIHR, 2014: 4). While this definition may seem to convey that a new voting technology must rely on ICT for both the casting and counting the votes, the OSCE/ODIHR handbook also includes ballot scanners among the technologies that can be observed, which in fact only count the votes.

Overall, it can be argued that the assumption behind the OSCE/ODIHR's methodology for observing voting technologies is the same assumption that guides this research: that "NVT systems are intended to fulfil the same functions as paper-based or mechanical systems and must, therefore, meet the same standards that apply to these systems" (OSCE/ODIHR, 2014: 8). In the case of the OSCE/ODIHR, those standards are the principles for democratic elections that we have already identified in chapter 2, namely: that "the voting process required the exercise of universal, direct, equal, and secret suffrage through the casting, counting and tabulation of ballots in an honest, transparent, and accountable manner" (OSCE/ODIHR, 2014: 8). The Handbook also references the Recommendation of the Council of Europe (at that time, the one from 2004) as offering some "benchmark" for assessment (OSCE/ODIHR, 2014: 8).

A detailed account of the provisions on secret suffrage in the OSCE/ODIHR's methodology for the observation of NVT is offered in the next chapter.

2. Technological standards on remote electronic voting

Being software artifacts, remote electronic voting systems do not only have to comply with electoral legal requirements, but with technological standards as well. In fact, remote electronic voting regulations sit somewhere in between both legal and technological standards. On example of it can be found in the OSCE/ODIHR's Election Expert Team Final Report to the 2015 Estonian Parliamentary Elections, in which the observers noted that "[t]he system relies on well-established cryptographic methods"[268] (OSCE/ODIHR, 2015b: 3). Which are the standards that define whether a cryptographic method is "well-established"?

So far, we have already identified some of them. For instance, in Switzerland "the VEleS examination of the software […] is based on the Security Functional Requirements (SFR) of the Common Criteria (CC) Protection Profile (PP) for voting systems" (Swiss Federal Chancellery, 2020b: 35). In this regard, "the new Swiss regulation defines a standard set of security requirements taken in part from the BSI Common Criteria Protection Profile for Internet Voting Products and the standards of the Council of Europe" (Puiggalí and Rodríguez-Pérez, 2018: 88).

In turn, many relevant properties of a remote electronic voting system, such as encryption for confidentiality (as we will see with more detail in the next chapter) or digital signatures for eligibility and integrity, depend upon these technological standards. As five experts argued during the Swiss expert dialogue, "[b]uilding-blocks[269] particularly risk

[268] Quite strikingly, notwithstanding, the Team that observed the 2019 *Riigikogu* elections found out instead that "some key properties are not precisely formulated and left open to interpretation by the SEO and the vendor tasked to implement the Internet voting system, including minimal acceptable levels of cryptographic strength, and accountability and verifiability requirements" (OSCE/ODIHR, 2019b: 9).

[269] It is important to highlight that, in the Swiss case, the Annex to VEleS prescribes certain cryptographic standards. For example, according to requirement 3.3.6., "[b]asic cryptographic components may only be used if the key lengths and algorithms correspond to the current standards (e.g. FIPS 143-3, NIST, ECRYPT, ESigA)" (Swiss Federal Chancellery, 2018d: 3.3.6). We will pick up this issue as part of our analysis of how to observe secret suffrage in remote electronic voting, in chapter 5.

being flawed if they are not taken from widely accepted standards and if they are modified" (Swiss Federal Chancellery, 2020b: 5).

This is particularly important for certain building blocks of internet voting protocols, such as mix-nets which, in the opinion of some experts in this same dialogue "are complex and generally defined in research-papers and not taken up by widely accepted standards" (Swiss Federal Chancellery, 2020b: 5). Thus, the experts in the dialogue pointed out that (Swiss Federal Chancellery, 2020b: 9):

> "[i]t is therefore beneficial to use mature technologies, including cryptographic primitives that have been standardised, are widely deployed, and are supported by talent. Absent such maturity, it would be wise to support the creation of standardised cryptographic building blocks and well-maintained crypto libraries supporting internet voting".

In the following chapters, we will address which standards may specifically apply to cryptographic primitives and algorithms for secret suffrage in remote electronic voting.

To conclude, this chapter has allowed to understand the context of the three national experiences as well as the parallel development of international standards for remote electronic voting. Analysing the three national experiences and the international standards on remote electronic voting has allowed to identify the existing legal framework, the actors involved in e-enabled elections, and the main issues in each of the different elections and votes. It has also allowed us to assess the relevance of secret suffrage, which have been important in all three countries: either as concerns, criticism, or being subject to judicial review.

More important, this first analysis has allowed to elicit specific requirements and questions about secret suffrage that are unique to remote electronic voting. Therefore, it is now time to look at these requirements and concerns with more detail.

4. The regulation of secret suffrage and remote electronic voting: an overview of international standards and national experiences

So far, secret suffrage has been identified as one of the five principles that any election must meet to be considered democratic. In chapter 2 it has been concluded that, in Europe, this principle is broadly understood as the right and duty of voters not to have the content of their ballots disclosed (Venice Commission, 2002a: 4). It has been also pointed out that the assumption behind secret suffrage is that it shields voters from pressures they might face if others learned how they had voted. Additionally, the principle of secret suffrage has been broken down into three minimum standards: individuality, confidentiality, and anonymity. Lastly, it has been observed that several mechanisms can be put in place to enforce these standards.

For example, in traditional paper-based elections the impossibility to trace the content of a vote to the identity of the voter who has cast it is ensured by physically breaking the link between the voter and their ballot when the latter is cast into the ballot box. If voters cast their votes in polling stations, confidentiality measures (such as envelopes or ballot booths) may be set in place for voters to be able to make their choices in private and to keep them secret. However, in chapters 1 and 3 we have already pointed out that with the steady introduction of different forms of remote electronic voting since the early 2000 different voices argued that such guarantees cannot be provided when remote electronic technologies are used to cast a vote.

In this chapter we analyse how the introduction of remote electronic voting for public political elections has affected the observance of secret suffrage. There is no doubt that the introduction of digital technologies entails a major change for well-known democratic procedures (Barrat, 2015: 136). This applies to secret suffrage as well. In the case of remote electronic voting, as it "takes place in an uncontrolled environment, the secrecy of the vote could be compromised as voters could potentially disclose for whom they voted by showing their choice as displayed"[270] (OSCE/ODIHR, 2016: 8).

The goal of the current chapter is thus twofold. First, we will assess how secret suffrage is regulated in remote electronic voting, starting with international standards (section I.1). Such an analysis allows us to provide a broader framework for analysing the intertwining of the principle of secret suffrage in remote electronic voting. To do so, we will assess the standards on secret suffrage in the Council of Europe's Recommendation on e-voting as well as in other European standards. Secondly, we address these experiences at the national level. Together, both sections allow us to assess the degree of compliance of both international standards and the national experiences against the three minimum standards of secret suffrage: individuality (II.1), confidentiality (section II.2), and anonymity (section II.3).

[270] Despite the fact that, as the authors of the OSCE/ODIHR report hurry to clarify in a footnote, "[t]his risk also applies to postal voting" (2016: 8).

I. SECRET SUFFRAGE IN REMOTE ELECTRONIC VOTING: INTERNATIONAL STANDARDS AND NATIONAL EXPERIENCES

The goal of the current section is twofold. First, we will assess how secret suffrage is regulated in remote electronic voting, starting with international standards. We will consider the standards on secret suffrage in the Council of Europe's Recommendation on e-voting as well as in other European standards. Secondly, we address these regulations at the national level. For that purpose, we study the three national experiences with remote electronic voting in regard to those issues related to secret suffrage: its legal framework, the reinterpretation of the legal principles, as well as potential concerns that may have been raised.

1. International standards on remote electronic voting and their provisions on secret suffrage

We start this analysis where we left chapter 3: with the assessment of international standards on remote electronic voting, this time focusing on secret suffrage only. Whereas in the historical assessment it was useful to start with national experiences and conclude with the international standards, focusing on secret suffrage demands the opposite approach: first, we look at the international provisions on secret suffrage and remote electronic voting, that are aimed at being common to different national constitutional traditions. Later we will look at the specific implementation of the international provisions in the national experiences.

When it comes to international standards on secret suffrage and remote electronic voting, the Recommendations of the Council of Europe and the methodology of the OSCE/ODIHR for the observation of NVT deserve special attention.

a) The Council of Europe's Recommendation (2017)5 on e-voting

As we have already seen, the Council of Europe's Recommendation Rec(2017)5 on e-voting remains the only international legal standard in the field. For this reason, we will use it as our guiding references when analysing international standards on secret suffrage and remote electronic voting. Since the foundation of the Recommendation is that e-voting should "respect all the principles of democratic elections and referendums", it also translates how electronic voting systems should comply with the principle of secret suffrage.

The Recommendation offers a definition of secret suffrage in its Explanatory Memorandum. Based on the Venice Commission's *Code of Good Practice in Electoral Matters*, secret suffrage is summarised as "the voter has the right to vote secretly as an individual, and the state has the duty to protect that right" [emphasis added] (Council of Europe, 2017b: para. 14). Based on what we have already seen, it is obvious that this definition is not fully aligned with the Venice Commission's interpretation of secret suffrage itself, for which "secret suffrage is not only a right, but also a duty [for voters]" [emphasis added] (Venice Commission, 2002a: 4.a). Therefore, at least to some extent international standards have already evolved to cope with the specificities of remote (electronic) voting channels, and in particular for when voters can cast their vote from unsupervised environments.

The Recommendation then identifies a set of standards to fulfil this principle. In what follows, we analyse these standards separately. First, we address those standards that are directly related to secret suffrage, which in the Recommendation are included in Section IV of Appendix I. Second, we identify some additional references to secret suffrage throughout the Recommendation and its additional documents. Lastly, we also deal briefly on some standards whose focus is not so much on the principle of secret suffrage itself, but rather on how to regulate electoral principles for (remote) electronic voting.

Secret suffrage: Section IV

Section IV in the first Appendix to the Recommendation is entitled secret suffrage and identifies eight standards related to this principle (standards 19 to 26).

The first of these standards provides a general overview about how (remote) electronic voting systems must comply with secret suffrage. In this sense, standard No. 19 reads that "[e]-voting shall be organised in such a way as to ensure that the secrecy of the vote is respected at all stages of the voting procedure" (Council of Europe, 2017a). This is an umbrella provision on secret suffrage that "sets the general requirement for secrecy of the vote which applies throughout the entire procedure" (Council of Europe, 2017b: para. 63). It covers the different dimensions of secret suffrage that we have previously identified. On the one hand, it references "encryption"[271] (Council of Europe, 2017b: para. 64), which is a mean to ensure the confidentiality of the vote. On the other, it also notes "that the votes cast are mixed in the electronic ballot box so the order in which they appear at the counting phase does not allow reconstruction of the order in which they arrived" (Council of Europe, 2017b: para. 64), as a mechanism to ensure anonymity.

Interestingly, the reference to "all stages of the voting procedure" in this standard could seem to exclude, at least *a priori*, the need to ensure the secrecy of the vote after the end of the electoral process. The Explanatory Memorandum confirms this suspicion by further detailing that (Council of Europe, 2017b: para. 63)

> "[t]his standard sets the general requirement for secrecy of the vote which applies throughout the entire procedure: in the pre-voting stage (e.g., transmitting of PINs, or electronic tokens to voters), during the completion of the ballot paper [sic], the casting and transmission of the ballot and during counting and any recounting of the votes".

[271] No definition of encryption is provided in the recommendation. Encryption can be understood as scrambling a piece of information into a form that makes no sense to anyone who observes it (Martin, 2020: 50). More specifically, encryption protects a *plain text* into a sequence of letters which does not make any apparent sense. Encrypted information is referred to as the *ciphertext*, in contrast to the *plaintext* (Martin, 2020: 50-51). According to Martin Keith (2020: 57):

> "The process of providing confidentiality using a cryptographic security mechanism is known as *encryption*. Any mechanism for providing encryption includes an *encryption algorithm*, which defines the basic process by which plaintext is scrambled, and a key, which provides the means of varying the way encryption is performed. The encryption algorithm takes as input both the plaintext and the key, and defines a process that eventually outputs the ciphertext.
>
> The process of reversing encryption is known as *decryption*. In decryption, the ciphertext and the key are input into a *decryption algorithm*, which outputs. The plaintext. The decryption algorithm is the process reversing the effect of the encryption algorithm."

Therefore, neither the Recommendation nor the Explanatory Memorandum[272] seem to consider in this standard the preservation of secret suffrage beyond the length of the electoral process as such.

Following, standard No. 20 provides that "[t]he e-voting system shall process and store, as long as necessary, only the personal data needed for the conduct of the e-election" (Council of Europe, 2017a). Including data protection provisions under the umbrella of secret suffrage is absolutely inadequate. Votes may be considered personal data in certain circumstances, but personal data is much broader than the legal assets protected by secret suffrage[273]. Standards No. 21 and 22 would both fall outside the scope of secret suffrage as well, since they deal with authentication data and voter's registers, respectively, and neither with the votes cast (confidentiality and anonymity) nor with the circumstances in which voters cast them (individuality and confidentiality). Secret suffrage is different from personal data protection, and therefore we will exclude these provisions from our analysis.

Section IV further details four additional standards, on: receipt-freeness (standard No. 23), election fairness (standard No. 24), a new provision about the secrecy of previous choices (standard No. 25), and anonymity (standard No. 26). These standards are indeed all related to secret suffrage and touch upon some of the key concerns about secret suffrage in remote electronic voting.

The first one of these four standards is undoubtedly related to individuality. More specifically, standard No. 23 reads that "[a]n e-voting system shall not provide the voter with proof of the content of the vote cast for use by third parties" (Council of Europe, 2017a). According to the Explanatory Memorandum, "[t]he aim of this standard is to prevent the breach of vote secrecy as well as vote selling" (Council of Europe, 2017b: para. 70). Importantly for our research, this standard has been reviewed, corrected, and clarified from the previous Recommendation (Driza Maurer, 2017: 155). Since this standard sits somewhere between secret and free suffrage, given that it is aimed at preventing vote selling, we are of the opinion that is the standard that better encompasses the dimension of individuality.

Second, both standards No. 24 and No. 25 can be related to confidentiality. On the one hand, according to standard No. 24, "[t]he e-voting system shall not allow the disclosure to anyone of the number of votes cast for any option until after the closure of the electronic ballot box. This information shall not be disclosed to the public after the end of the voting period" (Council of Europe, 2017a). On the other, standard No. 25 reads that "[e]-voting shall ensure that the secrecy of previous choices recorded and erased by the voter before

[272] On the other hand, the Guidelines for the implementation of this standard focus exclusively on voter register data which, according to the Guidelines, "should be clearly separated from voting components" (Council of Europe, 2017c: standard No. 19).

[273] At least, not according to the understanding and definition of secret suffrage developed in chapter 2 (in terms of individuality, confidentiality, and anonymity of the votes cast), and neither with the very definition provided in the Explanatory Memorandum. In standard 20, the Explanatory Memorandum to the Recommendation further adds that "[d]ata minimisation aims at ensuring data protection and is part of vote secrecy" (Council of Europe, 2017a). However, secret suffrage and personal data protection are complementary regulations, sometimes overlapping, but under no circumstances one "is part" of the other. For instance, personal data protection regulations apply as well to personal data processed about voters and candidates, while secret suffrage would deal only with the contents of the vote cast and the conditions in which voters cast them. Thus, data protection is in fact broader than vote secrecy (some aspects of data protection do not deal with the vote at all) and cannot "be part" of it. For a more detailed account of the distinction between data protection and secret suffrage, see Adrià Rodríguez-Pérez (2021).

issuing his or her final vote is respected" (Council of Europe, 2017a). Thus, first standard No. 24 builds on top of standard No. 19 and prescribes the sealing of the votes cast, thus ensuring its confidentiality. Interestingly, the wording of this provision is aimed at preventing the publication of partial results, and it not an end in itself, thus highlighting the link between secret and equal suffrage. Nevertheless, we have seen that confidentiality should be considered and end in itself and not just a means to prevent the publication of intermediate election results. Second, standard No. 25 extends the reach of confidentiality to the "previous choices recorded and erased by the voter before issuing his or her final vote" (Council of Europe, 2017a) and granting them "the same protection as the secrecy of the final vote" (Council of Europe, 2017b: para. 76). This is important because it highlights certain requirements that may have to be put in place specifically for (remote) electronic voting (and already unveils the constraints of those approaches based on analogy with paper-based voting channels, that we will address in chapter 5).

Lastly, among the standards listed under this section there is the explicit reference to anonymity. In this sense, standard No. 26 reads that "[t]he e-voting process, in particular the counting stage, shall be organised in such a way that it is not possible to reconstruct a link between the unsealed vote and the voter. Votes are, and remain, anonymous" [emphasis added] (Council of Europe, 2017a). The way that this standard prescribed anonymity is very similar to the definition offered in chapter 2. However, it is important to stress that here the link cannot be established with the unsealed vote. This clarification conveys that it should be possible to link a voter to a vote as long as the contents are protected, something that is quite common in remote voting channels (both in postal and Internet voting). This issue will be further elaborated in section II.3 below.

Beyond section IV

In addition to the standards which fall all directly under section IV on secret suffrage, the Recommendation also touches upon this principle in regard to standards No. 44, No. 45, and No. 46.

First, standard No. 44 reads that "[i]f stored or communicated outside controlled environments, the votes shall be encrypted" (Council of Europe, 2017a). Since our analysis focuses on remote electronic voting from uncontrolled environments, this standard fully applies to our scenarios. As we will see later, it goes hand in hand with standards No. 19, No. 24, and No. 25., since encryption ensures confidentiality.

Second, standard No. 45 can be linked to anonymity. This standard sets that "[v]otes and voter information shall be kept sealed[274] until the counting process commences" (Council of Europe, 2017a). Therefore, this standard "clarifies the moment where [sic] sealing ends" (Council of Europe, 2017b: para. 134).

Lastly, standard No. 46 provides that "[t]he electoral management body shall handle all cryptographic material securely" (Council of Europe, 2017a). This provision is key, not only because it is necessary to efficiently guarantee most of the provisions related to secret

[274] The Recommendation defines sealing as "protecting information so that it cannot be used or interpreted without the help of other information or means available only to specific persons or authorities, including through encryption" (Council of Europe, 2017a). Interestingly, the Recommendation leaves it open as to which alternatives to encryption could contribute to the sealing of the votes or the ballot boxes. For a definition of encryption see footnote 271 above.

suffrage, but also because it draws attention to the relevance of operational measures. In this sense, the key-distribution mechanisms described in the Guidelines for the implementation of this standard (Council of Europe, 2017c) are of paramount importance to ensure that both the dimensions of confidentiality and anonymity of the votes are preserved. On top of that, this Guideline acknowledges as well that "[t]he private cryptographic keys be [sic] should be generated at a public meeting" (Council of Europe, 2017c), bridging the principle of secret suffrage with the requirements for transparency and observation. We will delve more into the links between secret suffrage and transparency in chapter 5.

Indirect references to voting secrecy can also be found in standards No. 6 (related to equal suffrage), in standards No. 16 to No. 18 (in relation to free suffrage) and in standard No. 40 (related to the reliability of the system). While none of those standards deals in principle with secret suffrage, neither directly or indirectly, we have found that they reference the principle of secret suffrage either in the provisions of the Explanatory Memorandum or in the Guidelines on the implementation of these provisions.

We can analyse first those standards related to free suffrage (standards No. 16 to 18). Overall, the Explanatory Memorandum and the Guidelines for this standards detail that their provisions should be balanced against the requirements for secret suffrage. First, Standard No. 16 reads that "[t]he voter shall receive confirmation by the system that the vote has been cast successfully and that the whole voting procedure has been completed" (Council of Europe, 2017a). This provision is completed in the Explanatory Memorandum to the Recommendation, which reads that "[i]t is good practice to accompany these messages with a remainder and instructions to the voter on how to delete traces of the vote if voting was done from an uncontrolled device" [emphasis added] (Council of Europe, 2017b: para. 58).

Second, standard No. 17 provides that "[t]he e-voting system shall provide sound evidence that each authentic vote is accurately included in the respective election results. The evidence should be verifiable by means that are independent from the e-voting system" (Council of Europe, 2017a). For this standard, the Explanatory Memorandum to the Recommendation reads: "it should be possible to audit the evidence to verify its correctness with tools which are external and independent from the e-voting system. To do so, the e-voting system should provide interfaces with comprehensive observation and auditing possibilities, subject to the needs of secrecy and anonymity of the vote" [emphasis added] (Council of Europe, 2017b: para. 60).

Third, standard No. 18 notes that "[t]he system shall provide sound evidence that only eligible voters' votes have been included in the respective final result. The evidence should be verifiable by means that are independent from the e-voting system" (Council of Europe, 2017a: 6). For this standard, the Explanatory Memorandum to the Recommendation adds that (Council of Europe, 2017b: para. 41) [emphasis added]:

> "[v]oters and this parties should be able to check that only eligible voters' votes are included in the election result. At the same time counted votes should be anonymous. In the case of internet voting, there exist encryption methods that do not require

> decoding before votes are counted (homomorphic encryption). Counting can be performed without disclosing the content of encrypted votes"[275]

Overall, these standards highlight the need to balance the transparency and auditability of the election with the preservation of secret suffrage.

In a similar fashion, provisions on standard No. 6 also call for taking into account the principle of secret suffrage. More specifically, this standard provides that "[w]here electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the results" (Council of Europe, 2017a). In turn, the Explanatory Memorandum to the Recommendation sets that (Council of Europe, 2017b: para. 40) [emphasis added]:

> "[w]hen the number of e-votes or of paper votes is particularly small there is the risk that vote secrecy may be violated if the results of those few votes are disclosed. The aggregation method should contain the necessary technical and procedural safeguards to ensure the consolidation of results of the different voting channels before results are disclosed, thus ensuring secrecy. In addition, procedural rules, related namely to personnel intervening in the counting process, should take into account such cases"

Lastly, standard No. 40 prescribes that "[t]he electoral management body shall be responsible for the respect for and compliance with all requirements even in the case of failures and attacks. The electoral management body shall be responsible for the availability, reliability, usability and security of the e-voting system"[276] (Council of Europe, 2017a). This is an umbrella provision regarding the obligations of election administrations when they introduce (remote) electronic voting, which obviously also include compliance with secret suffrage.

Beyond secret suffrage: on the regulation of (remote) electronic voting

In one final point about the Recommendation, it is important to highlight that it also offers some guidance on how to regulate (remote) electronic voting. In spite of these standards

[275] This provision of the Explanatory Memorandum is quite striking because, as we have already seen, digitally signed votes tend to be encrypted (prior to their anonymization) which does not compromise neither the confidentiality nor the anonymity of the ballots and yet allows any third party to ascertain that all votes stored in the voting server have been cast by eligible voters. At the same time, while homomorphic encryption allows for anonymously decrypting the ballot, it is not a sufficient measure to ensure the property of eligibility of all votes cast unless they are digitally signed. This discussion will resume in chapter 5.

[276] The guidelines for the implementation of this standard, read, among others (Council of Europe, 2017c) [emphasis added]:

> "From the moment the vote is cast, no one should be able to read or change it or relate the vote to the voter who cast it. This is achieved by the process of sealing the ballot box, and where the ballot box is remote from the voter, by sealing the vote throughout its transmission from voter to ballot box. In some circumstances, sealing has to be done by encryption.
>
> To seal any ballot box, physical and organisational measures are needed. These may include physically locking the box, and ensuring more than one person guards it. In the case of an electronic ballot box, additional measures are necessary, such as access controls, authorisation structures and firewalls.
>
> A vote is sealed when its content has been subject to the measures that ensure that it cannot be read, changed or related to the voter who cast it."

This is an excellent example of regulating by analogy, so we will return to this provision in the next chapter.

not being only related to secret suffrage, it is worth looking at them for our analysis. These include standard No. 28 and No. 29.

Standard No. 28 prescribes that "[b]efore introducing e-voting, member States shall introduce the required changes to the relevant legislation" (Council of Europe, 2017a). Interestingly, the Explanatory Memorandum adds that "[e]xisting legislation is not written with automation in mind and may be ambiguous when applied to e-voting" (Council of Europe, 2017a). We would further add that not only may be existing legislation ambiguous, but it could be insufficient or even contrary to the observance of electoral principles when applied to remote electronic voting. This issue, in line with the latent ambiguities presented in chapter 1, will be resumed in chapter 5.

In turn, according to standard No. 29 "[t]he relevant legislation shall regulate the responsibilities for the functioning of the e-voting systems and ensure that the electoral management body has control over them" (Council of Europe, 2017a). While this standard stress the role and responsibility of electoral management bodies *vis-à-vis* other electoral stakeholders (in fact, mainly vendors[277]), when it comes to complying with secret suffrage in remote electronic voting it is important to recall the responsibilities of voters as well.

b) The OSCE/ODIHR's guidance on how to observe secret suffrage in (remote) electronic voting

Whereas the Council of Europe's Recommendation is the only specialised international legal document on election technologies and electronic voting, we have already seen that other standards can be used as benchmarks as well. When it comes to secret suffrage, the OSCE/ODIHR's methodology for the observation of NVT must be taken into account.

The OSCE/ODIHR's Handbook on this methodology devotes a section to the "Secrecy of the Vote" (OSCE/ODIHR, 2014: 9). It derives its interpretation of secret suffrage from paragraph 7.4 of the 1990 OSCE Copenhagen Document, that requires participant states to "ensure that votes are cast by secret ballot or by equivalent free voting procedure" (Copenhagen Document, para. 7.4). According to the Handbook, the "secrecy of the vote means that it should not be possible to associate a vote with a specific voter. This secrecy permits the voter to exercise her or his choice freely, without the potential for coercion, intimidation, or vote-buying" (OSCE/ODIHR, 2014: 9). Therefore, we see important similarities to the approach in the Council of Europe's Recommendation, where secret suffrage is seen as an enabler of free suffrage.

When applied to the context of NVT, secret suffrage translates as the requirement that "[v]oters must not be able to prove to anyone how they voted, and the system itself must

[277] While the first paragraph of the Explanatory Memorandum about this standard sets that "[t]here are numerous stakeholders that play a role and bear some degree of responsibility in developing, testing, certifying, deploying, applying, maintaining, observing and auditing e-voting systems" (Council of Europe, 2017b: para. 87), the following and last paragraph deals only with vendor-lock-in (Council of Europe, 2017b: para. 88). In a similar fashion, the four items listed in the Guideline for the implementation of this standard address aspects related to the links between electoral management bodies and vendors, namely: a) procurement, b) conflicts of interests, and d) dependency of vendors (Council of Europe, 2017c: standard No. 29). Possibly, only the separation of duties mentioned in item c) of the Guideline could be of application to stakeholders other than vendors (for instance, like in Estonia, where different public administrations are responsible for the operation of different system components).

not allow identification of a voter with her or his vote" (OSCE/ODIHR, 2014: 9). It is easy to find the similarity between these two requirements and standards No. 23 and No. 26 of the Recommendation, on receipt-freeness and anonymity, respectively.

At the same time, having been drafted at a time where individual verifiability had already been used, the OSCE/ODIHR does not exclude the adoption of mechanisms achieving recorded-as-cast verifiability. Notwithstanding, it also warns that "[w]hen NVT systems provide voters with receipts or codes in order to verify whether the vote was recorded as cast, supplementary measures should be implemented in order to safeguard secrecy" (OSCE/ODIHR, 2014: 9). Interestingly, no mention is made to cast-as-intended verifiability mechanisms, that by that time had already been used in Norway.

Lastly, the OSCE/ODIHR alerts that "a system that retains an electronic log that could be used to associate a voter with her or his choice would also [sic] fail to provide for the secrecy of the vote" (OSCE/ODIHR, 2014: 9). From this statement it can be understood that should a state not implement the supplementary measures to the recorded-as-cast mechanisms mentioned above, such mechanisms would breach the principle of secret suffrage.

Another interesting aspect regarding secret suffrage in the OSCE/ODIHR's methodology are the provisions on how to regulate electoral principles[278]. Regarding the principle of secret suffrage, the OSCE/ODIHR identifies as a key task the examination of whether the electoral legislation clearly defines this principle (2014: 21). Regarding the definitions of the principles, it also adds that "[i]f special provisions are required to ensure that NVT systems guarantee these principles, they should ideally be set out in the electoral legislation" (OSCE/ODIHR, 2014: 21). It is the observers' responsibility to assess whether the provisions related to the use of (remote) electronic voting are consistent with the requirements of the secrecy of the vote, "as well as whether it regulates the use of NVT in a similar way to paper-based voting" (OSCE/ODIHR, 2014: 21). While it is not exactly clear what is meant by "a similar way" here, we assume that observers are entrusted with addressing whether secret suffrage is complied with. However, it does not necessarily convey that those protections for secret suffrage in paper-based voting should be assessed *ceteris paribus* when (remote) electronic voting channels are used[279].

[278] the Handbook also touches upon the regulation of (remote) electronic voting more broadly. The Handbook distinguishes between those cases where detailed regulation is provided primarily in electoral laws and those where the legal framework establishes only general rules, "leaving the detail to binding regulations issues by the electoral authority" (OSCE/ODIHR, 2014: 21). In the opinion of the OSCE/ODIHR, "the latter [approach] is advantageous in terms of flexibility, [but] it can give too much scope for election procedures to be adapted to the needs of the technology, instead of the other way around, and to circumvent important safeguards if time becomes scarce due to delays in the implementation of the NVT system" (2014: 21). The Handbook also warns that "[t]here must also be no significant gaps in the legal framework; for instance, it should be clear what steps are taken if the NVT partially or completely fail in one or more polling stations" (OSCE/ODIHR, 2014: 21).

[279] The OSCE/ODIHR's methodology also includes a reference to data protection issues, although not as part of the provisions on secret suffrage. More specifically, the Handbook reads (OSCE/ODIHR, 2014: 23):

> "data protection […] is especially relevant in technological applications where a voter's identity may be recorded in some way, such as in an Internet voting process. The EOM should determine what data

The OSCE/ODIHR's Handbook also devotes one section to the security and secrecy of the vote. It starts by stressing that "[s]afeguarding the secrecy of the vote […] must be part of the fundamental design of the NVT system" (2014: 35) and warns that secret suffrage "can be adversely affected by technological or design flaws" (2014: 35). The OSCE/ODIHR highlights that "even when the basic architecture of the system is appropriately designed to safeguard the secrecy and integrity of the results, NVT will still be subject number of potential security threats" (2014: 35). In the opinion of the organisation, such threats are especially worrisome –even if they also exist in traditional paper voting processes– since "may require technological skills and significant resources not possessed by the typical voter to be detected or observed" (OSCE/ODIHR, 2014: 35).

From the perspective of secret suffrage, the most relevant attacks include voter intimidation, coercion and vote buying, which result from the fact that "the voter cannot be protected to the same degrees by the election commission from such undue influence as within polling stations" (OSCE/ODIHR, 2014: 37). Once again, it is also acknowledged that such attacks also applied to paper-based postal voting (OSCE/ODIHR, 2014: 37). In turn, also acknowledges "the possibility to re-cast a ballot more than once or to cancel the electronic vote with a paper vote prior to election day, including in a polling station" (OSCE/ODIHR, 2014: 37). Beyond these provisions, most of the threats identified are related to the integrity and availability of the system, rather than to the secrecy of the vote.

To sum up, it is worth looking into the questions pinpointed by the OSCE/ODIHR in relation to secret suffrage. This can help us inquire about the organisation's interpretation of secret suffrage and (remote) electronic voting:

- "Does the law fully provide for the equality and secrecy of the vote? Are legal provisions relating to NVT consistent with these principles? For example, does the law give the voter an opportunity to retain any document or data that could enable the voter to prove the content of the vote when coerced, or does the verification process associate voters with their votes?" (OSCE/ODIHR, 2014: 24)
- "What measures are in place to ensure secrecy of the vote?" (OSCE/ODIHR, 2014: 34)
- "Does the NVT system contain any design elements that could allow a voter to be identified with her or his vote, or that could permit a voter to be directly intimidated or influenced in her or his choice?" (OSCE/ODIHR, 2014: 37)
- "If the NVT rely on transmission of data by Internet, what measures are in place to prevent or detect external hacking to either retrieve or alter data?" (OSCE/ODIHR, 2014: 37)
- "Are measures in place to provide voters with the ability to avoid undue influence, such as the ability to re-cast a ballot electronically or cancel an electronic vote by casting a paper vote? Are these measures effective?" (OSCE/ODIHR, 2014: 37)

protection requirements exist and whether the NVT system complies with these requirements, including any special requirements that may exist for systems processing sensitive personal data, such as voters' political opinion. Furthermore, an EOM should try to assess whether the benefits of using NVT, especially when personal data is involved, are proportional to their added value to an electoral process. Data protection standards require that every voter is made aware of the existence of automated processing, the kind of data collected and the identity of the data collector; that the data is only processed in relation to the respective election and not used for any other purpose; and that it is not kept for a period longer than is necessary (i.e., it is destroyed after the end of the complaint and appeals process)."

In this regard, we see that the first question focuses on the regulation of secret suffrage and (remote) electronic voting, stressing the requirements for receipt freeness and anonymity. The second question is broader and enquires whether there are measures in place to ensure the secrecy of the vote. These measures (or at least the potential attacks that they should be prevented) are detailed in the tree questions that follow. Of these three questions, the first one warns about the possibility of breaches in the anonymity of votes cast, and about the possibility of voters being coerced or influenced while voting from non-supervised environments. The second focuses on the security of the data during transmission through the Internet, the channel in which remote electronic voting relies on to cast the vote from the voting device and to store it in the voting server. The last question looks again into freedom, this time focusing on whether there are mechanisms to prevent –or at least mitigate– the threat of coercion during the casting of the vote, as well as on their effectiveness.

2. National experiences, on secret suffrage: principles, regulations, and concerns for remote electronic voting

In addition to requiring new international standards on (remote) electronic voting, "complying with the principle of secrecy poses new obstacles for many countries" (Vinkel, 2016: 42). The goal of this section is thus to understand how these problems have been dealt with in thee three national experiences.

We base our assessment in Priit Vinkel's broader approach towards the constitutionality of remote electronic voting. In the opinion of this author (Vinkel, 2016: 41):

> "[t]he question of whether remote internet voting with binding results in public political elections complies with the constitutional principles of sound and fair voting cannot be answered with a simple "yes" a [sic] "no". As such, two sub-questions were proposed. The first sub-question was whether the legal norms in an abstract sense comply with the constitutional provisions of the state, and the second whether the technical solutions used to conduct e-voting procedures in a certain election guarantees constitutionality."

Can this approach be adopted for our analysis of secret suffrage in remote electronic voting? We think so. And since the question of whether remote internet voting complies with the constitutional principle *of secret suffrage* cannot be answered with a simple "yes" or "no" either, we rephrase Priit Vinkel's sub-questions as follows:

(1) Do legal norms in the abstract comply with the international standards and constitutional provisions on secret suffrage?
(2) Do the technical solutions used to conduct remote electronic voting procedures guarantee the principle of secret suffrage?

Therefore, to approach the three national experiences we will need to assess both the legal and administrative framework, as well as the specific technological implementation. This forces us to look beyond the national Codes and Acts, and to identify specific requirements in administrative regulations, or even technological documentation. This assessment is of course limited. We do not have the necessary technological knowledge to answer whether technical solutions actually comply with these requirements. Therefore, our analysis is limited and should be complemented with additional assessments and evaluations of the actual technologies and their operation

To answer these two sub-questions, the remainder of the chapter has been divided into two. First, in this section (I.2) we provide a short overview of the three national experiences in terms of how they regulate secret suffrage, which requirements can be found in their legal and regulatory frameworks regarding the enforcement of this principle in remote electronic voting, and we pinpoint some issues that have been raised regarding this principle during their adoption of Internet voting (sub-question 1). Following, in Section II we will break down this assessment to evaluate whether and how the three minimum standards of secret suffrage (i.e., individuality, confidentiality, and anonymity) are met both in the international standards and the three national experiences (sub-question 2). Therefore, the next section provides a deeper analysis of the national experiences but focusing only on those issues related to secret suffrage in remote electronic voting. It builds on the historical analysis in the previous chapter, although it is mainly concerned with current issues regarding secret suffrage. Our goal here is to assess whether and how the principle of secret suffrage has been observed in the three national experiences and to set the stage for the broken-down assessment that will be conducted in the next section.

a) Switzerland

In Switzerland, the guarantee of political rights protects both principles of free and secret suffrage. It confers on each voter the right to vote in secret and free from any external pressure that they may experience (Swiss Federal Council, 2013a: 71). Interestingly, however, secret suffrage has never been explicitly written into the Federal Constitution (Swiss Federal Council, 2002: 626-627). Notwithstanding, it is indisputably recognised by law, by case law and by doctrine. For example, art. 5.7 of the Federal Act on Political Rights prescribes that "[v]oting secrecy must be preserved". For Internet voting[280], art. 8a.2 requires that "[t]he verification of eligibility to vote, voting secrecy and the counting of all the votes cast must be guaranteed and abuses prevented" (Federal Act on Political Rights).

In line with these provisions, some of the initial requirements identified in the first report by the Swiss Federal Council were that "it must be impossible to capture, modify or hijack the votes of the electronic vote" and that "no third party should be able to observe the votes cast electronically" (Swiss Federal Council, 2002: 627). Briefly put, the 2002 report noted that "[a]ll voters must be able to vote without it being possible –neither during the vote nor afterwards– to know how they voted" (Swiss Federal Council, 2002: 627). Interestingly, we may see here a first reference to the requirements for long-term privacy. In turn, the Swiss Federal Chancellery also highlighted in its intermediate report that "[s]ecurity must also be able to ensure the secrecy of the vote, the level of which must be equal to that of postal voting. It is therefore imperative that the various data cannot be used to link a vote to the person who has cast it" (Swiss Federal Chancellery, 2004: 20).

The 2006 report also included secret suffrage as one of the three requirements that should be guaranteed in remote electronic voting, together with the control of the voter's

[280] Whereas for advance voting in (certain) polling station, the Act mandates the cantons to "enact the required provisions relating to the counting of all the votes cast, the preservation of voting secrecy and the prevention of abuses" (Art. 7.4 Federal Act on Political Rights). The Federal Act on Political Rights also sets that "[t]he cantons shall provide a simple procedure for postal voting. In particular, they shall enact provisions to guarantee the verification of eligibility to vote, voting secrecy and the counting of all the votes cast, and to prevent abuses" (Art. 8.2).

status and the counting of all the votes (Swiss Federal Council, 2006: 5213). That very same report compared secret suffrage in remote electronic voting to postal voting[281] (Swiss Federal Council, 2006: 5262): "maintenance of the secrecy of the vote / data protection: the will of the voters must remain secret, and the indications relating to data protection must not reach third parties"[282]. Therefore, two main requirements were elicited: first, the separate storage of personal data and voting components on different systems; and second, the permanent and random shuffling of the electronic ballot box to avoid that someone can establish the identity of a specific person based on the order of arrival of the votes.

These requirements have been enshrined in the ordinances enabling the use of remote electronic voting. For example, the Ordinance on Political Rights sets that the initial licence by the Federal Council may be only granted to a canton if it ensures that will conduct the trials with electronic voting in line with the federal requirements (art. 27b.a), and in particular that it will take all the effective and adequate measures to ensure that no third parties can become aware of the content of the electronic votes (secrecy of the vote) (art. 27b.a.4).

The Federal Chancellery Ordinance on Electronic Voting (VEleS) further develops this provision. For example, to introduce Internet voting at any level, "the canton must document in detailed and understandable terms that any security risks are within adequate limits [by the means of a risk assessment]" (art. 3). One of the security objectives that such assessment must cover is precisely "the protection of voting secrecy and non-disclosure of early provisional results" (art. 3.1.a). Even more detailed are the provisions in the Annex to VEleS on Technical and administrative requirements for electronic vote casting. The Annex offers a set of requirements for confidential and secret data, which include (Swiss Federal Chancellery, 2018d)

- 2.8.1. It is guaranteed that neither employees nor externals obtain data that allow a connection to be made between the identity of voters and the votes they have cast.
- 2.8.2. It is guaranteed that neither employees nor externals obtain data before the decryption of the votes that allow early provisional results to be determined.
- 2.8.3. It is guaranteed that the results of the vote are treated as confidential between the decryption of the votes and the time of publication of the results.
- 2.8.4. It is guaranteed that data that indicate whether a voter has voted electronically are treated as confidential.
- 2.8.5. It is guaranteed that personal data from the electoral register will be treated as confidential.

[281] As expressed by the Swiss Federal Council, « synthèse des exigences et des mesures de mise en oeuvre afférentes au vote électronique qui sont le fruit de réflexions juridiques et sécuritaires; […] à titre de comparaison, les exigences et les mesures afférentes au vote par correspondance » [emphasis added] (2006: 5262)

[282] Based on an analogy with postal voting, where "the completed ballot papers reach the municipal administration in a separate envelope, which is sealed. The legitimation card and the ballot paper must be slipped into separate ballot boxes after verification of the credibility of the signatures" (Swiss Federal Council, 2006: 5262).

- 2.8.6. It is guaranteed that individual votes will be treated as confidential even after tallying.
- 2.8.7. It is guaranteed that the results of the vote will be treated as confidential if only a small number of voters in a constituency can vote electronically.
- 2.8.8. Upon validation and in accordance with a documented process, the system operator destroys all data created as part of the electronic ballot that relate to the individual votes received and that are classified as confidential or secret."

Interestingly, the Annex distinguishes between confidential and secret data and information. On the one hand, "[d]ata and information are confidential if they may only be disclosed to specific individuals", whereas they "are secret if they are confidential and may not be disclosed to anyone"[283] (Swiss Federal Chancellery, 2018d: 1.3.6.1). The question arises as why individual votes should be treated as confidential even after tallying, and not as secret. Does it mean that individual votes may be disclosed to specific individuals? The fact that results of the vote will be treated as confidential if only a small number of voters in a constituency can vote electronically, and not as secret, could breach secret suffrage as well.

The provisions in the Annex on security requirements partially address these concerns (Swiss Federal Chancellery, 2018d:):

- 3.3.3. In order to guarantee the confidentiality of data records that substantiate voting secrecy and the avoidance of early provisional results, effective cryptographic measures that correspond to the state of the art must be used.
- 3.3.4. Votes must not be stored or transmitted in unencrypted form at any time from being entered to tallying.

  […]
- 3.3.6. Basic cryptographic components may only be used if the key lengths[284] and algorithms[285] correspond to the current standards (e.g. FIPS 143-3, NIST, ECRYPT, ESigA)."

It is important to note that, according to the Swiss Federal Council, secret suffrage is not understood as an end in itself, but rather as a means of guaranteeing the rights of voters

[283] This terminology should not be confused with our three standards for secret suffrage, where confidentiality means that only the voter should know how they have voted, and they should be able to make their choices in private.

[284] A cryptographic key is a special item of data that a computer needs to represent as a binary number (Martin, 2020: 29). The size of a cryptographic key is an important security measure, and that is why reference is made to the *key length* here. Key length, together with the randomness used to generate them, "is what makes cryptographic keys so difficult to both guess and memorize" (Martin, 2020: 38). For more information on keys and cryptographic algorithms see footnote 285 below.

[285] According to Keith Martin, "[a]n algorithm is essentially a recipe dictating a sequence of operations that must be performed in a specific order" (2020: 35). On the link between an algorithm and a key, the author notes that"[s]ince cryptographic keys are numbers, any process that incorporates a cryptographic key will necessarily involve a sequence of mathematical operations such as adding, multiplying, shuffling, or swapping" (Martin, 2020: 35). The result of these operations is defined as the output of the algorithm. For more information on keys and cryptographic algorithms see footnote 284 above.

and ensuring their freedom (2002: 627). As a result, it is considered an obligation for the authorities, but a right of the voters.

As more recently noted by the Swiss Federal Council: this right, in turn, creates and obligation for the authorities to provide the necessary conditions for its fulfilment (2013a: 71). This is undoubtedly a result of the extensive use of postal voting throughout the country. In this same report, the Swiss Federal Council noted that in regard to the protection of the secrecy of the vote during postal voting (and therefore outside the polling stations) the Swiss authorities appealed to individual responsibility and trust[286] (Swiss Federal Council, 2013a: 71).

In this sense, both the federal and the cantonal legal frameworks provide for the secrecy of the vote as a responsibility of each individual voter. In this vein, the 2011 OSCE/ODIHR's EAM concluded that "as a consequence of the high level of trust, strict controls are not always in place to safeguard the secrecy and integrity of the voting and counting processes" (2012a: 1). Swiss voters' confidence in the electoral system and authorities is reciprocated by the trust which the system has in voters. Therefore, while it "is a fact that postal voting may facilitate family voting; the Swiss Federation relies on each voter to protect the secrecy of his/her vote and, by doing so, maintains a credible postal voting system which should uphold the secrecy of the ballot" (OSCE/ODIHR, 2008: 17).

As a matter of fact, the OSCE/ODIHR missions have also reported lax practices when it comes to compliance with secret suffrage for voting in polling stations, such as the lack of voting booths or privacy screens (OSCE/ODIHR, 2012a: 14) or the absence of a requirement that ballots be folded or placed in an envelope before being stamped by polling officials[287] (OSCE/ODIHR, 2008: 18; OSCE/ODIHR, 2012a: 14). Along these lines, in OSCE/ODIHR's reports it is acknowledged that the principle of secret suffrage cannot be directly enforced and depends upon the political culture and the ethical stand of the voters (OSCE/ODIHR, 2007c: 8). Based on what has been said above, it should thus not come as a surprise that the OSCE/OIDHR's Expert Team deployed to observe the 2015 Swiss federal elections noted that "[t]hose who acknowledged potential vulnerabilities of Internet voting in terms of security and secrecy of the vote[288] believed that the benefit of increased and easier access outweighed the risks" (2016: 4).

[286] In turn, « on fait appel à la responsabilité individuelle et à la confiance. Ceci est valable également vis-à-vis de la poste, canal de transmission du vote par correspondance. La confiance s'applique d'ailleurs à tous les services postaux (vote des Suisses de l'étranger) mais les autorités sont conscientes des limites du canal, notamment à l'étranger » (Swiss Federal Council, 2013a : 71).

[287] According to the Swiss Federal Council (2006: 5261-62):

> « [Un] étude de l'Université de Berne constate que la volonté des électeurs est souvent faussée dans le cadre familial lors du remplissage du bulletin de vote, précisément qu'il arrive en particulier que l'homme remplisse le bulletin de son épouse en même temps que le sien, alors que le cas inverse ne se produit jamais. L'étude ne fournit aucun renseignement sur la fréquence des abus qui sont commis. Elle arrive cependant à la conclusion qu'il semble justifié de constater que l'abus et la fraude constituent des événements plutôt rates et isolés. Les chancelleries communales interrogées estiment que le danger représenté par les abus commis dans le cadre du vote par correspondance est bien plus faible qu'en cas de vote par procuration. Le Conseil fédéral a par ailleurs chargé la Chancellerie fédéral, en décembre 2004, d'identifier les risques liés au vote par correspondance et de les comparer aux résultats correspondants obtenus dans les projets pilotes en matière de vote électronique. »

[288] Along similar lines, already in its 2002 report the Swiss Federal Chancellery had worked under the assumption that "[t]he protection of the secrecy of electronic voting should not be less than what it is today for voting in general. The strict protection of the type of protection that prevails for

In Switzerland, the respect of secret suffrage in remote electronic voting was an issue of key importance during the first stages of the introduction of this technology[289]. Already in 2002, the Swiss Federal Data Protection and Information Commissioner assessed the introduction of Internet voting with criticism. In their annual activity report, they saw a conflict between the principle of secret suffrage (i.e., the standard of anonymity) and the need to trace the operations to a certain extent (Swiss Federal Council, 2006: 5216). Likewise, several parliamentarians also raised privacy concerns when debating the 2002 report by the Swiss Federal Council. In October 2002, on the occasion of an event organised on the topic of remote electronic voting, the Swiss association for the development of legal informatics (in French, *Association suisse pour le développement de l'informatique juridique*) also raised several concerns regarding the secrecy of votes cast through electronic means (Swiss Federal Council, 2006: 5219).

The Swiss Federal Council also identified specific threats to this principle in its 2006 report. For example, it acknowledged the possibility that the devices used to vote could be compromised with malware that would reveal the voter's preferences and their choices, or by means of intrusions by system's administrators (Swiss Federal Council, 2006: 5218). While some of these concerns still remain today[290], the current focus has shifted towards transparency and verifiability issues more than on potential challenges to secret suffrage. For example, one of the questions posed during the dialogue with the experts (Swiss Federal Chancellery, 2020b: 56) acknowledged that, "[d]espite postal voting being used by more than 90% of the voters, vote-buying and coercion are not considered to be a concern in Switzerland" (Swiss Federal Chancellery, 2020b: 56). The experts were divided on this issue. Half of them concluded that risks are not or not much higher, whereas the other half highlighted that such risks are higher "with internet voting, mainly due to anonymity and increased scalable technical feasibility" (Swiss Federal Chancellery, 2020c: 18). In turn, the Final report of the Steering Committee on the "Redesign and relaunch of trials" merely called upon considering these risks in updated guidelines for the conduct of risk assessments (Swiss Federal Chancellery, 2020d: 23).

postal voting should suffice. It is already complex enough for electronic voting" (2002: 627). The analogy drawn here between postal and remote electronic voting will be dealt with further in the next chapter.

[289] However, since the adoption of VEleS such concerns seem to have shifted towards issues of cantonal oversight and verifiability (OSCE/ODIHR, 2015c: 2). The OSCE/ODIHR mentions once their interlocutors' concerns with secret suffrage (OSCE/ODIHR, 2015c: 7). Notwithstanding, they do not highlight these concerns in the rest of the report and the EET deployed during the federal elections does not mention them at all. In contrast, some concerns regarding the processing of personal data are mentioned (OSCE/ODIHR, 2015c: 2 and 7; OSCE/ODIHR, 2016: 5, 8-9). Overall, it seems feasible to conclude that in spite of concerns about secret suffrage still existing, they are no longer as key as they may have been in previous phases.

[290] For instance, during the consultation on the partial review of the Swiss Federal Act on Political Rights, some political parties « mentionnent notamment à cet égard le risques accru de manipulation des systèmes de vote électronique, la nécessite (mais aussi la difficulté) de garantir le secret du vote sans affecter la traçabilité et enfin l'importance de la transparence et de la traçabilité » (Swiss Federal Chancellery, 2019c: 8). Likewise, the technology provider Procivis AG also argued that online voting was one of the most complex problems in ICT, most especially if one would take into account the need to preserve the secrecy of the vote (Swiss Federal Chancellery, 2019c: 11).

b) France

In France, and in contrast to the Swiss case, secret suffrage is one of the electoral principles enshrined in art. 3 of the Constitution, together with universal and equal suffrage[291]. According to Romain Rambaud, the principle of secret suffrage implies that sufficient practical guarantees are foreseen in the voting rules (2019: 111). However, it is up to the legislator to lay down the specific rules that guarantee secret suffrage in a particular election. Likewise, it is up to the legislature whether to foresee criminal sanctions for those behaviors which are not in line with these rules. The Constitutional Council, entrusted to protect this principle both as part of its constitutional review as well as in its role as electoral judge, has acknowledge the role of the legislator in this regard[292] (Rambaud, 2019: 111).

In line with these constitutional provisions, secret suffrage in enshrined in art. L59 of the Electoral Code, that sets that the ballot is secret. Art. L60 then establishes the envelope as a confidentiality measure to preserve this secrecy, and in turn art. 62 prescribes the voting booth[293]. According to this provision, voters must make their choice alone in the voting booth. Notwithstanding, their layout in such a way as to conceal the electoral operations from the public prevents anyone from ascertaining whether they are actually alone. In a similar way, these provisions are developed in the regulatory part of the Code[294].

Provisions on remote electronic voting are only included under the regulatory part of the Code, in the section dealing with voting by French voters abroad. Sub-section 4 on remote electronic voting includes 10 articles. The first of these articles prescribes that personal data about the voters and the votes are processed separately, in different files (art. R176-3 I.). In turn, art. R176-3-3 mandates the *bureau de vote électronique* with overseeing the proper conduct of the electoral operations, with specific mention to the security mechanisms that guarantee the secrecy of the vote[295]. The Code also prescribes end-to-end encryption of the votes, already from the device used to cast them (art. R176-3-9). In additional, art. R176-3-9 also prescribes channel encryption. In turn, the same

[291] Interestingly, free suffrage is not explicitly mentioned in art. 3 of the French constitution, that reads that "[s]uffrage may be direct or indirect as provided for by the Constitution. It shall always be universal, equal and secret" [emphasis added]. Notwithstanding, and as we have mentioned elsewhere, the principles of secret suffrage and free suffrage go hand by hand, and so is understood in France as well (Rambaud, 2019: 34).

[292] At this point, it should be noted as well that France has been found not to comply with soft law standards on elections. For example, Romain Rambaud (2019: 145-146) has noted that France does not respect the provisions of the Code of Good Practice on Electoral Matters on those aspects concerning the stability of the electoral law, that is that "the electoral system proper, membership of electoral commissions and the drawing of constituency boundaries, should not be open to amendment less than one year before an election, or should be written in the constitution or at a level higher than ordinary law" (Venice Commission, 2002a: 2.b). Therefore, it should not surprise us if we found deviations for the Council of Europe's Recommendation on e-voting.

[293] It is interesting to see how, amidst the pandemic, provisions about voting booths have been also revisited. For example, as a health measure in polling stations during the 2021 municipal elections it was prescribed a specific orientation of the voting booths (for example towards a wall) to guarantee the secrecy of the vote while avoiding the manipulation of the curtains (Buffet, 2020: 13).

[294] For example, art. R54 details the requirements for the envelopes, whereas art. D56-2 introduces the need for voting booths accessible to persons using wheelchairs.

[295] Art. R176-3.II. also mandates the Ministry of Foreign Affairs to decide not to use an electronic voting system if it is found that the system cannot ensure the secrecy of the vote.

article precludes any possibility of multiple voting (only when the voter has not confirmed their vote will they be able to vote using another channel).

The Code prescribes as well procedural measures to ensure the secrecy of the votes, namely a key-sharing mechanism that splits the decryption key between the members of the *bureau de vote électronique*. The key must be created and split at the beginning of the voting operations (art. R176-3-8) and the votes can be decrypted only with at least four of these shares (art. R177-5). From the moment voting ends on Wednesday and until the counting stage on Sunday, the president of the *bureau de vote électronique* safeguards the encrypted votes (art. R176-3-10).

Lastly, the CNIL's updated Recommendation (2019a: 3) also identifies several security objectives related to the secrecy of the vote. In what follows, we provide a list of these security objectives:

- "Security objective n° 1-04: Ensure the strict confidentiality of the ballot from its creation on the voter's computer.
- Security objective n° 1-05: Ensure the strict confidentiality and integrity of the ballot during its transport.
- Security objective no. 1-06: Ensure, in an organizational and/or technical manner, the strict confidentiality and integrity of the ballot during its processing and storage in the ballot box until the counting.
- Security objective no. 1-07: Ensure total sealing between the identity of the voter and the expression of their vote throughout the duration of the processing.
- Security objective no. 1-08: Reinforce the confidentiality and integrity of data by distributing the secrecy allowing the counting exclusively within the electoral office and guarantee the possibility of counting from a determined secrecy threshold.
- Security objective n° 1-09: Define the counting as an atomic function usable only after the close of the poll."

From the fact that they are all security objectives at level 1[296], we can infer the importance of secret suffrage. As we have already mentioned, the CNIL also offers some possible mechanisms to achieve the security objectives. For example, in order to achieve the security objective no. 1-04, it is suggested to encrypt the vote from the voting device, client-side prior to its casting, using a public algorithm reputed to be strong (CNIL, 2019c). For the security objective no. 1-07, it recommends that no link exists between the voter and their encrypted vote once it is cast and that votes are not timestamped (CNIL, 2019c). The CNIL also prescribed that the *liste d'émargement* and the votes are stored separately (2019c).

Regarding the interpretation of secret suffrage, it is understood as requiring voters to cast their vote free from any outsider's gaze. The principle implies anonymity for the ballot cast into the ballot box and prevents any traceability. As highlighted by Alain Anziani and

[296] Additionally, at level 2 the system should the physical and logical security measures recommended by the ANSSI (Security objective number 2-06). When it comes to the ANSSI's RGS, on secret suffrage Jacky Deromedi and Yves Détraigne have emphasised requirement number 266, which states that the e-voting system's holder sets up an encryption device to protect all transactions made by users of the system's application services (2018: 39).

Antoine Lefèvre (2014: 10): no link should be established between the vote cast and the voter who cast it. The authors highlight as well that even if a voter publicly proclaims their choices, they should have no way to prove their claim[297]. In this way, they conclude, "[t]he secrecy of the vote is a particularly strong condition of the freedom of the voter" (Anziani and Lefèvre, 2014: 10).

Lastly, some concerns can be found regarding secret suffrage in remote electronic voting. For example, Jacky Deromedi and Yves Détraigne highlight the difficulty of ensuring the personal and secrecy of the vote from the moment that remote electronic voting allows voters to cast their vote from unsupervised environments, such as their home or any other location. In their opinion, this opens the door to coercion (Deromedi and Détraigne, 2018: 34). These authors specifically stress the lack of guarantees provided by the voting booth in remote electronic voting. The criticism raised after the 2006 elections to the Assembly of French Citizens abroad, which we have already mentioned in the previous chapter, also echoed this concern. In addition, this criticism also focused on the fact that the system did not prevent the votes from being decrypted when only a handful of them had been cast in certain electoral districts (Pelegrini, 2006: 2; Lang, 2006).

Finally, Romain Rambaud is more straightforward and simply highlights that in recent years the issue of the secrecy of the vote has posed the most problems in regard to postal and remote electronic voting (2019: 34). Interestingly, this author seems to weight equally both voting channels, even if he specifies that remote electronic voting is only authorised in the context of non-political elections[298]. In turn, the concerns raised by Alain Anziani and Antoine Lefèvre revolve around the need to redefine certain offenses in the Electoral Code precisely to take into account the specificities of remote electronic voting. More specifically, they suggest that the penalties described in art. L. 99 for preventing a voter from freely casting their vote should not be limited to polling stations, since with remote electronic and postal voting voters can cast their vote from anywhere (Anziani and Lefèvre, 2014: 59).

c) Estonia

As in the two other cases, secret suffrage in Estonia has been defined based on the mechanism for traditional paper-based voting channels. In this sense, Ülle Madise notes that "the secrecy of the vote has traditionally been viewed […] as the right and obligation to cast a vote while being by oneself in a voting booth" (2007: 16). Notwithstanding, we have already seen that such a mechanism cannot be put in place in remote electronic voting from unsupervised environments, where if understood in these terms "it is impossible to ensure the privacy[299] aspect of the voting procedure" (Vinkel, 2016: 40). In the opinion of Priit Vinkel, "[t]he voter's right to anonymity during the tallying of the votes can be guaranteed, indeed to the extent to which this can be secured in the case of remote

[297] This is ensured, as in other jurisdictions, by declaring invalid any ballot that have any distinctive marks on them (art. L66 and R66-2 of the French Electoral Code).

[298] We do not understand this appreciation, since shortly after the author acknowledges that remote electronic voting is foreseen as well for the two elections by French voters abroad: elections to the National Assembly and for the representatives of French citizens abroad.

[299] It is important to recall that the privacy aspect is equivalent to the standards of individuality and confidentiality.

postal voting. Therefore, remote electronic voting requires a rethinking of the privacy principle"[300].

In Estonia the principle of secret suffrage is expressly enshrined in the country's Constitution. For example, art. 60 on the elections to the *Riigikogu* stablishes that "Members of the *Riigikogu* are elected in free elections according to the principle of proportional representation. Elections are general, uniform and direct. Voting is secret". Similar principles are enshrined in regard to the elections to local authorities, since art. 156 sets that "[e]lections of local authority councils are general, uniform and direct. Voting is secret". The provisions on secret suffrage are also included in the different electoral laws. For example, art. 1(2) of the *Riigikogu* Election Act reads that "*Riigikogu* elections shall be free, general, uniform and direct. Voting shall be secret"[301].

With the introduction of remote electronic voting, new provisions were defined in these laws[302]. Several provisions can be found in the *Riigikogu* Election Act regarding the principle of secret suffrage. For example, art. 48.2.(2) sets that "[a] voter votes on their own. On the conditions prescribed in this Act, a voter may change their vote cast by electronic means". The option to cast multiple ballots is further developed in art. 48.5. This provision, that was amended in 2018 to extend the internet voting period until election day and entered into force for the first time during the local elections of 2021, prescribes that:

> A voter has the right to change their vote cast by electronic means:
>
> 1) by voting again using electronic means at the time prescribed in clause 4 of subsection 2 of § 38 of this Act;
>
> 2) by voting with a ballot paper until 20:00 on the election day.

When a voter casts multiple votes, only the last vote cast is taken into account (art. 48.7(1)). The Act also provides that "[w]here a voter has voted using electronic means as

[300] These statements are telling for two reasons. On the one hand, they already conceive two different standards of secret suffrage: privacy, which allegedly cannot be achieved in remote electronic voting from uncontrolled environments; and anonymity, which can be guaranteed to the same degree than in postal voting. This links with the second question at stake: the analogy with postal voting. Whereas the starting point draws a comparison between the two voting channels, the author hurries to highlight that a rethinking of the principle of secret suffrage is required. Furthermore, Priit Vinkel adds: "[e]-voting adds a twist here, as the principles are partially ensured by way of complicated technical systems involving encryption and communications between IT systems that are hard for any layman [sic] to understand" (2016: 55). Therefore, what initially could have been framed as an analogy with postal voting, is partially overcome.

[301] Identical provisions can be found in the Municipal Council Elections Act, the European Parliament Election Act, and the Referendum Act. The Municipal Council Election Act reads in its first article that "[t]he elections of members of municipal councils (hereinafter *councils*) shall be free, general, uniform and direct. Voting shall be secret". In turn, the European Parliament Election Act states that "[e]lections to the European Parliament shall be free, general, uniform and direct. Voting shall be secret" (art. 2(2)). Lastly, the Referendum Act sets that "[a] referendum is free, general, uniform and direct. Voting shall be secret" (art. 2(1)).

[302] Currently, Chapter 7 on electronic voting in the Municipal Council Elections Act and in the European Parliament Election Act redirect to Chapter 7 of the *Riigikogu* Election Act, in very similar terms: "[e]lectronic voting shall be organised […] pursuant to the procedure provided for in Chapter 7 of the *Riigikogu* Election Act" (art. 53 of the Municipal Council Elections Act, art. 47 of the European Parliament Election Act). The Referendum Act also refers to the *Riigikogu* Election Act in its art. 41.2, although some provisions for this voting channel remain in the Act defining the stages for voting.

well as with a ballot paper, the ballot paper of the voter is taken into account" (art. 48.7(2)).

The Act also prescribes the encryption of the vote[303], since it sets that (art. 48.4(4)) [emphasis added]

> "[t]he voter indicates the candidate in the electoral district of their residence for whom they wish to vote. The application used for electronic voting encrypts the voter's vote using the vote-encryption key. The voter confirms the vote by a digital signature in compliance with the requirements of the Electronic Identification and Trust Services for Electronic Transactions Act."

Lastly, the Act mandates a key-sharing mechanisms. First, it states that "[p]rior to the start of electronic voting, the State Electoral Office creates the encryption key for electronic votes and the vote-opening key. The means of access to the vote-opening key are distributed among the members of the National Electoral Committee and the State Electoral Office" (art. 48.3(3)). for the counting of the votes cast electronically, it is set that "the members of the National Electoral Committee and the State Electoral Office use the means of access provided in subsection 3 of § 48.3 of this Act, which ensure access to the vote-opening key"[304] (art. 60.1(4)).

The State Electoral Office of Estonia (2017) has also issued a General Framework of Electronic Voting and Implementation therefor at National Elections in Estonia. The document succinctly describes some of the mechanisms to guarantee secret suffrage. The principle of secret suffrage is acknowledged in the document, which introduces the requirements for remote electronic voting as follows (State Electoral Office of Estonia, 2017: 6) [emphasis added]:

> "I-voting must adhere to all Acts concerning elections and must follow all election principles, and be at least as secure as regular voting[305]. Thus, i-voting has to be uniform and secret, only the persons who have the right to vote may (i-)vote, every person has one vote, and it must be impossible for voters to prove for whom they cast their vote.

[303] Since in Referendums voters do not vote for candidates, this is one of the provisions that is kept different in the Referendum Act, although the later also prescribed the encryption of the vote in the voter's voting device. More specifically, art. 41.3(4) of the Referendum Act reads that "[a] voter marks the answer " *jah* " [yes] or " *ei* " [no]. The application used for electronic voting encrypts the voter's vote using the vote-encryption key. The voter confirms the vote by a digital signature in compliance with the requirements of the Electronic Identification and Trust Services for Electronic Transactions Act."

[304] These are the core provisions on secret suffrage, but they are only a fraction of all the actual mechanisms that contribute to the enforcement of this electoral principle. Sutton Meagher (2009: 367) offers the following overview of the relevant legal framework:

> "Estonia is able to comply with the ICCPR secret ballot requirement through a combination of its election laws, penal code, and the design of its Internet voting procedures. Most importantly, the Estonian Constitution and Estonian election Laws create a strong legal framework because they both state that elections must be secret. Because Internet voting takes places in an environment that election officials do not oversee, there is an increased chance of voter coercion or violation of the secret ballot. In light of these dangers, the Estonian government has established additional laws and special voting procedures to guarantee that voters will be able to exercise their right to a secret ballot when voting over the Internet."

[305] This formulation reminds us of the initial approach in the Council of Europe's Recommendation. Interestingly, by the time this version of the current document was issues this approach had been challenged at the international level. The comparison between remote electronic voting and other voting channels is discussed in chapter 5.

> The main difference between i-voting and voting with paper ballot is that the voter can vote repeatedly electronically; only the last vote cast is counted. This principle enables to protect i-voters against coercion. A coerced voter can vote again after becoming free from coercer, invalidating the vote cast under pressure."

The document also describes the envelope scheme and the anonymisation of the i-votes, which enforce secret suffrage. These schemes will be described with more detail in section II.2.

For our research, the most interesting issue in the Estonian case lies in the fact that secret suffrage has been reinterpreted so it can be accommodated to the remote electronic voting channel. This reinterpretation is built based on three issues: the breaking down of secret suffrage into the privacy and anonymity standards; the understanding of secret suffrage as a means to free suffrage, and not as an end in itself; and, consequently, the understanding of secret suffrage not as a duty of voters, but instead as their right.

Regarding the configuration of the principle of secret suffrage in Estonia, we have already advanced how it is split into two different standards, which are referred to as "sub-principles"[306]. Ülle Madise and Tarvi Martens (2006: 18) summarise this approach as follows:

> "The principle of secrecy consists of the sub-principle of privacy and anonymity (secrecy of the election decision). Remote Internet voting requires in the first line rethinking of the principle of privacy. Voting in privacy should not be regarded as an aim by itself. The principle of secrecy, and its sub-principle of privacy, is there to protect an individual from any pressure or influence against her of his free expression of political preference. Therefore, it is a mean for guaranteeing freedom of choice"

The second building block of the Estonian approach to secret suffrage is based on its teleological interpretation, which means that the principle is not considered as an end in itself, but instead as a way to realise another principle: free suffrage. Priit Vinkel (2016: 42) summarises this approach as follows:

[306] In their 2007 about the use of remote electronic voting in that year's parliamentary elections in Estonia, Alexander H. Trechsel et al. (2007: 14-15) also resort to this understanding of secret suffrage based on the two "sub-principles [sic] of anonymity and voting in privacy to guarantee the freedom of the voter's choice" [emphasis added]. In this approach, the already mentioned dimensions of individuality and confidentiality are seen as one. This is evidenced by these authors themselves, when they argue that "the principle of privacy obviously poses some difficulties for this new voting channel via the Internet. The problem of 'family voting' and similar possible influences on the individual voter's decision represents a major criticism of the use of Internet voting" (Trechsel et al., 2007: 15). This approach is also echoed in the Final Report of the OSCE/ODIHR's Election Assessment Mission to the 2007 *Riigikoku* elections, when they mention that "[s]ecrecy of the vote is composed of two aspects: the secrecy of the voting environment and the anonymity of the vote once cast" (OSCE/ODIHR, 2007b: 17). Thus, in Estonia, the concerns about group voting that we have identified as breaches of the individuality of voting are seen, more broadly, as breaches of privacy. Notwithstanding, we prefer maintaining the division of secret suffrage into three different dimensions, as it allows for a more granular understanding of the challenges of remote electronic voting to secret suffrage and a more accurate assessment of whether Internet voting would comply with this principle of democratic elections. This case is also more obvious when it comes to the approach by the OSCE/ODIHR observers, since their interpretation omits potential breaches of the secrecy of the vote that can take place from the moment the vote is cast (i.e., "secrecy of the environment") until it is anonymised. Since votes needs to be kept digitally signed while encrypted at least until the end of the advanced voting period, this phase spans a few days in which the content of the votes could be revealed while they are still digitally signed.

> "According to the teleological interpretation of the principle of secrecy, the act of voting is seen not as an aim but as a measure to guarantee freedom of voting, and the anonymity aspect of the principle of secrecy can be guaranteed. The analysis of the compliance of the Estonian e-voting system with the ICCPR (1976) has given positive results as well."

More specifically, it is argued that the "[sub-]principle of privacy is there to protect a person from any pressures acting against their free expression of a political preference" (Vinkel, 2016: 40). From this perspective, Ülle Madise (2007: 16) argues that "instruments aimed at securing secrecy can be adapted provided that voters are given the opportunity to freely vote for their preferred party without fearing condemnation or expecting moral approval or material reward". Such teleological approach to secret suffrage has been at the core of remote electronic voting from the outset[307] (Madise and Martens, 2006: 18; Vinkel, 2016: 40).

From the understanding that secret suffrage is not an end in itself, but a means to secret suffrage, follows that it cannot be imposed to citizens. Simply put, "[v]oting in privacy in the remote unsupervised Internet voting context is a right, not a duty" (Madise and Martens, 2006: 26). The burden of secret suffrage is then shifted from the electoral authorities, who for voting in polling station are responsible for ensuring the proper layout and the setup of the voting booths, the envelopes, etc. to the voter. Priit Vinkel explains this shift as follows (2016: 40):

> "the provisions enabling e-voting are based on the premise that the government has to trust the citizen and avoid, whenever possible, interference with decision-making at the individual level. The voter has to be aware of the risks, and he or she has to have the right to decide whether to use the opportunity of e-voting. Therefore, e-voting cannot, under the same conditions, replace traditional paper voting and should be considered a complementary solution."

Notwithstanding, Estonian electoral authorities are not alien to the conditions in which remote electronic voters cast their ballots. Instead, they have come up with a mechanism that can avoid –or at least mitigate– the concerns related to coercion and vote-buying, among those that are usually considered for voting from unsupervised environments. This rationale has been described by Ülle Madise and Tarvi Martens (2006: 18) as follows:

> "If we can not use compulsory privacy for guaranteeing the principle of freedom to vote, we must find another method. The Estonian election law gives the e-voter the right to alter the vote given by electronic means with another e-vote or paper-ballot whereby the paper-ballot has priority. So a 'virtual polling booth' is created: the e-voter can choose the moment, when she or he is alone, free of any possible pressure. On the other hand it is unefficient against purchasing of votes. The e-voters possibility to change their e-vote reduces the motivation to exercise any influence or pressure including offer money or goods for any votes"

[307] For example, Wolfgang Drechsler and Ülle Madise (2002: 239) describe that :

> "As to whether e-voting would influence these principles, the Minister and Ministry based themselves on […] a teleological approach to Constitutional interpretation, i.e. to say that Constitutional problems should be understood through the problems the given principles were meant to solve. As an example […], the principle of secrecy (raised most strongly in Parliament later on) was said to protect and individual from any pressure or influence against her or his free expression of the political preference – i.e., that it is a means, not and end. This includes the threat that the state or a public official can check who voted for whom"

Therefore, and as argued by Priit Vinkel, "in the case of Estonia, the legal norms comply with the constitutional provisions, because […] the 'virtual voting booth' (the right to replace an e-vote with another e-vote or a paper ballot) and the virtual double-envelope system ensure the freedom of anonymous voting and the uniformity of elections"[308] (2016: 42).

To sum up, a description of how privacy is preserved can be found in the 2005 decision of the Supreme Court of Estonia that deals with the constitutionality of remote electronic voting (Supreme Court of Estonia, 2005),

> "[u]pon voting by electronic means a voter makes his or her choice, which shall be encoded. At the end of the voting procedure the voter shall approve the choice by his or her digital signature, which means that personal data is added to the encoded vote. The personal data and encoded vote shall be stored together until the counting of votes on the election day, with the aim of ascertaining that the person has given only one vote. The personal data of a voter and the e-voting given by the voter shall be separated before the counting of votes, after the fact that the voter has given only one vote has been checked. As it is not possible to transfer the votes together with personal data into the computer counting the votes, the secrecy of voting is also guaranteed."

The teleological approach towards secret suffrage in remote electronic voting may have paved the way for the widespread use of this channel in contemporary elections in Estonia. Notwithstanding, and as we have already seen, it did not prevent criticism towards the new voting channel. For example, we have already mentioned that there were certain political parties who initially opposed the use of remote electronic voting, primarily due to concerns regarding secrecy of the vote. The OSCE/ODIHR (2007a: 6) describes their stance as follows:

> "These parties expressed concerns that the unsupervised nature of remote voting makes it impossible to observe, thereby creating the potential for illegal pressure, coercion or inducement of voters. They noted that such occurrences could potentially take place in a voter's home or workplace, and additionally stated that any person with a laptop computer and ID card reader could travel to residences and 'collect' votes."

In addition to political criticism, "[d]uring the first ten years, complaints on equality, secrecy, technical uniformity, procedural soundness and security of the system have been raised. However, no violations have been found" (Vinkel, 2016: 43). For which a major theme was, indeed, the privacy and the secrecy of the vote. Such concerns make sense if, as Priit Vinkel has argued, the privacy and the secrecy of the vote "are arguably the most

[308] Recently, Arne Koitmäe, Jan Willemson, and Priit Vinkel (2021: 143) have succinctly summarised this approach as follows:

> "In the jurisprudence of the model case of Estonia, the current thinking regarding secrecy and Internet voting is based on the teleological approach, meaning that constitutional principles should be understood through the problems these principles were meant to solve. It was first noted in 2004 as the underlying motivation for the draft legislation allowing for Internet voting. In addition to that, the second source of the current approach is the liberal idea of trusting the voter. The principle of secrecy would protect an individual from any pressure or influence against her or his free expression of a political preference. Thus, the principle of secrecy is a means, not an end goal. Influence resistance in the Estonian i-voting system is guaranteed by the possibility of re-voting, thus the principle of secrecy, the end goal, is actually achieved. This approach has now been generally accepted and expanded on as not just the reasoning behind the original draft legislation, but as the actual explanation to how Internet voting conforms to the principle of secret ballot."

important issues in any electronic voting system, as they form the backbone of the secret ballot, which is central to democratic elections" (Vinkel, 2016: 55).

The teleological approach of secret suffrage also has found some critics. For example, according to Ülle Madise (2007: 17), Hubertus Buchstein has called this re-interpretation of the principle of secrecy into question. In the opinion of this author (Buchstein, 2005: 120),

> "any critique which weakens the normative status of the secret ballot faces a dilemma: on the one hand such a critique is necessary in order to put pressure on political reforms which will foster concern for the common good; on the other hand any weakening of the status of the secret ballot may give way to an even further privatization of politics through online-voting."

II. REMOTE ELECTRONIC VOTING AND SECRET SUFFRAGE: STANDARD BY STANDARD

So far, we have already covered the international and national regulations of secret suffrage in remote electronic voting, as well as the national (re)interpretation of this principle and some of the most important concerns. It is now time to assess to what extent the introduction of remote electronic voting in the three experiences has complied with the standards of secret suffrage and which mechanisms have been put in place to guarantee this principle (i.e., sub-question 2: do the technical solutions used to conduct remote electronic voting procedures guarantee the principle of secret suffrage?).

To that end, in this section we plan to assess each of the three national experiences, as well as the international standards presented in section I in this chapter, against the standards of secret suffrage already introduced in chapter 2, namely: individuality, confidentiality, and anonymity:

- Individuality: each voter makes and individual choice.
- Confidentiality: only the voter should know how they have voted, and the voter should be able to make their choices in private.
- Anonymity: there must be no link between the vote cast and the voter's identity.

We have already seen that these standards are acknowledged in the international standards and the national experiences, at least to some degree. For example, in Estonia a similar approach has been found in which the principle of secret suffrage is broken down into the "sub-principles" of privacy and anonymity. There is no doubt that both the standard of anonymity and the Estonian sub-principle enshrine the same values. Similarly, the sub-principle of privacy is aimed "to protect an individual from any pressure or influence against her of his free expression of political preference" (Madise and Martens, 2006: 18) and therefore fits well with the standards of individuality and confidentiality. At this point we should therefore decide whether to keep these two standards separate or analyse them together.

On the one hand, it makes sense to consider both individuality and confidentiality as just one standard or "sub-principle". At the end of the day, only if each voters makes their choices in private will they make an individual choice. Similarly, if only they should know how they have voted, they must make their choice in private. It goes without saying that if someone were to vote together with more people, they would not be able make their choices alone and they could not keep these choices secret from those being with them at

the time of voting. That is why it may seem wise to consider both individuality and confidentiality as one single standard.

Notwithstanding, our approach will still maintain a clear-cut distinction between individuality and confidentiality, as two different –yet reinforcing– standards. In our view, it is important to distinguish the threats against secret suffrage that may arise from the voter not making an individual choice, and more specifically if they are being bribed or coerced (i.e., individuality), from those breaches of confidentiality that may result at any other stage of the voting process (e.g., while the vote is being cast from the voting device to the voting server, or while stored in the voting server before the counting stage). Furthermore, and as we will argue in the next chapter, there is a possibility for the confidentiality of the vote to be breached at the casting stage, even if the voter is making an (apparently) individual choice.

We are aware that such a distinction is not always clear-cut. In fact, we acknowledge that this approach based on standards is indeed artificial. In truth, the three standards complement each other, and only when the three of them are met can we truly speak of secret suffrage being observed. For example, if there were to be no confidentiality (the contents of a vote could be revealed at any time) it would be impossible not to create a link between each vote and the voter who has cast it (thus breaching, in turn, anonymity). Likewise, if there were a link between the vote cast and the voter's identity (as it happens indeed within some jurisdictions), the possibility would always exist to know how each voter has voted (thus partially breaching confidentiality). In the absence of measures preventing any such breaches, it would be more difficult to guarantee the standard of individuality, since it would be easier for vote-buyers and coercers to influence a voter's decision. Notwithstanding, from a research perspective we still see value in this disaggregated analysis and will maintain it for our assessment.

On the other hand, we agree with Priit Vinkel that "[t]he fact that it is not possible to fulfil all of the theoretical and conceptual requirements set for an (originally paper-based) voting system is not enough for declaring e-voting to be unconstitutional" (2016: 41) or that secret suffrage is not observed. Therefore, what needs to be assessed here is whether and how remote electronic voting can comply with the values behind secret suffrage, that is: its standards –or "sub-principles"–, its *telos*. Furthermore, "[r]emote electronic voting as a concept is never absolutely secure (the same applies to any voting method). Constant development of the system needs to be maintained to stay ahead of possible risks and threats" (Vinkel, 2016: 42). For these reasons, it is also worth maintaining this granular approach, because it is more useful to identify and assess these specific risks and threats to each standard.

1. Individuality

For these reasons, our starting point is the principle of individuality, as something different but complementary to confidentiality. Individuality has been defined as *each voter making an individual choice*. The threats to individuality come from group voting, and from other forms of coercion and vote-buying. When the voter is being coerced or bribed, their choice

is actually being made, respectively, by the coercer and the vote-buyer and not by the voters themselves[309].

The Council of Europe's Recommendation on e-voting enshrines individuality in two of its standards (Council of Europe, 2017a):

> Standard No. 19: "[e]-voting shall be organised in such a way as to ensure that the secrecy of the vote is respected at all stages of the voting procedure"
>
> Standard No. 23: "[a]n e-voting system shall not provide the voter with proof of the content of the vote cast for use by third parties"

The Guidelines on the implementation of standard No. 23 provide some additional information on how to observe this standard. For remote electronic voting it provides that "no residual information[310] related to the voter's decision should be displayed after the vote has been cast" (Council of Europe, 2017c). The guidelines also stress the importance of informing voters about these risks and giving recommendations to mitigate them. In the case of remote electronic voting, the Guidelines provide extensive advice about the need to inform voters of these risks[311]. The provisions in the Explanatory Memorandum on

[309] The two cases are obviously different. If there is coercion it goes without saying that the voter is not making an individual free choice. In the case of vote-buying, however, the voter may individually make the choice to sell their vote. It may be more difficult to consider this threat as an actual breach to the freedom of the voter. The same goes for certain practices in which abstainers voluntarily vote on behalf of someone else who experiences difficulties to vote, such as voters abroad (e.g., Sánchez Sánchez, 2015). In spite of such voters making an individual and theoretically free choice to give away their votes, vote-buying (even if for free) is undoubtedly a breach of secret suffrage, and we will continue considering it as such.

[310] According to the guidelines (Council of Europe, 2017c: standard No. 23):

> "The term 'residual information' refers to information that remains accessible at various locations (in the personal computer's memory, the browser cache, the video memory, swap files, temporary files, etc.) after the vote has been cast and which may reveal the voter's decision.
>
> The provision advises the system developers or service providers to design the e-voting system in such a way that residual information is deleted after the vote has been cast. Technically there may be limited means to ensure this in a remote voting environment. Nevertheless, every measure possible should be taken to delete such residual information when the vote has been cast. However, individual verifiability can be implemented provided adequate safeguards exist to prevent coercion or vote-buying."

[311] The guidelines are completed with the following provisions (Council of Europe, 2017b: standard No. 23):

> "In the case of remote e-voting, voters should be clearly informed of the risk of breach of secrecy of the vote and on measures and good practices to adopt to counter this risk, for instance by using firewalls, cleaning traces, etc. The system itself should delete automatically as many such traces as possible.
>
> E-voting from a remote, uncontrolled environment implies shared responsibilities between the voter and the e-voting system/election administration body. It is part of the voter's responsibility to adopt the recommended measures (referred to in this provision). It is the duty of the electoral authority to clearly inform the voter on at least three points: the principle of shared responsibilities; the different measures to be adopted by the voter to reduce risk (running an anti-virus software, firewall, deleting traces of the vote, etc.); and remaining risks and verifiability techniques.
>
> Such information should reach the voter well ahead of the voting period. Based on this, the voter can decide whether or not to use remote e-voting.
>
> Warning messages may appear at the beginning of the e-voting procedure; a message on recommended steps that the voter should follow after voting (deleting traces, for instance) may need to be transmitted to the voter at the end of the e-voting procedure. However, such messages are only reminders and do not replace the initial complete information that the voter should receive ahead of the e-voting period."

receipt-freeness are even more detailed[312]. They distinguish between possible breaches of this standard at the level of the web application, the browser, and the utility software on the computer of the voter (although it should possibly read voting application, since not all voting clients are web-based). The provisions of the Explanatory Memorandum are also interesting because they distinguish the technological dimension of such breaches, and propose both technological and legal measures (i.e., criminal law provisions that deal with violations of individuality).

Lastly, it is important to highlight that such provisions do not preclude the adoption of individual verifiability mechanisms, something that is specified both in the Explanatory Memorandum (Council of Europe, 2017b: para. 70). We will get back to the latent ambiguities introduced by individual verifiability in chapter 5.

The interpretation of this standard in the three national experiences is somehow different. In the three cases, the burden of voting individuality from unsupervised environment is placed on the voter, although criminal provisions against coercion and vote-buying still apply. For Estonia, Sutton Meagher (2009: 368) has described the importance of the legal guarantees as follows:

[312] Relevant provisions in the Explanatory Memorandum regarding Standard No. 23 are the following ones (Council of Europe, 2017b: para. 70-74):

> "70. The aim of this standard is to prevent the breach of vote secrecy as well as vote selling. However, individual verifiability can be implemented provided adequate safeguards exist to prevent coercion or vote-buying.
>
> 71. Provisions that handle cases of breach of vote secrecy or vote selling should be in place. In many countries criminal law provisions deal with such violations. They cover all voting channels used and should apply also when e-voting is used. If necessary they should be updated to take into account e-voting specificities.
>
> […]
>
> 73. In a remote e-voting system using the internet, the voter should be informed on the necessity to delete traces of the voting transaction from the device used to cast the vote and on how to do so. Such traces could be kept for instance in the personal computer's memory, the browser cache, the video memory, swap files, temporary files, etc.
>
> 74. Specific attention should be paid to the way in which the anonymity and secrecy of the vote are implemented when designing an e-voting system. With respect to remote e-voting, there are at least three layers to be considered: the web application, the browser and the utility software on the computer of the voter.
>
> a. The web application should not allow the user to retain a copy of his or her vote. It should not offer the functionality of printing, saving or storing the vote or (part of) the screen on which the vote is visible.
> b. The browser should not offer the option of printing the screen on which the vote is visible. It should be noted that browsers can and do retain information in several ways. For example, by using the 'back' button on a browser, one or more previous screens can be displayed. As far as possible, this generic functionality of browsers should be disabled by the web application. At the very least, there should be no storing of information after the voter has finished casting the vote.
> c. Pieces of software that can record in some way what actions a specific user of a computer has performed have to be accounted for. Three common examples are screen shot utilities, utilities that make films of the sequence of screens and utilities that record the key strokes a user makes. Such software can be present as malware in the user's computer, without the user's knowledge. The e-voting system may not be able to prevent the presence of such malware. The voter should be informed about the possibility of such malware, the potential risks they present, the good practice to be adopted by him or her to minimize the risks and, more generally, about alternative and more secure voting channels that are open to him or her."

> "Estonian laws provide effective protection against voter coercion[313] with a two-way approach that criminalizes coercion and places a duty on voters to keep their vote secret. The Estonian election laws require that 'a voter shall vote himself or herself'. This affirmative duty protects the secrecy of the ballot because it prohibits a voter from allowing another person to vote in his or her place. Estonia's laws also make it a crime to influence or coerce a voter. Although Estonia's criminal laws do not specifically contemplate coercion in the context of Internet voting, the broad language of the statutes permit the government to enforce the criminal provisions against coercive conduct directed at Internet voters."

In the two other experiences, criminal provisions against coercion and vote-buying exist as well. For example, art. 281 of the Swiss Criminal Codes criminalises electoral bribery, understood as the purchase or sale of votes (Swiss Federal Council, 2006: 5260). Nevertheless, "Switzerland having already a generalised system of distant postal voting, threats related to 'family voting' are not considered as they are not specific to e-voting" (Driza Maurer, 2019: 91).

In addition to the criminal provisions on vote-buying and coercion Estonia has introduced an innovation by giving voters the option to re-vote. The option to re-vote (also referred to as multiple voting) is expected, precisely, to mitigate some of the concerns linked to coercion and vote-buying, such as group and family voting. This approach has been succinctly described by Kristjan Vassil in the following terms[314] (2016: 9):

> "An often-debated issue in terms of internet voting is the question of how to ensure vote secrecy in unsupervised environments. Because internet voting does not ensure that voters cast their votes alone, the validity of internet voting must be demonstrated on other grounds. To ensure that the voter is expressing their true will, they are allowed the change their electronic vote by voting repeatedly (electronically) during advance polls or by voting at the polling station during advance polls. This mechanism ensures that the vote buyer or coercer will not know for sure which ballot will be eventually counted rendering vote buying or coercing meaningless"

Importantly, the option to cast multiple ballots not only ensures that voters will be able to cancel a vote cast under coercion[315], but also disincentivises any attempt to buy votes.

[313] Nevertheless, it is important to notice that on the Final Report by the OSCE/ODIHR's Election Assessment Mission to the 2007 *Riigikohu* elections it is reported that (OSCE/ODIHR. 2007b: 24):

> "[t]here were a few cases reported of vote-buying schemes during advance voting. According to the CEC in Tartu, at least four cases were brought to the attention of Tartu authorities, with at least two persons admitting that they had received compensation for their vote. The ballot boxes in question were sealed, and a police investigation was initiated. The CEC later determined that the scale of the offence was so limited that cancellation of the results was not warranted. Investigations were also reportedly launched in Jogeva County. The Public Prosecutor took an active approach by publicly urging that any case of vote-buying be reported to the police"

[314] In a similar way, Sutton Meagher (2009: 369-370) has explained it as follows:

> "The Estonian election laws allow a voter to go to the polling place and recast an electronically cast ballot, which provides a safeguard in the event that another person coerced the voter or hacked into the Internet voting system and manipulated the vote tally. In the event that a voter does recast her ballot at the polling place, the ballot at the polling place will cancel out the electronically cast ballot. The Estonian Supreme Court has held that this provision is necessary to bring the Internet election law into compliance with the Estonian Constitution, because it ensures that a voter who has been coerced still has the opportunity to vote a secret ballot."

[315] For example, in Alexander H. Trechsel et al. (2007: 15) it is noticed that

Since a voter can cancel their vote at any time, a vote buyer will not have any guarantees that the vote that they have bought will be actually included in the final tally. According to Ülle Madise and Epp Martens (2006: 21)

> "A voter who has been illegally influenced or watched in the course of electronic voting can restore his or her freedom of election and the secrecy of voting by voting again either electronically or by a ballot paper, after having been freed from the influence. In addition to the possibility of subsequently rectifying the vote given under influence, the possibility of voting again serves an important preventive function. When the law guarantees a voter, voting electronically, the possibility to change the vote given by electronic means, the motivation to influence him or her illegally decreases. There are no other equally effective measures, besides the possibility to change the vote given by electronic means, to guarantee the freedom of election and secrecy of voting upon electronic voting in an uncontrolled medium. The infringement of the right to equality and uniformity, which the possibility of e-voters to change their votes for unlimited number of times can be regarded as amounting to, is not sufficiently intensive to overweight the aim of increasing the participation in elections and introducing new technological solutions"

In fact, according to Unt, Solvak and Vassil, (2016: 81), the option to cast multiple electronic ballots and to cancel any electronic vote by casting a paper ballot has three main advantages:

- "First, if someone e-voted under duress, meaning they are coerced to vote in a specific matter, then the person can theoretically cast a new vote at a later time free from coercion.
- Second, the knowledge that a vote can be changed should clearly lower the effectiveness of using coercion or buying votes, maybe even make it wholly pointless, as the potential vote manipulator has no guarantee that their machinations will deliver the desired results.
- Third, if the e-voter is suspicious that their vote might have been compromised somehow (e.g., a malicious computer virus), then they can remove the potential threat and cast their vote anew from the same machine or another safe computer."

Individuality was a key concern during the introduction of remote electronic voting in the country and the option to re-vote was the mechanism envisaged to mitigate these concerns. According to the OSCE/ODIHR, already during the NAM ahead to the 2007 parliamentary elections (OSCE/ODIHR, 2007a: 6) certain political parties

> "expressed concerns that the unsupervised nature of remote voting makes it impossible to observe, thereby creating the potential for illegal pressure, coercion or inducement of voters. They noted that such occurrences could potentially take place in a voter's home or workplace, and additionally stated that any person with a laptop computer and ID card reader could travel to residences and 'collect' votes."

> "To guarantee the voter's expression of free will the right to change the e-vote is applied. After having cast a vote, the voter can change his/her mind an unrestricted number of times and only the last e-ballot is count. Furthermore, the priority of the paper-ballot tackles the problem of "family-voting": manual e-voting is allowed and if the vote is cast in paper during advance polling station voting days, the e-vote is revoked."

Along these lines, Wolfgang Drechsler and Ülle Madise also reported on the public response to such threats. According to these authors (2002: 239)

> "the problem that e-voting would facilitate some families, friends or colleagues voting together, i.e. practice collective voting, as well as the buying and selling of votes, was said to hinge on the question of whether the State would have to protect an individual only from other individuals or also from her- or himself. It was not seen that collective voting could be a problem for the state as well, and not only for the individual"

Notwithstanding, among the three national experiences the Estonian case is unique[316]. In fact, the option to re-vote is strictly forbidden in Switzerland and France[317]. In the Swiss case, the OSCE/OIDHR (2007c: 8) reported it as follows:

[316] A different matter is how effective multiple voting is to mitigate coercion and vote-buying, if it can be measured at all. One interesting finding from the study commissioned by the Council of Europe for the first elections where remote electronic voting was used in Estonia shows that, while the overall majority of electronic votes were cast from home (from where 54,5% all e-votes were cast), the second voting place was for the workplace and/or educational institution (36,6%) (Breuer and Trechsel, 2006: 14). The report by Ülle Madise, Priit Vinkel and Epp Maaten also provides an analysis of the IP addresses from where most e-votes were cast during this election. The most common IP addresses in 2005 were "Ühispank offices, Citizenship and Migration Board and Tallin City Government, and also the offices of Elion, EMT and Hansapank […] A number of state agencies and large enterprise Eesti Energia follow, i.e. the places where workers have the possibility to use computers with Internet access and ID card reader" (Madise, Vinkel and Maaten, 2006: 37). The second study commissioned by the Council of Europe, for the 2007 parliamentary elections, also found that "a large majority of e-voters cast their e-ballot from home (68.3 percent) or at their workplace (28.4 percent). Only a very limited number of e-voters (2.8 percent) logged onto the system in order to vote from another place, i.e. a café, a friend's place, or a public Internet access point" (Trechsel et al., 2007: 27). These findings may indeed be explained by issues of access to Internet or smart-card readers, but those are also the spaces where votes could have been cast under the duress of a family member or an employer. Aware of these concerns, Sutton Meagher (2008: 383) recommends that

> "Estonia should place restrictions on the locations from which voters may cast online ballots. Such restrictions would enhance the secret ballot element of the Internet voting system and reinforce the secret ballot standards of the ICCPR. Because many of the fears of undue influence often involve voting that might occur in a voter's work place, Estonia should make it a crime to vote at work and also require employers to block the NEC website from workplace computers."

Given the importance of this mechanism, we will discuss it further in the next chapter.

[317] In contrast, in the two cases the standard of individuality is diverted towards voter identification. For example, the Swiss Federal Council reported in its first report on e-voting that (2002: 633-34):

> "Swiss case individuality is intrinsically linked to voter identification. For instance, in its feasibility study, the Swiss Federal Council highlighted the need to identify voter while respecting the secrecy of the vote (2002: 634). At this stage, several mechanisms were suggested, including identification code, passwords, or personal identification numbers, or even cards, such as a SIM card, a CD card, or a smartcard."

For example, in France similar concerns are repeatedly echoed by Jacky Deromedi and Yves Détraigne (2018: 45-46)

> « L'identification des électeurs représente l'une des principales difficultés du vote par Internet : l'identité de la personne qui se connecte sur la plateforme est difficilement vérifiable, en particulier lorsque plusieurs membres d'une famille votent sur le même ordinateur […] Dès lors, il paraît nécessaire de sécuriser l'identificaion des électeurs, notamment en ayant recours à des techniques biométriques. Cette identité numérique pourrait aussi ouvrir l'accès à d'autres services administratifs, sous réserve de la nécessaire protection des données à caractère personnel.
>
> […]
>
> L'exemple estonien illustre les possibilités offertes par l'identité numérique, notamment en termes de simplification des démarches administratives. Ce modèle n'est toutefois pas directement transposable en France car il nécessite de centraliser de nombreuses données à caractère personnel au sein d'un même dispositif informatique »

> "The Federal Act on Political Rights, as well as cantonal laws and regulations, provide for the secrecy of the vote as being a responsibility of each individual voter. Interlocutors acknowledged that this cannot be directly enforced with postal voting, but referred to the political culture of Switzerland and the ethical stand of the voters, which would theoretically ensure that secrecy of the vote is guaranteed."

Interestingly, in the Swiss case it was even discussed whether voters should choose a voting channel ahead of each vote[318]. However, the Swiss expert group warned that voters would not have the option to decide in the last minute whether to vote online or on paper, or switch the voting channel in case of irregularities[319].

This option does not exist in France either. For example, the OSCE/ODIHR's observation mission to the 2012 legislative elections stressed that "[o]nce the voter cast his/her vote, it could not be changed even if cast by mistake or under pressure" (2012c: 10). The French case highlights an interesting contradiction. In the recent Senate report analysing the introduction of remote voting channels for the 2021 regional and departmental elections, it was noted that voters should keep the right to vote in polling stations, even when they had already voted by post[320] (Buffet, 2020: 29). Yet, when voting electronically voters are prevented from changing their vote[321]. Interestingly, this is the result of a legal requirement[322] and the subsequent technological design, and not a technological constraint. The same terms in which voters could cancel their remote ballot by going to the polling station and casting a paper one could be prescribed both for postal and for remote electronic voting.

According to Ardita Driza Maurer, "France and Switzerland do not allow multiple voting and assign the same value to a validly issued ballot, be it on paper or electronic" (2014: 114). In turn, the current Recommendation (2017)5 on e-voting neither recommends nor

[318] The Swiss expert group on remote electronic voting discussed this option in the following terms (2018 : 5):

> « la dématérialisation soulève aussi la question de la dissociation du canal que constitue le vote électronique. […] il va peut-être falloir mettre en place un système dans lequel les électeurs devront choisir avant le scrutin le canal de vote qu'ils utiliseront (par ex. au moyen d'une procédure leur permettant de s'inscrire pour voter par voie électronique). Cette solution reviendrait à renoncer au principe que l'on connait aujourd'hui, qui consiste à pouvoir opter à tout moment pour le canal de vote de son choix. Les modalités de la dématérialisation sous la forme d'un vote électronique économe en papier doivent être établies de manière à laisser aux cantons une marge de manœuvre pour imaginer leurs propres solutions. »

[319] Within the current framework, a voter can decide not to confirm the vote that they have cast and instead cast their vote by post or in polling stations. However, should they be supposed to choose a channel ahead of each vote, this option would no longer be possible. Therefore, the Swiss expert group on remote electronic voting (2018 : 29) concluded that:

> « Les électeurs concernés ont aujourd'hui la possibilité d'interrompre le processus électronique après réception du code de vérification et d'exprimer leur vote en recourant à un canal classique. La possibilité de rabattre sur un canal éprouvé est notamment dans l'intérêt des électeurs dont le vote pourrait avoir été manipulé et de ceux qui se sentent désorientés durant le processus de vote par voie électronique. »

[320] In principle, such right would result from potential changes or news during the campaign that could modify the opinion of the voter to modify their vote.

[321] Art. R 176-3-9 of the Electoral Code

[322] In the opinion of François-Noël Buffet, "[w]hile this rule simplifies the organization of the election and makes it possible to avoid 'double votes', it directly calls into question the primacy of voting at the ballot box" (2020: 49).

precludes multiple voting[323]. Why such different approach? For Ardita Driza Maurer, France and Switzerland's "point of view is that internet voting is just another form of distant voting from an uncontrolled environment, and that coercion will not be addressed differently for internet voting than for postal voting" (2014: 114). As we will show in the next chapter, this approach is flawed and fails to take into account the differences between paper-based and remote electronic voting channels. For this reason, it will be important to resume the discussion on multiple voting as part of chapter 5 (and, more specifically, in section I.2.a)).

2. Confidentiality

The second standard of secret suffrage is confidentiality. Confidentiality means that *only the voter should know how they have voted, and they should be able to make their choices in private*. This standard applies from the moment the vote is cast and until the announcement of the results, or even longer if there is a recount (PACE, 2007b: 7).

Several standards of the Council of Europe's Recommendation deal with confidentiality[324] (Council of Europe, 2017a):

> Standard No. 19 "[e]-voting shall be organised in such a way as to ensure that the secrecy of the vote is respected at all stages of the voting procedure"
>
> Standard No. 24 "[t]he e-voting system shall not allow the disclosure to anyone of the number of votes cast for any option until after the closure of the electronic ballot box. This information shall not be disclosed to the public after the end of the voting period"
>
> Standard No. 25 "[e]-voting shall ensure that the secrecy of previous choices recorded and erased by the voter before issuing his or her final vote is respected"
>
> Standard No. 44 "[i]f stored or communicated outside controlled environments, the votes shall be encrypted"
>
> Standard No. 45 "[v]otes and voter information shall be kept sealed until the counting process commences".
>
> Standard No. 46 "[t]he electoral management body shall handle all cryptographic material securely"

However, and in contrast to individuality, the Guidelines touch upon these standards only succinctly. For example, on standard No. 19, the Guidelines specify that "[w]here votes and anonymised[325] [sic] voter information are kept together, end-to-end encryption

[323] Nevertheless, multiple voting literally contradicted the phrasing of legal standard No. 5 in the (2004)11 Council of Europe Recommendation, which read that "[i]n relation to any election or referendum, a voter shall be prevented from inserting more than one ballot into the electronic ballot box" (Council of Europe, 2004a: 2). Notwithstanding, the Supreme Court of Estonia (2005) and Jordi Barrat et al. (2012) concluded that giving voters the option to cast multiple votes could be interpreted to respect the Recommendation. On this topic, see also Jones (2004) in Driza Maurer (2014: 114).

[324] Appendix II of the Recommendation contains a definition of confidentiality. It is understood as "the state characterising information that should not be made available or disclosed to unauthorised individuals, entities or processes" (Council of Europe, 2017a). When we speak about confidentiality, however, we limit who can access the information about how a voter has voted only to the voter who has cast it, and nobody else. As we will see later, in computer *jargon* this information is usually referred to as private information.

[325] For a discussion on the use of anonymisation, see footnote 350 in the next section.

must protect this information" (Council of Europe, 2017c). Since our focus is on remote electronic voting, and in line with standard No. 44, it should be understood that the vote shall be encrypted from the moment it is cast (since the casting implies that the vote is communicated and stored outside controlled environments). In turn, the guidelines on standard No. 46 prescribes that "the private cryptographic keys should be generated at a public meeting and should be divided in separate parts and shared by at least two people who are unlikely to collude" (Council of Europe, 2017c). Therefore, this provision can be understood as recommending the use of a key-sharing mechanism[326].

The Explanatory memorandum is a bit more detailed. For example, when it comes to standard No. 19 it specifies that "[t]he necessary measures include of course encryption[327]" (Council of Europe, 2017b: para. 64). For standard No. 24, it is explained that "[t]his standard aims at preventing the establishing and publication of intermediary results of the e-voting channel" (Council of Europe, 2017b: para. 75). Therefore, it is not clear whether the ultimate goal of this provision is to ensure the confidentiality of the votes or to guarantee the principle of equal suffrage by preventing partial results from being known[328]. In practice, encrypting the votes may ensure both secret and equal suffrage, but since this Standard is described under the section dealing with secret suffrage it should be rephrased to focus on confidentiality. In turn, standard No. 25 extends the guarantee of confidentiality to previous choices, by requiring "that the secrecy of previous choices which were entered and then deleted by the voter during the voting process shall receive the same protection as the secrecy of the final vote" (Council of Europe, 2017b: para. 76). The Explanatory Memorandum further develops Standard No. 44 prescribing both the encryption of the votes as well as of the ballot box[329]. Lastly, when it comes to Standard No. 46 the

[326] According to Steven Levy, "secret sharing" was one of the most significant creations in cryptography. Its development is explained as follows (Levy, 2001: 165):

> "Only two years after helping invest RSA, Shamir had been intrigued by what he considered to be a problem looking for a solution–how do you share a single key among several parties, particularly when mistrust and suspicion festers among them? The classic situation is an electronic equivalent of what happens in nuclear missile silos: in order to launch, multiple keys must be turned simultaneously, requiring more than one person. Could you replicate this safeguard in cyberspace? It turns out you could, and once Shamir got to thinking about it, he came up with the idea of secret sharing, a means to parcel out a decryption key among several people. If a foe got hold of an individual's share of the key (known as a 'shadow'), he or she would have no advantage in an attempt to retrieve the entire key."

[327] Encryption is not defined in the recommendation. Therefore, we understand is as defined in footnote 271. According to Keith Martin, "a good cryptographic algorithm should behave like a random number generator. If you encrypt some data, then the result should appear "nonsensical" and lack any meaningful patterns. This apparent randomness can be sent over the internet, with anyone who observes it seeing merely bland numerical fog" (2020: 38)

[328] According to the Swiss Federal Council (2013a: 72),

> « [l]a question du moment du décryptage de l'urne électronique a été traitée sous l'angle du secret du vote. Ce dernier protège également contre toute révélation anticipée des résultats du scrutin, même partiels, du vote qui pourrait conduire à une mobilisation de dernière minute dans le but d'influencer l'issue du scrutin. Lorsqu'il donne son autorisation, le Conseil fédéral détermine également le moment à partir duquel l'urne peut être décryptée et rappelle que tout divulgation de résultats, même partiels, avant midi le dimanche de scrutin est interdit. Les cantons quant à eux connaissent le dépouillement anticipé notamment dans le cadre du vote par correspondance (dépouillement manuel), ce qui leur permet de publier des résultats rapidement après la fermeture des urnes. Ils adoptent des mesures organisationnelles a fin d'empêcher toute publication de résultats. »

[329] It clarifies that (Council of Europe, 2017b: para. 132):

> "From the moment the vote is cast, no one should be able to change it or relate the vote to the voter who cast it. This is achieved, among other measures, by the process of sealing the ballot box,

Explanatory Memorandum "reminds that adequate, state of the art procedures must be foreseen for the handling of cryptographic material" (Council of Europe, 2017b: para. 135).

All in all, these provisions therefore prescribe the "sealing" or the encryption of the votes. In principle, according to the Guidelines on Standard No. 19 by using end-to-end encryption at least when votes and anonymised voter information are kept together, and in all circumstances for remote electronic voting, according to Standard No. 44. In addition to encryption of the votes, the ballot box should also be protected. In turn, both technological (i.e., firewalls) and procedural guarantees are suggested (such as control of access and authorisation structures). These are to be combined with secure procedures for the handling of cryptographic "materials", such as key-sharing mechanisms (Guidelines on Standard No. 45).

a) The encryption of the vote

When it comes to confidentiality, we observe more similarities between the three national experiences. For example, in all three cases end-to-end encryption of the vote is offered.

In Switzerland, confidentiality was envisaged as an important requirement from the outset. In this regard, already in the initial stage of remote electronic pilots in the country the Declaration of Intent between the cantons of Geneva, Neuchâtel, Zurich and the Federal Council set that no third party should be able to know the content of the votes cast electronically, out of four key requirements[330] (Swiss Federal Council, 2006: 5214). Among others, there were concerns that system administrators in corporate networks may attempt to observe how the employees voted (Swiss Federal Council, 2006: 5218). Thus, already in its 2000 feasibility report the Swiss Federal Council identified some basic mechanisms to guarantee the confidentiality of the votes, namely the security in the transmission of the votes (Swiss Federal Council, 2002: 633). Nowadays, such requirements are part of the Annex to VEleS (Swiss Federal Chancellery, 2018d):

- 2.8.2. It is guaranteed that neither employees nor externals obtain data before the decryption of the votes that allow early provisional results to be determined.

  […]

- 2.8.6. It is guaranteed that individual votes will be treated as confidential even after tallying.

The provisions on security requirements are even more specific (Swiss Federal Chancellery, 2018d):

> and where the ballot box is remote from the voter by sealing the vote throughout its transmission from voter to ballot box by using encryption. A vote is sealed when its content has been subject to the measures that ensure that it cannot be read, changed, or related to the voter who cast it.
>
> To seal and protect an electronic ballot box, physical and technical measures may be necessary, such as control of access, authorisation structures and firewalls."

[330] The three remaining criteria were that (Swiss Federal Council, 2006: 5214)

> « il doit être impossible de capter, de modifier, out de détourner les suffrages exprimés par voie électronique ; seules les personnes autorisées à voter doivent pouvoir voter ; toute personne autorisée à voter ne doit disposer que d'une seule voix. »

- 3.3.3. In order to guarantee the confidentiality of data records that substantiate voting secrecy and the avoidance of early provisional results, effective cryptographic measures that correspond to the state of the art must be used.
- 3.3.4. Votes must not be stored or transmitted in unencrypted form at any time from being entered to tallying.

  […]

- 3.3.6. Basic cryptographic components may only be used if the key lengths and algorithms correspond to the current standards (e.g. FIPS 143-3, NIST, ECRYPT, ESigA)."

In France, votes are also encrypted in the voter's device[331]. This is actually a requirement defined in the Electoral Code itself. Art. R176-3-9 sets that the vote is encrypted in the voting device from the moment it is cast. The CNIL recommendation prescribes confidentiality as well. In this regard, the following security objectives are all related to this standard (CNIL, 2019a: 3):

- "Security objective n° 1-04: Ensure the strict confidentiality of the ballot from its creation on the voter's computer.
- Security objective n° 1-05: Ensure the strict confidentiality and integrity of the ballot during its transport.
- Security objective no. 1-06: Ensure, in an organizational and/or technical manner, the strict confidentiality and integrity of the ballot during its processing and storage in the ballot box until the counting.

Lastly, also in Estonia "the voting software encrypts the cast ballot to prevent a third party from ascertaining for whom the voter voted" (Meagher, 2009: 358). This is usually referred to as the envelope scheme. The General Framework of Electronic voting defines this scheme in the following terms[332] (State Electoral Office of Estonia, 2017: 8):

> "I-voting is based on so-called 'envelope scheme', which is known from voting by paper mail, where an anonymous closed envelope with the vote is placed into an outer

[331] In his 2006 report, François Pellegrini explained it as follows (2006 : 6):

> « L'accès au site Web de vote […] se fait au moyen d'une connexion cryptée (utilisation du protocole HTTP sécurisé par cryptage SSL). Une fois ses identifiants personnels tapées, un « applet » (fragment de programme destiné à s'exécuter au sein du navigateur Web de l'électeur) est téléchargé, qui vérifie localement la conformité de son suffrage avec les règles de procédure électorale (nombre de candidats choisis, etc.) […] L'applet utilise alors une clé de chiffrement pour crypter le bulletin électronique, avant de le transmettre au serveur
>
> Cette clé de chiffrement est la clé publique d'une paire de clés, générée sur un ordinateur dédié peu avant l'ouverture du scrutin, et dont la clé privée, qui servira au déverrouillage de l'urne, a été tronçonnée en fragments conservés sur des supports numériques individuels remis au président et aux assesseurs du bureau de vote. »

According to Andrew W. Appel, "[a] Java applet is used, instead of just ordinary HTTP, so that the vote can be encrypted and then signed before it is sent over an SHTTP channel. Encrypting the ballot and signing it on the client machine is supposed to ensure the secrecy and authenticity of the ballot" (2006: 6).

[332] In a similar way, Kristjan Vassil (2016: 7) explains it as follows:

> "The downloaded e-voting app encrypts the vote (PIN1). The encrypted vote can be regarded as the vote contained in the inner, anonymous envelope. After this the voter gives a digital signature to confirm their choice (PIN1). By digitally signing the vote, the voter's personal data or outer envelope is added to the encrypted vote. Before the ascertaining of voting results during the evening of the Election Day, the encrypted votes and the digital signatures (i.e. the data identifying the voter) are separated. Then the anonymous e-voted are 'opened' and counted. The system opens the votes only after the personal data is remoted."

envelope with the voter's name and signature. With the help of the programme used for i-voting (so-called *Voter Application*), the i-voter:

1) Encrypts the vote and the random number generated by the computer with the elections-specific public key[333], forming the 'inner envelope';

2) Signs the encrypted vote by using a digital signature tool, forming the 'outer envelope'.

A vote encrypted with the public key can be decrypted only with the private key."

Therefore, the "Internet voting system employs two separate encryption keys–one for the voter to encrypt his [sic] ballot and another for the election officials to decrypt the ballot. This double-encryption method[334] creates a secure system that protects voter privacy" (Meagher, 2009: 368).

These experiences also show that, in addition to encrypting the votes, the voting channel can be encrypted as well[335]. In Switzerland, for example, "[v]oters could access the voting platform via an Internet browser protected by basic Secure Sockets Layer (SSL) technology" (OSCE/ODIHR, 2016: 7). In this way, the transmission of the votes from the voting client (the device used to vote) and the voting server is protected by means of the SSL standard (Swiss Federal Council, 2013a: 76). The use of SSL is reported as well in the

[333] It is important to distinguish between symmetric and asymmetric encryption. According to Keith Martin, "[a]n encryption algorithm in which the same key is used to both encrypt and decrypt is described as being *symmetric*" (2020: 59). In contrast, "[e]ncryption mechanisms in which different keys are used for encryption and decryption are referred to as being *asymmetric*" (Martin, 2020: 60). Whereas in symmetric encryption any of the parties that hold the key can encrypt and decrypt a message, the keys used in asymmetric encryption are different (although mathematically related). In this regard, "when Alice sends the scrambled message off, only one person in the world has the information necessary to reverse the calculation and decipher it: Bob, the holder of the private key" (Singh, 1999: 71). The difference between symmetric and asymmetric encryption is explained by Keith Martin as follows (2020: 77):

> "A digital padlock thus needs to be a form of encryption that allows anyone to encrypt but only the designated recipient to decrypt. Since everyone can encrypt and encryption involves a key, the key used for digital padlock encryption will need to be something everyone knows –in other words, a key that is *not* secret. Such a key is known as *public key* because ti can be made publicly available […]
>
> In contrast, the designated recipient should be the only person capable of unlocking a digital padlock. Just as for symmetric encryption, the key used to decrypt will need to be kept secret by the recipient. This key is usually referred to as a *private key*, because it is private to the key holder and not shared with anyone else, just as for a physical padlock key. In the case of asymmetric encryption, the keys used to encrypt and decrypt are thus *different*. Of course, even though the encryption key and decryption key are different, they must be related to one another in some way."

For this reason, asymmetric encryption is sometimes referred to as public key encryption (or more generally as asymmetric or public key cryptography). On this topic, see also Simon Singh (1999: 269-270).

[334] More specifically, the General Framework also clarifies that (State Electoral Office of Estonia, 2017: 11):

> "Secrecy is guaranteed by encrypting the votes with asymmetric cryptography tools. For every voting, the key pair of the system – a public key (encryption key) and private key (decryption key) is created with the help of the Key Application.
>
> The Voter Application uses the public key to encrypt votes. The private key is used in the Key Application to decrypt votes. After the voting results have been announced, the private key is exterminated [sic]."

[335] For an overview of some channel encryption protocols, see footnote 431 below.

French experience, against being a requirement set in the Electoral Code itself (Art. R176-3-9).

However, channel encryption is not sufficient by itself to guarantee the confidentiality of the votes. Switzerland shows us the reason why. Initially, in some Swiss cantons encryption was offered by only encrypting the voting channel[336], but not the vote itself, which was encrypted at the server-side of the voting application[337].

In these protocols, the encryption of the votes was assigned to different security servers whose task was to decrypt the incoming request, and then to encrypt them (Swiss Federal Council, 2002: 633). This approach had a vulnerability, since it is possible for the server to know how a voter have voted, which breaches their confidentiality. After the first pilot phase (2002-2005) the canton of Geneva started working on the development of a new encryption method that would enhance the protection mechanism against possible attacks between the voting device and the electronic ballot box (Swiss Federal Council, 2006: 5225). To do this, voters would have to install a specific application in the voting device[338]. This measure was justified by the evolution of possibilities in the security sector. However, by 2012 the canton of Zurich had not yet adopted this encryption method. In this regard, in 2012 the OSCE/ODIHR mission reported that "[w]hile the consortium system encrypts the vote only once it is received by the server, the Geneva system provides an additional layer of security by encrypting the vote on the voter's computer before it is sent" (OSCE/ODIHR, 2012a: 17).

[336] The exception here was Neuchâtel, where (Swiss Federal Council, 2006 : 5253).

> « les votes cryptés sont stockés directement dans l'urne, sans être décryptés puis recryptés. En plus de cryptage SSL, les données sont cryptées avant de transiter par le canal SSL. […] l'examen de la structure et l'intégrité des votes n'est effectué que lors du dépouillement, contrairement à ce qui se fait dans les cantons de Genève et de Zurich. »

In fact, already in 2004, the Swiss Federal Chancellery (2004: 42)reported for the pilot project in Neuchâtel that

> « [a]u niveau de contenu, il est envisagé de crypter le vote de l'électeur de bout en bout au moyen de clés publiques (cryptage asymétrique) contrôlées par les représentants des autorités ou des partis politiques. Le vote crypté sera ensuite déposé dans l'urne électronique, son contenu restant totalement illisible jusqu'à la clôture du vote. Ce n'est qu'à ce moment que les représentants des autorités et des partis politiques procéderont au décryptage et au comptage des votes après avoir enregistré leu clé privée. »

[337] The 2006 report by the Swiss Federal Council (2006: 5253) explains this process in detail:

> « Dans les applications pilotes de trois cantons, on distingue deux phases de cryptage. Un premier cryptage des votes ainsi que des données, d'identification et d'authentification est opéré sur l'appareil de saisie de l'électeur. Il s'agit là d'un cryptage usuel à 128 bits (SSL337), qui correspond aux normes de sécurité en vigueur dans le télébanking. Ainsi cryptés, les votes sont acheminés par Internet dans le système de vote électronique (réseau administratif) protégé par des pare-feu. Dans les cantons de Genève et de Zurich, les données entrantes subissent un contrôle de structure et d'intégrité avant d'être cryptés une seconde fois (au moins à 1024 bits) et acheminées dans la zone de haute sécurité, à savoir dans l'urne électronique. Ces données cryptées ne sont pas manipulées avant que le dépouillement ait lieu. »

[338] This was reported in the Swiss Federal Council's 2013 report (2013a: 61),

> « une appliquette java a été ajoutée, afin de sur-encrypter les données circulant sur Internet et de permettre d'authentifier l'électeur sur la base d'une dérivation de son numéro de carte d'électeur. Un contrôle de cohérence des votes à leur arrivée dans l'urne électronique a également été ajouté, afin d'éviter qu'un code exécutable ou des votes illisibles n'entrent dans l'urne et en altèrent le contenu. »

b) Sharing a secret

As important as the encryption of the votes is their decryption. In this regard, we have seen that the Recommendation proposes the use of key-sharing mechanisms. For this process we also see important similarities. In the three national experiences electoral commissions or committees have been set up to preserve the confidentiality of the ballots until the counting stage.

In the Swiss case, these commissions were set up already for the first trials[339]. They were formal organisations[340], in some cases gathering representatives from different political parties and from the cantonal administration[341], who were entrusted with

[339] The Swiss Federal Council (2006: 5258) describes their role in the following terms:

> « Dans les cantons de Genève et de Neuchâtel, le décryptage des votes électroniques ne peut être opéré que sous la surveillance d'une commission électorale. Seuls les membres de cette commission peuvent déclencher le processus de décryptage, car eux seuls disposent des mots de passe et des clés nécessaires » […] « Les clés électroniques qui servent à crypter et à décrypter tous les votes électroniques sont protégées par des mots de passe détenus par ces mêmes commissions. On empêche ainsi que des personnes non autorisées, notamment les membres des autorités électorales et même les administrateurs des systèmes (attaques internes) puissent accéder aux suffrages cryptés qui sont stockés dans l'urne. Les risques liés aux solutions mises en œuvre dans les systèmes cantonaux peuvent être qualifiés de faibles »

More specifically, for the case of Geneva decryption worked as follows (Swiss Federal Council, 2006: 5223):

> « Le dépouillement des suffrages électroniques a lieu dans les locaux de la police cantonale, en présence des contrôleurs des partis politiques. Un ordinateur personnel est relié à l'urne électronique par un câble distinct. Seuls les contrôleurs peuvent alors procéder au décryptage des suffrages en saisissant deux mots de passe qu'ils ont eux-mêmes créés à l'ouverture de la procédure de vote. »

In contrast, in Zurich the communes who were responsible for the decryption of the votes (Swiss Federal Council, 2006: 5255)

> « Dans le canton de Zurich, par contre, chaque commune est autorisée à activer séparément le décryptage et le dépouillement des votes au moyen de la saisie du mot de passe et du numéro de la clé. Tant les mots de passe que les clés sont envoyés aux communes par courrier postal. Le canton dispose d'une clé générale pour parer aux cas d'urgence »

[340] For example, the Canton of Geneva « à lui « formalisé » le rôle de la commission électorale en adoptant plusieurs dispositions à ce sujet. Cette instance est composée de représentants des forces politiques au Grand Conseil désignés pour une législature et pouvant s'entourner de spécialistes. […] Elle participe au cryptage et décryptage de l'urne électronique » (Swiss Federal Council, 2013a: 31). In the canton of Neuchâtel, their role has been described as follows (Swiss Federal Chancellery, 2004: 42):

> « Pour le dépouillement des votes électroniques le jour du scrutin, la commission électorale se réunit à nouveau en récupérant l'ensemble du matériel (poste de travail et enveloppées scellés) ramené par la Chancellerie d'Etat et par la Police cantonal. Les membres de la commission électoral récupèrent leurs cartes à puce et saisissent leurs mots de passe afin de libérer la clé privée pour le décryptage des votes. Une fois décryptés, les votes et les accusés de réception sont extraits et brassés. »

[341] For example, the electoral commission in Neuchatel has been described as follows (Swiss Federal Council, 2013a: 31):

> « A Neuchâtel, une pratique établie implique la commission électorale – instance composée de représentants des forces politiques au Grand Conseil et de l'administration cantonale – dans le fonctionnement du vote électronique. La Commission électorale détient une partie des clés de l'urne. Sa présence est indispensable au fonctionnement du vote électronique dans la mesure où elle participe au cryptage et au décryptage des votes de bout en bout. Tout décryptage est donc impossible en l'absence de la commission. »

In contrast, the commission in Geneva (Swiss Federal Chancellery, 2004: 34; Swiss Federal Council, 2006: 5222):

> « Avant l'ouverture du scrutin, l'urne électronique est verrouillée avec deux clefs digitales (des mots de passe) crées par les contrôleurs. Ils sont les seuls à connaitre et posséder ces clés. De la

safeguarding the keys necessary to decrypt the votes. However, the OSCE/ODIHR has found some shortcoming in the handling of these keys during the 2011 Federal Assembly elections (OSCE/ODIHR, 2012a: 18).

> "A particular concern in this regard was the handling of cryptographic material. Access to the private keys used to decrypt the electronic ballot box should be limited and closely monitored. In the consortium system, the private keys were generated by external operators and delivered to election officials in person via an insecure medium (CD ROM). The passwords to access the keys were also generated by the external operator and mailed to the election officials by standard post. While no problems were reported, such a procedure opens the possibility for external operators to access the private key and password, allowing them to impersonate an electoral official at any stage of the process. To decrypt the votes, election officials uploaded the key remotely to the consortium internet voting servers.
>
> In the Geneva system, the private key was generated at a meeting of the election commission with four members of different political parties present. The key was stored on insecure media (CD ROM and memory stick), sealed in an envelope and immediately passed to the police for storage. The password consisted of two parts, each part separately generated and retrained by different election officials, with a copy also provided to a notary in a sealed envelope. The election commission reconvened to jointly decrypt the votes."

For these reasons, the EAM recommended cantons to "adhere to good practice when handling cryptographic material, which provide that the private key be generated at a public meeting and that the key be divided in separate parts and shared by at least two people who are unlikely to collude" (OSCE/ODIHR, 2012a: 18). Instead of CD ROM, the OSCE/ODIHR recommended that the shares were generated and stored using secure cryptographic media such as smartcard (OSCE/ODIHR, 2012a: 18).

In France, the task of safeguarding the decryption key is entrusted to the members of the *bureau de vote électronique*. The law itself prescribes this procedure[342]. According to the Electoral Code, the key must be created and split at the beginning of the voting operations (art. R176-3-8) and the votes can be decrypted only with at least four of these shares (art. R177-5). From the moment voting ends on Wednesday and until the counting stage on Sunday, the president of the *bureau de vote électronique* safeguards the encrypted votes (art. R176-3-10).

Lastly, also in Estonia "[t]he generation of the key pair and the use of the private key are organised by several *keyholders*" (State Electoral Office of Estonia, 2017: 11). According to the State Electoral Office of Estonia (2017: 11)

> sorte, un contrôlé croisé des partis entre eux et des partis sur l'administration s'exerce à la fermeture et à l'ouverture de l'une. Durant le scrutin, l'accès au lieu physique où se trouve l'urne électronique est strictement contrôlé. »

[342] However, this procedure was already adopted in the first experiences with online voting. Some examples can be found in the report written by François Pellegrini (2006: 6) and by Bernard Lang (2006). The former described the procedure as follows (Pellegrini, 2006: 6)

> « la clé privée, qui servira au déverrouillage de l'urne, a été tronçonnée en fragments conservés sur des supports numériques, individuels remis au président et aux assesseurs du bureau de vote. […]
>
> Après la clôture du scrutin, le président et ses assesseurs joignent leurs fragment de clé privée pour reconstituer la clé privée complète, qui est utilisée pour décrypter le contenu de l'« urne électronique » et fournir les résultats de l'élection. »

> "The number and list of keyholders is determined under the established rules. The private key can only be activated I the previously agreed number of keyholders are present. Keyholders receive physical and knowledge-based keyshares (e.g. chip card and password) to activate the private key."

Originally, the private key was protected in Hardware Security Modules[343]. However, this process has evolved, and in 2011 the NEC "planed the setup of the Internet voting system, including key generation, between 15 and 18 February 2011" (OSCE/ODIHR, 2011a: 6). Four years later, the OSCE/ODIHR stressed that the generation of the key and its management by the NEC remained one of the critical processes to ensure the overall end-to-end security of the system (OSCE/ODIHR, 2015a: 6). Nowadays, the *Riigikogu election acts* prescribes this key-sharing mechanism, that during the counting of the votes works as follows (State Electoral Office of Estonia, 2017: 18):

> "Votes are opened and counted with the help of the Key Application in an off-line environment. Counting is organised by the Tallier together with the keyholders between whom the private key has been distributed.
>
> 1. Both the list of candidates and the list of electoral districts are loaded into the Key Application.
> 2. Anonymised (and optionally mixed) votes are loaded into the Key Application.
> 3. To activate the private key, the keyholders use the keyshares distributed to them in the course of the generation of the key pair.
> 4. Votes are decrypted. If, as a result of the decryption of the votes, it appears that the candidate is not listed among the candidates standing as candidates in the relevant electoral district, the vote is deemed invalid.
> 5. Eligible votes are summed by candidates and electoral lists. The counting process also issues a zero-knowledge tally-proof, which can be used to prove the correctness of the opening of votes.
> 6. At the end of the process, the private key is deactivated."

In a nutshell, several important issues can be identified from these experiences. First, not any sealing or encryption works, it has to be the encryption of the vote. Ideally, this encryption should take place at the level of the application, and not only channel

[343] According to the OSCE/ODIHR (2007b: 14)

> "The Counting Server decrypts the votes using the Hardware Security Module and counts them. By law, at least half of the NEC members, including the Chairman [sic] or Deputy, must be present in order to decrypt and count the votes. Decryption of the votes is performed by the Hardware Security Module (HSM). In order to enable the HSM, six physical keys must be inserted. Seven keys are in possession of the NEC members and two are held by the operators; four of the keys used must come from the NEC members"

This process is further defined in the following terms (2007b: 16)

> "no one can decrypt votes other than the NEC members together. The private key does not leave the Hardware Security Module […] The secure storage of votes was implemented by a tamper-evident Hardware Security Module which generated the digital key pair without revealing the private key. This module was stored in a secure place and was only used before the election for the set up procedure and after the election for the counting procedure." However, as detailed by the Mission, [t]o ensure the availability of the election results in the event of failure of the Hardware Security Module, there was a backup of the private key which was kept secret by one of the members of the NEC. The existence of a backup key creates a hypothetical security risk, which was assessed by the NEC as being more acceptable than the risk of not having the results available."

encryption. Furthermore, this encryption has to be asymmetric, that is: use public key cryptography. Only with the use of asymmetric encryption is it possible to use a different key for the encryption and the decryption of the votes. In addition to the technological means, the private key needs to be secured by the election administration.

c) Open questions on confidentiality

In addition to the encryption and the decryption of the votes, from the perspective of confidentiality three additional issues deserve special attention. The first one is related to the use of encryption and the restrictions imposed in Switzerland to voting online from abroad. The second issue is linked to whether confidentiality extends beyond the choices made by the voter to the knowledge of whether they have voted at all. The last of these issues has been already introduced in our analysis of the Council of Europe's Recommendation and is related to the protection of the voters' previous choices.

Limitations to the use of cryptography[344] and the encryption of the vote

First, and since confidentiality depends upon the encryption of the vote, it must be addressed whether there are limitations to the use of cryptography. This is an issue that was taken into account in Switzerland, where remote electronic voting from abroad was restricted to the EU, the state parties to the Wassenaar arrangement[345], to Andorra, Liechtenstein, Monaco, Saint-Martin, the Vatican City and Northern Cyprus. The restriction was aimed at guaranteeing that the countries from where it would be possible to vote online allowed their residents to receive and send encrypted data[346] (Swiss Federal Council, 2013a: 34). By 2013, about 90% of voters abroad where living in one of these countries. However, any Swiss voter not residing in one of them was directly excluded from remote electronic voting, even if the canton in which they were registered theoretically gave them access to Internet voting (Swiss Federal Council, 2013a: 101).

Interestingly, no such restriction has been put in place in France or Estonia, where the option to vote online is offered as well to voters abroad. For example, in the French case

[344] We have not yet offered a definition of cryptography. According to Simon Singh (1999: 6)

> "*cryptography* [is] derived from the Greek word *kryptos,* meaning 'hidden'. The aim of cryptography is not to hide the existence of a message, but rather to hide its meaning, a process known as *encryption* […] To render a message unintelligible, it is scrambled according to a particular protocol which is agreed beforehand between the sender and the intended recipient. Thus the intended recipient can reverse the scrambling protocol and make the message comprehensible. The advantage of cryptography is that if the enemy intercepts an encrypted message, then the message is unreadable. Without known the scrambling protocol, the enemy should find it difficult, if not impossible, to recreate the original message from the encrypted text".

[345] The Wassenaar Arrangement was signed in December 1998 by 33 nations. The arrangement limits arms exports, "which also covers powerful encryption technologies" (Singh, 1999: 311). Since there is no list of countries from where remote electronic voting is authorised or prohibited, the Swiss Federal Council based their decision in the fact that the signatory countries of the Wassenaar arrangement at least expressly authorize the electronic transmission of encrypted data (2013a : 101).

[346] The restriction was justified in the following grounds (Swiss Federal Council, 2013a: 101-102):

> « Les Suisses de l'étranger ont droit comme les autres au secret du vote, qu'ils s'expriment par voie électronique ou postale. En matière de vote électronique, c'est le cryptage des données qui garantit ce secret. Dès lors qu'un électeur parvient à lancer la procédure de vote en saisissant les paramètres secrets de sa carte d'électeur il a l'assurance que le procédé de cryptage est en place et qu'il fonctionne. C'est probablement le cas dans la plupart des pays de Wassenaar ou pas. »

the Electoral Code states that voters established in a country from which the transmission of encrypted computer data is impossible or prohibited shall be informed (art. R176-3-6). In fact, the Organisation of Swiss Abroad[347] was against the restriction and suggested adopting the French approach: raising awareness among voters residing abroad about the fact that in certain countries electronic voting comes with a risk of censorship, when it is not simply impossible (Swiss Federal Council, 2013a: 34). In turn, the Wassenaar restriction had some limits: a Swiss voter established in a signatory country could very well cast their vote from any other country with Internet access, even from those that were not part of the agreement. Therefore, to protect the secrecy of their vote, voters would be responsible for ensuring the security of their computers (Swiss Federal Council, 2013a: 101-102)

For this reason, the Swiss Federal council finally decided to remove this restriction. The swiss Federal Council reasoned that should such a problem arise, its consequences on the result of an election would be minimal given the low number of Swiss voters established in a country not a signatory to the Wassenaar arrangement[348]. Furthermore, since not all these Swiss lived in the same country, it was unlikely that such an issue would affect them all (Swiss Federal Council, 2013a: 102). Notwithstanding, voters residing in a country where the use of encryption is impossible or prohibited (or in which electronic voting must be considered risky for any reason whatsoever) should be made aware of the risks of voting online from those countries.

On the lists of people having actually voted

Nominally, confidentiality means that only the voter should know how they have voted, and they should be able to make their choices in private. Therefore, nothing prevents that the information about who has voted is made public. Notwithstanding, the Venice Commission has extended the protection of confidentiality to whether a voter has voted or not.

For example, the Code of Good Practice on Electoral Matters sets that "since abstention may indicate a political choice, lists of persons voting should not be published" (Venice Commission, 2002b: para. 54). In 2016, the Venice Commission issued an *Interpretative Declaration on the publication of lists of voters having participated in elections*. The Interpretative Declaration acknowledges that "a balance needs to be struck between data

[347] The Organisation of Swiss Abroad challenged this restriction. According to the Swiss Federal Council (2013a: 101):

> « Cette restriction a été régulièrement critiquée par les Suisses de l'étranger eux-mêmes et par l'Organisation des Suisses de l'étranger (OSE), qui défend leurs intérêts. En effet, les pays non-signataires de l'arrangement de Wassenaar présentent fréquemment l'inconvénient supplémentaire que leurs services postaux fonctionnent mal, ce qui rend quasiment impossible le vote par correspondance des Suisses qui y sont établis »

[348] Nowadays, there could be concerns that votes cast from the United States can be subject to unfounded monitoring. For example, there has been criticism about "U.S. surveillance under FISA 702 and E.O. 12333 [due to]: (1) the lack of ex-ante limitations ensuring that surveillance programs abide by the "principle of proportionality" (i.e., that the programs only collect data that is strictly necessary); and (2) the ineffective ex-post redress for individuals whose personal data is subject to these surveillance programs" (Congressional Research Service, 2021: 5). As a result, the European Court of Justice has ruled that the United States does not offer enough level of protection when it comes to the processing of personal data. However, regardless of the laws applicable in the United States, the authorities could not decrypt by themselves a vote that has been encrypted end-to-end using asymmetric encryption (unless the algorithm or the key management are flawed).

protection and secrecy of the vote on the one hand and stakeholders' interest in consulting the signed (or stamped) voter lists on the other" (Venice Commission, 2016: para. III). For this reason, it was interpreted that while the publication of these lists should be avoided, "access to the lists of voters having participated in elections may be granted to certain electoral stakeholders" (Venice Commission, 2016: para. IV.A.2). Such access could be granted, for example, to candidates or to those electoral stakeholders alleging irregularities. It is unclear whether electoral observers and auditors could have access to these lists if no such irregularities are alleged, although the examples in the Interpretative Declaration do not seem to be *numerus clausus*. At the same time, the fact that additional voting channels are offered poses new questions regarding access to these lists: how to prevent a voter from casting multiple ballots through different channels, including online?

In the Swiss case, the case-law of the Federal Court and the doctrine maintain that the publication of the names of citizens who did not vote is not admissible[349], and that the confidentiality of the vote should remain guaranteed after the electoral process ends (Swiss Federal Council, 2013a: 72-73). However, despite these lists not being published, the authorities should still know whether someone has voted or not. By extension, it was assumed that a helpdesk put in place during the voting period should be authorised to have access to this information as well. In this regard, the Swiss Federal Council noted that such services should access to the database of eligible voters and even to re-establish the link between the identity of the voter and their voter number should they be asked whether a specific vote had been recorded by the system (Swiss Federal Council, 2013a: 72-73).

Such lists are also necessary to prevent voters having voted online to cast a paper ballot, either in polling stations or by post. The Swiss Federal Chancellery (2018d: 9) has recently summarised this process in the following terms:

> "The system provides the information required to determine, using a voter identification card, whether a voter who wishes to vote in person or by post has already cast an electronic vote. In the case of trials involving a very limited electorate (for example the Swiss abroad only), in order to preserve voting secrecy, no list that identifies voters who have cast an electronic vote may be given to any agency outside the infrastructure. Instead on request it must be confirmed whether a vote has been received from an individual voter. Alternatively, the system may provide a list giving anonymous codes that correlate with the voter identification cards used."

As a result, in the Annex to VEleS a requirement has been added that protects precisely the list of people having voted. It states that "[i]t is guaranteed that data that indicate whether a voter has voted electronically are treated as confidential" (Swiss Federal Chancellery, 2018d: 2.8.4). Since this information is deemed confidential, access to it is limited but not forbidden.

In contrast, there are no such restrictions in Estonia. According to Ülle Madise and Epp Martens, "[i] Estonia […] the fact whether a person entitled to vote did participate in voting or not, is not regarded as part of the principle of secrecy. The voter lists that contain information about participation and chosen voting method are preserved in the archive and can be used for research purposes" (2006: 19). In this regard, Arne Koitmäe, Jan Willemson, and Priit Vinkel argue that "full participation secrecy is impossible to implement

[349] With the exception of the canton of Schaffhausen, where voting is compulsory and were the names of the people not having voted is published (Swiss Federal Council, 2013a: 72-73).

as voting in the polling station is public by nature" (2021: 144). According to these authors, "[t]he act of voting and content of the ballot are not approached the same way by voters and election stakeholders. As a result, voter lists (at least individual data of a voter) do not really fall under the umbrella of maintaining vote secrecy" (Koitmäe, Willemson, Vinkel, 2021: 144).

In fact, in Estonia researchers have studied personalised data on internet voters (Madise and Martens, 2006: 19; Koitmäe, Willemson and Vinkel, 2021: 144); including an e-voting survey. However, and in the opinion of Ülle Madise and Epp Martens "unfortunately weakened somewhat the public trust against e-voting" (2006: 19). This is another example of the links between technologies for secret suffrage and voters' perceptions, something that we already introduced in chapter 2.

The confidentiality of previous choices

However, encryption is only applied to the votes cast, which leaves unprotected the secrecy of previous choices. In contrast, the provisions of the Council of Europe's Recommendation specifically extend the standard of confidentiality to the choices recorded and erased by the voter before issuing their final vote (Council of Europe, 2017a: standard No. 25).

This is an interesting point. Additionally, it is something quite unique to (remote) electronic voting. Despite its relevance, however, the issue is not extensively addressed in any of the three national experiences. At least, not at the level of the regulations that we have identified here. This finding is quite striking because such risks were acknowledged in some national reports at initial stages of the national experiences. For example, already in the 2006 report by the Swiss Federal Council it was described how someone could use the data stored in the buffer of a voting device to find out how a person voted (2006: 5218). Why has it not been regulated, then? Two potential explanations can be inferred.

The first explanation is based on acknowledging that the confidentiality of previous choices is already resolved with the requirements for receipt-freeness that we have seen as part of the standard on individuality. In fact, standard No. 23 of the Council of Europe's Recommendation on e-voting sets that "[a]n e-voting system shall not provide the voter with proof of the content of the vote cast for use by third parties" (Council of Europe, 2017a). Furthermore, the Explanatory Memorandum completes this provision by specifically stressing that "traces could be kept for instance in the personal computer's memory, the browser cache, the video memory, swap files, temporary files, etc." (Council of Europe, 2017c: standard No. 25). At the end of the day, the individuality of the vote is closely linked to the confidentiality of the voter choices and if such traces are not stored for the vote that is actually cast, the same protections apply to any other attempts to vote (i.e., the so-called "previous choices"). However, we have already observed that neither France nor Switzerland have envisaged specific mechanisms against coercion and vote-buying in remote electronic voting, and therefore this explanation is not completely satisfactory.

The second explanation builds on top of one of our key hypotheses: that secret suffrage in remote electronic voting has been regulated by analogy to paper-based voting channels, and as a result some specific risks have been left out of the regulations. Since the regulator did not have to face the scenario where a voter could mark uncast paper ballots, such provisions have not been translated into remote electronic voting regulations and it has

resulted in a *lacunae*. The first section in chapter 5 deals precisely with this one and other consequences of regulating by analogy.

3. Anonymity

The third standard of secret suffrage is anonymity. According to this standard, *there should not be a link between the vote cast and the identity of the voter who has cast it*. The standard is specified in several provisions of the Council of Europe's Recommendation on e-voting (Council of Europe, 2017a):

> Standard No. 19: "[e]-voting shall be organised in such a way as to ensure that the secrecy of the vote is respected at all stages of the voting procedure"
>
> Standard No. 26 "[t]he e-voting process, in particular the counting stage, shall be organised in such a way that it is not possible to reconstruct a link between the unsealed vote and the voter. Votes are, and remain, anonymous"
>
> Standard No. 45 "[v]otes and voter information shall be kept sealed until the counting process commences".
>
> Standard No. 46 "[t]he electoral management body shall handle all cryptographic material securely"

Standard No. 26 deals directly with anonymity, and therefore is where our analysis should start. The Guidelines on this provision are actually quite detailed. They first one of these guidelines prescribes that "[v]oter information should be separated from the voter's decision at a pre-defined stage of the counting process" (Council of Europe, 2017a). This provision is very revealing. To some extent, it even contradicts our definition of anonymity. Whereas our definition prescribes that anonymity should be ensured from the moment the vote is cast, according to the Council of Europe's Recommendation anonymity should be ensured before the counting stage, but not necessarily during the casting. Once again, this is a consequence of the standard being defined with paper-based voting systems in mind.

Instead, most electronic voting systems maintain a link between the encrypted vote cast and the identity of the voter who has cast them. In fact, this is also the case for most advanced voting methods (including both remote and voting in specific polling stations in advance of election day). Votes cast their vote within an envelope that contains a proof of their identity, and this link is maintained until the counting stage (the so-called double envelope scheme, which is actually used in all three experiences. By keeping a link between the protected votes and the voters who have cast them it is possible to ascertain that all votes have been cast by eligible voters and to prevent that one voter casts votes using different voting channels. Furthermore, some schemes such as the Estonian re-voting mechanism would not work if votes stored in the voting server were anonymous: how could it be possible to identify which one is the last vote cast by a specific voter? Therefore, in order to accommodate both remote electronic ang postal voting our standard needs to be rephrased, as follows: there should not be a link between the vote cast and the identity of the voter who has cast it *by the time the votes are individually decrypted*. We will be using this new definition from this point forward.

The Guidelines for the implementation of standard No. 26 also prescribe that "[a]ny decoding required for the counting of the votes should be carried out as soon as practicable after the closure of the voting period" (Council of Europe, 2017a). However, the Recommendation does not prescribe what is meant by 'as soon as practicable'. In fact, one

issue is whether anonymisation is required at all. The Guidelines detail that the counting operations are "carried out with decoded[350] votes, which cannot be related to any voter" (Council of Europe, 2017a). This reasoning is, again, based on analogy with postal voting, when the link between voter information and the sealed envelope with the vote are stored together. However, here the Recommendation acknowledges that different approaches are possible as well. In this regard, the Guidelines mention homomorphic encryption as a property that would allow the counting of still encrypted (and therefore not necessarily anonymised) votes. Therefore, in spite of acknowledging that anonymous counting can be conducted with non-anonymised votes, the Recommendation still prescribes that "voter information should be separated from the voter's decision at a pre-defined stage of the counting process"[351] (Council of Europe, 2017a). In this regard, the new approach in the Standard No. 26 has not been mainstreamed in the corresponding guidelines. However, our new definifition of anonymisation, which stresses the importance to break the link if votes are individually decrypted, still accommodates such alternative methods for anonymous tallying.

[350] The use of 'decoded' here is quite confusing. The Recommendation does not offer a definition of this term in their Appendix, and it can be confused with how 'decoding' is used in computer *jargon.* This is not what is meant in this provision, which reads as follows:

> "The term 'voter information' refers to anonymised information on the voter, such as the identification codes used in remote e-voting. Whereas the link between such information and the sealed vote must be maintained for a certain time under appropriate protection, to allow, in particular, the possibility of multiple voting while respecting the 'one person, one vote' principle, the link should be destroyed before the counting takes place.
>
> The encryption of votes will generally be necessary to secure the anonymity of voting. In many cases the vote is encrypted before starting the transmission via computer networks. It is held encrypted in the ballot box and is decoded before counting. The counting is carried out with decoded votes, which cannot be related to any voter."

It is more likely that what is meant by 'decoded' here is actually anonymised. However, the very recommendation already (mis)uses anonymised to refer to "information on the voter, such as the identification codes used in remote e-voting" (Council of Europe, 2017c: standard No. 26). This is obviously a contradiction. Identification codes cannot be anonymous. At best, they may be pseudonymous. Here it would be wise to rewrite this provision in the Guidelines, as follows (Council of Europe, 2017c: standard No. 26):

> The term 'voter information' refers to *pseudonymised* information on the voter, such as the identification codes used in remote e-voting. Whereas the link between such information and the sealed vote must be maintained for a certain time under appropriate protection, to allow, *for example*, the possibility of multiple voting while respecting the 'one person, one vote' principle, the link should be destroyed before the counting takes place.
>
> The encryption of votes will generally be necessary to secure the *confidentiality* of voting. In many cases the vote is encrypted before starting the transmission via computer networks. It is held encrypted in the ballot box and is *anonymised* before counting. The counting is carried out with *anonymised* votes, which cannot be related to any voter.

Even if in principle it would not seem necessary to use pseudonymous data to link a vote to the voter who has cast it, there are important reasons not to use actual data (for example, requirement on data protection regulations that prescribe the securing processing of personal data, such as national identification numbers).

[351] There is still a third provision that prescribes "Member States should take the necessary steps to ensure that the confidentiality of any information obtained by any person while carrying out auditing functions is guaranteed" (Council of Europe, 2017c: standard No. 26). The Explanatory Memorandum also contains a similar provision regarding anonymity and audit systems: "[a]n audit system should maintain voter anonymity at all times, except when specifically required otherwise under domestic legal provisions. In all cases the information gathered by the audit system has to be protected against unauthorised access" (Council of Europe, 2017b: para. 81). Since sections I and II in chapter 5 are precisely devoted to secret suffrage and the transparency of the elections, we will discuss these provisions later.

When it comes to the Explanatory Memorandum, it further details the scope of standard No. 26. The first provision in the Explanatory Memorandum details that "[t]his standard provides that it must not be possible to link the vote to the voter who cast it and thus prevents vote secrecy breaching" (Council of Europe, 2017b: para. 77). Again, this statement should be understood in the light of the standard itself, which specifies that no such link should exist with the unsealed vote. These provisions offer additional explanations for both remote and non-remote electronic voting, where the provisions for remote electronic voting are similar to those of the Guidelines[352]. The Explanatory Memorandum also accommodates those traditions where the anonymity of the vote is conditional[353], such as in the United Kingdom. Whereas anonymity in remote electronic voting is conditional[354], the provisions on when it can be revealed the link between the vote cast and the identity of the voter who has cast it do not fit well within any of the three national experiences.

The provisions of Standard No. 19 build on top of those that have been described for the standard of confidentiality. In this regard, the Explanatory Memorandum reminds that it in addition to encryption "the votes cast are mixed in the electronic ballot box so that the order in which they appear at the counting phase does not allow reconstruction of the order in which they arrived" (Council of Europe, 2017b: para. 64). Lastly, on standard No. 45 the Explanatory Memorandum stresses, once again, "the moment where sealing ends: just before counting" (Council of Europe, 2017b: para. 134). The provision also reminds that "before unsealing, votes are mixed" (Council of Europe, 2017b: para. 134). In this provision the Explanatory Memorandum even acknowledges an "analogy with the physical ballot box" (Council of Europe, 2017b: para. 134), which *a priori* would exclude the alternative forms of anonymous counting mentioned in the Guidelines.

[352] More specifically, paragraph 79 of the Explanatory Memorandum reads that (Council of Europe, 2017b: para. 79)

> "In the remote voting process, information linked to the voter (usually a code) and the votes are connected up to a certain stage. In countries that allow multiple voting, this link is necessary to handle multiple votes and their effect (a vote erases another). The separation has to be made electronically at a predefined stage before counting takes place. This requires specific technical solutions."

[353] This provision in the Explanatory Memorandum reads that (Council of Europe, 2017b: para. 80)

> "[i]n cases where domestic law requires a permanent link between the voter and the vote to exist and to be maintained during the election or referendum and for a specific period thereafter, it has to be assured that the link between a voter and his or her ballot is sufficiently protected throughout the period in order to ensure the secrecy of the vote. This is only revealed pursuant to an order of a competent judicial authority and it must be ensured, that even where the link is so revealed, no voter is compelled to reveal how he or she has voted."

[354] Even in a system where voter information is not attached to the sealed vote, it may be possible to link it to the voter who has cast it by analysing the IP address from where the vote has been cast. In this regard, Keith Martin stresses that cyberspace is not as anonymous as we may think. For example, he notices that (2020: 152)

> "each device accesses the internet using a unique address, which acts as an identifier of the connection and sometimes the device itself. Infrastructure companies, such as mobile operators and internet service providers, often log network activity. Computing devices typically have a range of features that can be used to identify them on the basis of their specific hardware and software. Almost every action in cyberspace leaves a trace, and many of these can be used to unmask a casual attempt to remain anonymous."

If the vote is encrypted, such link would not become a breach of secret suffrage as long as the counting of the votes is anonymous. Otherwise, the only way to mitigate such a breach is to use anonymous channels (for more on anonymous channels see Keith Martin, 2020: 152-154).

In relation to anonymity, the three national experiences show similarities as well as important differences. The main similarities are linked to the enshrinement and regulation of anonymity. Regarding the regulation, specific requirements are envisaged both in the Swiss and the French and Estonian cases. In the case of Switzerland, one of the requirements in the Annex entails that "[i]t is guaranteed that neither employees nor externals obtain data that allow a connection to be made between the identity of voters and the votes they have cast" (Swiss Federal Chancellery, 2018d: 2.8.1). In France, and in contrast to the previous standards, anonymity is not enshrined in the Electoral Code. However, security objective no. 1-07 in the CNIL's framework does require the "total sealing between the identity of the voter and the expression of their vote throughout the duration of the processing" (CNIL, 2019a: 3). Lastly, for the Estonian case it is an important standard as well. In fact, it is acknowledged as one of the two "sub-principles" of secret suffrage.

However, there are important differences in relation to how votes are actually anonymised. In a first stage, it seems that anonymisation was mainly ensured by means of a strict separation of voter data and their votes. For example, in its initial feasibility report, the Swiss Federal Council already identified some basic mechanisms to guarantee the anonymity of the votes, such as the strict separation of citizen data and the votes (Swiss Federal Council, 2002: 632) and the storage on separate servers of the data on citizens and the results of popular consultations (Swiss Federal Council, 2002: 633). For example, in Geneva the identities of the voters and the ballots were kept in two separate, unrelated databases (Swiss Federal Council, 2006: 5223). The description of this process was more detailed in the 2002 report. The votes cast online would be stored independently of the electoral roll, in an encrypted file that would act as the ballot box[355] (Swiss Federal Council, 2002: 649). In the French case, the electoral roll and the 'electronic ballot box' were also hosted on two separate computers, in line with the CNIL's recommendation[356]. However, a computer acted as 'supervisor', integrating the two machines hosting the electronic ballot box and the *liste d'émargement* to check their consistency at regular intervals[357] (Pellegrini, 2006 : 5).

Another technique used is data pseudonymisation. For example, in the first pilot phase of remote electronic voting in Switzerland the three pilot cantons rendered all personal data (name, address, birthdate, etc.) pseudonymous in unique voting cards. Geneva pseudonymised the identity of voters by encoding them into a personal number of 16 digits that encoded their year of birth, their gender and the commune where they were registered

[355] Additionally, the key allowing access to this file was in the possession of the persons who control the counting of the ballots on behalf of the voters. The electronic ballot box would only be emptied at the time of the count and its content will be added to the votes cast by mail and in the polling stations (Swiss Federal Council, 2002: 649).

[356] According to the CNIL, « [l]e secret du vote doit être garanti par la mise en œuvre de procédés rendant impossible l'établissement d'un lien entre le nom de l'électeur et l'expression de son vote. Il en résulte que la gestion du fichier des votes et celle de la liste d'émargement doivent être faites sur des systèmes informatiques distincts, dédiés et isolés » (2003: §I.2).

[357] According to François Pellegrini, the voting process worked as follows (2006: 6): when the encrypted vote arrives at the web server, the receiving program makes two requests to the other two computers. On the one hand, based on the identifiers of the voter transmitted by the latter, it asks the computer managing the *liste d'émargement* list to update it. From this moment, any new connection attempt from the same voter will be refused by the system, to avoid double votes. On the other hand, the encrypted ballot, after a new verification of its conformity over its encrypted form, is transmitted to the server responsible for hosting the 'electronic ballot box'.

to vote. This number was detailed in their voting card, together with their six-digit password (Swiss Federal Council, 2006: 2002). To verify whether a voter had already voted, it was necessary to check in the register whether the voter linked to a number in the voting cards had already cast their ballot (Swiss Federal Council, 2006: 5216). In Zurich the process was a bit different. Individual access codes were also established and printed on the voting cards. However, after printing the voting cards all personal data was erased from the virtual electoral roll and it was no longer possible to establish a link with a particular person (Swiss Federal Council, 2006: 5234).

However, the OSCE/ODIHR identified shortcomings to this method in their report for the 211 Federal Assembly elections (2012: 17):

> "In principle, the secrecy of the vote is protected by the separate storage of personal data and voter credentials following the secure generation of the polling card and before the electronic ballot box is opened. However, during the printing process in the cantons using the consortium system, electoral officials received a report that linked voter names with their voting credentials. This report allowed officials to block access from a given polling card if it was reported lost or if the voter moved and was no longer eligible to vote via the internet in that contest. Although the intention of such a report is to protect the integrity of the vote, it also risks undermining the secrecy of the vote."

Therefore, such mechanisms are not sufficient and some form of anonymisation is required ahead of the actual counting. This is why the Council of Europe's Recommendation prescribes the mixing of the votes (Council of Europe, 2017b: para. 134) or homomorphic tallying (Council of Europe, 2017b: para. 60). Nowadays, all three countries use some form of anonymisation, but not all the methods used fit well within these two categories.

In Switzerland, anonymisation is based on a mix-net[358]. This method was implemented for the anonymisation of the votes since the start of the trials. In Geneva, the contents of the 'electronic ballot box' were mixed by applying an algorithm that changed the order in which the votes were stored (Swiss Federal Chancellery, 2004: 35 ; 2006: 5223). This prevented that someone could compare the order of the votes in the 'electronic ballot box' with the order of the voters in the electoral roll. According to the Swiss Federal Chancellery, the mixing process is based on a repeated cryptographic shuffling and decryption of the vote that changes the order and encryption of the votes (Swiss Federal Chancellery, 2018c: 14). Each shuffle is conducted by a different agent (also known as nodes) in such a way that a single agent cannot repeat the process backwards to retrieve the original order and encryption of the votes.

[358] For a more detailed description of how a mix-net from a technological perspective, we suggest looking at the paper written by Jordi Puiggalí-Allepuz and Sandra Guasch-Castelló (2010).

In contrast, in France the anonymous tallying is achieved by means of homomorphic encryption[359]. "[H]omomorphic encryption[360] enables data owners to perform a range of different types of computation (such as addition and multiplication) on encrypted data without first decrypting it" (Martin, 2020: 241). As a result, it is possible to obtain the final results without having to decrypt each individual vote. According to Keith Martin (2020: 242):

> "Homomorphic encryption schemes allow a data owner to compute the average value of some encrypted numerical database in terms by first computing the average ciphertext value (in the normal way), which are returned to the data owner, who then decrypts this value locally to obtain the average plaintext value"

The process in Estonia is a bit more complex. In the Baltic country, votes are not signed with pseudonymous data, but with their national identifier[361]. Therefore, "[b]efore the ascertaining of voting results during the evening of the Election Day, the encrypted votes and the digital signatures (i.e., the data identifying the voter) are separated. Then the anonymous e-voted are 'opened' and counted. The system opens the votes only after the personal data is removed" (Vassil, 2016: 7). As a result, following the anonymisation process "election officials will have two separate sets of information – a vote tally and a list of voters who voted electronically" (Meagher, 2009: 358-359). Ülle Madise and Epp Martens offer a more detailed description of the whole process (2006: 19-20):

> "Upon voting by electronic means a voter makes her or his choice, which shall be encoded (placed in a so-called virtual inner envelope). Thereafter the voter shall approve the choice by his or her digital signature, which means that personal data is added to the encoded vote (so-called outer envelope). The personal data and the encoded vote shall be stored together until the counting of votes on the Election Day, with the aim of ascertaining that the person has given only one vote. The personal data of a voter and the vote given by the voter shall be separated after the fact that the voter has given only one vote has been checked and repeated votes have been eliminated. It is possible to open the so-called inner envelope only after the personal data added to the encoded vote have been separated with the help of a key given only to the members of the National Electoral Committee, after the polling stations have been closed. Thus, the system of electronic voting guarantees that only one vote per voter shall be taken into account, ensuring, at the same time, that the voting decision remains secret"

[359] Interestingly, the use of homomorphic tallying is not the result of a legal requirement. The Electoral Code does not prescribe any anonymisation procedure, whereas the CNIL's recommendation only sets in security objective 1-07 that the complete sealing between the voter's identity and the expression of his/her vote throughout the processing should be ensured (2019a). The CNIL draws an analogy to remote postal voting here, by setting that the solution to achieve this security objective is « [n]e disposer d'aucun lien entre le votant et son bulletin chiffré dès lors que le vote est exprimé. Le bulletin n'est pas horodaté, contrairement à la liste d'émargement, et le bulletin et la liste sont conservés dans des espaces de stockage distincts » [emphasis added] (CNIL, 2019c)

[360] Homomorphic encryption is different from searchable encryption. Both schemes allow "encrypted data to be processed while still being stored securely" (Martin, 2020: 241). However, in contrast to homomorphic encryption, "*searchable encryption schemes* enable data owners to search data while it remains encrypted […] allows the encrypted database to be searched, items matching the search to be identified, and only those matching items then to be returned to the data owner, who decrypts them" (Martin, 2020: 241).

[361] According to Kristjan Vassil (2016: 7), "[t]he downloaded e-voting app encrypts the vote (PIN1). The encrypted vote can be regarded as the vote contained in the inner, anonymous envelope. After this the voter gives a digital signature to confirm their choice (PIN1). By digitally signing the vote, the voter's personal data or outer envelope is added to the encrypted vote."

The current General Framework of Electronic Voting describes a stage in which votes are anonymised by grouping them by electoral districts and removing personal data from i-votes. The process is specified as follows (State Electoral Office, 2017: 7):

> "Before the counting of i-votes, they are sorted by electoral districts, the list of i-voters is compiled, and the digital signatures are removed.
>
> During the counting of votes, anonymous and mixed votes are decrypted with the election-specific private key, and the summarised results of i-voting are issued."

Here the reference to mixed votes is confusing. According to the General Framework of Electronic Voting, the mixing stage is optional. Mixing is also distinguished from anonymisation of i-votes, where the latter consists in two steps (State Electoral Office, 2017: 18): first, i-votes are grouped by electoral districts; and second, personal data is removed for i-votes. The document also adds that "[t]he result of the stage is anonymous i-votes grouped by electoral districts (encrypted votes). In order for the counting of votes to be publicly verifiable, cryptographic mixing can be used" [emphasis added] (State Electoral Office, 2017: 18). Therefore, according to this provision the goal of mixing[362] the votes is to obtain a publicly verifiable tallying. However, if votes are not mixed and the results are neither tallied using the homomorphic properties, in principle nothing prevents that the order of the results is mapped to the order in which votes were stored before being anonymised[363]. This means that the anonymity of the votes cast could be breached by a system administrator who operates the anonymisation and the tallying.

As it is the case for the confidentiality measures (i.e., encryption), the effectiveness of these anonymisation procedures depends upon procedural safeguards. In this regard, we have already seen that the Council of Europe's Recommendation prescribes the use of key-sharing mechanisms[364]. Currently, such mechanisms are used in the three national experiences, as we have described already above. However, the concerns already mention also cast shadow on the guarantees for anonymity. Furthermore, these mechanisms may not be enough if the number of votes cast is low.

[362] By mixing it is understood the process by means of which (State Electoral Office, 2017: 18):

> "The Processor (or the Mixer authorised therefor) mixes anonymous i-voted grouped by electoral districts, suing the Mixing Application. Mixing consists of random shuffling of cryptographic re-encryption of votes. A precondition for using the latter technique is the use of a homomorphic cryptosystem in the encrypting of votes. Mixing must be carried out so that the decryption of both the input and the output would give the same result. As a side-result of the process, a *mix-proof* is issued which ca be used, with the help of the Audit Application, to prove the correctness of the process.
>
> Both mixed and unmixed votes may be sent to counting. If the Organiser wishes to prove the correctness of the use of the private key in his or her possession in the counting process, it is necessary to also go through the mixing stage."

[363] This risk may be somehow mitigated because the counting is conducted in an off-line environment.

[364] The requirement for key-sharing should not be confused with the recommendation to split tasks between different agents. According to Bernard Lang (2006),

> « [l]a raison de cette recommandation est la même que celle qui justifie d'imposer la combinaison de trois clés pour procéder au dépouillement. Un secret est d'autant mieux gardé que le nombre de personnes ou de systèmes à compromettre simultanément pour y accéder est plus important.
>
> […] la séparation totale de responsabilités doublerait la sécurité concernant la préservation du secret du vote, elle prémunirait mieux contre des erreurs architecturales en imposant de facto une totale séparation des systèmes. »

This was an important issue in France for the 2006 elections, when the number of voters eligible to vote online in certain electoral districts was so low (e.g., just one voter in Kabul[365]) that any anonymisation procedure would have been useless. For this reason, François Pellegrini declared it necessary to cancel the elections for the offices whose number of votes received by Internet was lower than a given threshold (Pellegrini, 2006: 11). His proposal was that these votes should not even be tallied but discarded. It is assumed that those voters should be then encouraged to vote using another voting channel, since discarding their vote without giving them the option to cast another one would have disenfranchised them, thus breaching the principle of universal suffrage.

In Switzerland the same issue was acknowledged, but the authorities opted for an alternative approach: the Federal Council has forbidden the separate publication of the results of the electronic vote at municipal level[366] on the grounds that it could constitute a violation of the secrecy of the vote (Swiss Federal Council, 2013a : 73). Currently, the Anex to VEleS also prescribes the adoption of certain measures in these cases. In this regard, (Swiss Federal Chancellery, 2018d)

> "• 2.8.7. It is guaranteed that the results of the vote will be treated as confidential if only a small number of voters in a constituency can vote electronically.
>
> • 2.8.8. Upon validation and in accordance with a documented process, the system operator destroys all data created as part of the electronic ballot that relate to the individual votes received and that are classified as confidential or secret."

Once again, the different responses can be the result of distinct approaches. If the issue is dealt with an analogy to paper-based elections, the only option is not to publish the results (or to accept that the privacy may be breached). In contrast, alternative approaches may acknowledge the advantages of digital technology: whereas it may be rather difficult to aggregate physical ballots from physical ballot boxes (especially for polling stations abroad), this operation can be conducted easily with electronic votes. Therefore, it is not necessary to publish the results at the lowest level (e.g., the polling stations abroad, or the commune) if such publication would compromise the anonymity of the votes. This issue will be therefore taken up again when discussing the consequences and limitations of regulating by analogy in chapter 5.

[365] According to François Pellegrini (2006 : 6-7):

> « Le déroulement de ce scrutin pose un problème grave de violation du secret du vote de certains électeurs
>
> Vu les faibles nombres d'électeurs s'étant engagés à voter par Internet dans certains bureaux […] il existe une très forte probabilité que les membres de l'organisation des bureaux de vote puissent savoir quel sera le suffrage de certains de leurs électeurs.
>
> Ainsi, à la date du samedi 10 juin 2006, à 23h35, le seul électeur inscrit au bureau de Kaboul n'avait pas voté, mais s'il le fait, son suffrage sera connu avec certitude ; de même pour les bureaux de Riga et de Skopje. Pour le bureau de Colombo, les deux électeurs inscrits ont déjà voté, et la probabilité qu'ils votent de la même manière, et donc leurs deux suffrages soient connus des membres de l'organisation, est der 50% si leurs votes son indépendants ; i els de même pour d'autres bureaux, comme Banda Seri, Erevan et Tbilissi. Si les seuls électeurs d'Oulan Bator et Suva à avoir voté pour le moment ne sont pas rejoints, leurs suffrages seront connus avec certitude, et si un autre électeur les rejoint, à 505, et ainsi de suite.
>
> Il aurait été préférable de prévoir un seuil de nombres d'inscrits par bureaux au-dessous duquel le vote par Internet n'aurait pas été activé (cela aurait été possible, puisque par exemple le scrutin électronique n'a pas été ouvert pour le bureau d'Hambourg en raison d'un problème se saisie. »

[366] By analogy to the reasoning about the publication of lists of voters and their (non-)participation in the vote, the authorities are not prevented from knowing the results of the electronic voting channel (Swiss Federal Council, 2013a : 73).

Lastly, it is also interesting to address the issue about the decryption time. It is not resolved in the international standards, and the Recommendation just prescribes that "[v]otes and voter information shall be kept sealed until the counting process commences" (Council of Europe, 2017a). This is something that has been extensively discussed in the Swiss case.

In its report for the 2011 Federal Assembly elections, the OSCE/ODIHR warned that "[i]n all cantons, the ballots were decrypted after internet voting closed on 22 October, the day before election day" (2012: 17). For these elections, certain cantons had enquired about the possibility to decrypt the remote electronic votes on the Saturday afternoon preceding polling day. They argued that in the case of an election the decryption procedure lasted longer and only by decrypting the results beforehand would the *communes* be able to receive the results in time to carry out the consolidations with the other channels (Swiss Federal Council, 2013a : 72). However, and as rightly pointed out by the OSCE/ODIHR, this practice posed a risk to secret suffrage. Furthermore, if the results were not properly safeguarded, their dissemination could account to the publication of intermediate results[367], breaching in turn equal suffrage.

In the report following the 2011 elections, the Swiss Federal Council concluded that the time of the decryption should be set according to the start of the counting of paper ballots (Swiss Federal Council, 2013a : 113). By 2015 this was no longer an option, and the OSCE/ODIHR reported that "[t]he opening of the electronic ballot boxes and decryption of the votes took place on the morning of election day" (OSCE/ODIHR, 2016: 9). Interestingly, an analogy was drawn with paper-based ballot procedures[368]. As a result, the Swiss Federal Council did not forbid the conduct of preparatory works. In the case of postal voting, the separation of the voter cards from the sealed envelopes containing the vote was permitted, and therefore it was concluded that advancing such preparatory work for remote electronic voting would not encourage any attempts to decrypt the votes beforehand (Swiss Federal Council, 2013a: 113).

[367] According to the Swiss Federal Council (2013a: 113):

> « La suisse, comme de nombreux autres pays, refuse par principe de publier des résultats anticipés partiels sur la base des votes déposés. Cantons et communes ont toutefois à cœur de publier les résultats d'un scrutin le plus rapidement possible, ce qui implique que le dépouillement commence le plus tôt possible. Les cantons fixent donc, avec l'accord de la Confédération, à quel moment et selon quelles restrictions le dépouillement des votes papier peut commencer. Le décryptage des votes électroniques prend lui aussi un certain temps. Certains cantons dotés d'une organisation décentralisée et d'un grand nombre de communes craignent de ne pas disposer du résultat du vote électronique au moment prévu. Il faut donc déterminer le meilleur moment pour commencer le décryptage. »

[368] According to the Swiss Federal Council (2013a: 113):

> « Autre élément à prendre en compte : le vote par correspondance et les procédures qui s'y rattachent jouissent globalement de la confiance de la population
>
> […] Pour garder secrets des votes papier, il faut les conserver sous clé, par exemple dans l'urne scellée du bureau de vote. Les votes par correspondance sont eux aussi conservés sous clé ou du moins sous surveillance, protégés par une enveloppe. Quant aux votes électroniques, le meilleur moyen de préserver leur secret est de les laisser cryptés. »

At the same time, the differences between the two channels were acknowledged (Swiss Federal Council, 2013a: 113):

> « Vu l'importance des votes électroniques par rapport à l'ensemble des voix exprimées – surtout du point de vue de l'extension du troisième canal de vote –, leur divulgation permettrait d'établir des pronostics beaucoup plus fiables que les résultats des votes papier enregistrés dans un bureau de vote. Cela tient au fiat que leur décompte est assuré de manière centralisée par le système dans lequel ils sont exprimés. »

5. Beyond analogies and trade-offs: contending principles for democratic remote electronic elections?

In the previous chapter we have analysed how international standards and national experiences with remote electronic voting have coped with the principle of secret suffrage. Our broken-down analysis against the three minimum standards reveals which mechanisms have been put in place to observe them. First, individuality can be guaranteed by allowing voters to cast multiple votes, either online or both electronically and on paper. Second, confidentiality is ensured with the use of encryption, which should be applied to each vote (and not just to the voting channel) from the moment they are cast (and not server-side). At the same time, encryption may be reinforced with the use of key-sharing mechanisms that will mitigate the risk of votes being decrypted ahead of the counting phase. Key-sharing mechanisms thus in turn call for the use of asymmetric or public key encryption. Third, anonymity is ensured with several techniques. Among them, mix-nets and homomorphic encryption have proven to be the most effective (while important flaws have been already identified for other alternatives). It has also been found that anonymity in remote electronic voting is conditional, in a similar way to other alternative voting channels (such as postal voting or advanced voting in polling stations). For this reason, and as it is the case with encryption, the use of a key-sharing mechanisms mitigates the risk of breaches of anonymity as well.

However, the approach adopted in the previous chapter is flawed. Merely translating the standards of secret suffrage, devised for paper-based elections, to remote electronic voting does not fully address our questions about secret suffrage in remote electronic voting. Some of them remain unanswered: should multiple voting be enabled for remote electronic voting? Is it possible to publish the lists of voters having voted online? How is the confidentiality of previous choices preserved?

For this reason, in this chapter we challenge the very formulation of such principle by identifying specific challenges to secret suffrage in remote electronic voting (section I). In turn, we identify some mechanisms that can be put in place to address them but that also scape any approach towards secret suffrage in remote electronic voting by analogy to paper-based voting channels. All in all, this chapter calls for revisiting the very principle of secret suffrage in the context of remote electronic voting in general and, more precisely, for abandoning the resort to analogy (i.e., with postal voting) in the regulation of electoral principles for e-enabled elections.

So far, our approach is also limited for another reason: the experiences have only been assessed against the principle of secret suffrage. However, democratic elections also have to comply with the principles of universal, equal, free and direct suffrage. These principles impose additional requirements to the conduct of democratic elections, which span from voter eligibility and authentication, to integrity, transparency, and observation. Is it possible that conflicts emerge as a result of the need to comply with these different principles? Building on the theories presented in the Introduction (section II.2.b)), we can ask ourselves: do e-enabled elections raise any latent ambiguities? Are we facing any unprecedented? The question is salient when it comes to the verifiability of remote

electronic voting[369], and especially individual verifiability mechanisms that allow voters to ascertain that their vote has been cast-as-intended and recorded-as-cast. Therefore, we need to analyse to what extent the verifiability mechanisms[370] offering this traceability comply with the principle of secret suffrage. Approaching this issue based on analogies to paper-based voting channels is flawed, and for this reason we are analysing it within this chapter[371].

Therefore, our goal in this last chapter is to identify specific risks and threats to secret suffrage in remote electronic voting, including both computer and human challenges. To do so, we will first challenge on-going approaches based on analogies to paper-based voting channels (that is, the comparison that e-voting should be 'as reliable and secure as' paper-based alternatives) (section I). This assessment will allow us to argue that the regulation of secret suffrage for remote electronic voting should be more detailed regarding the guarantees for individuality, confidentiality, and anonymity. Following, we will consider the need to balance and for trade-offs between different principles, with special focus on universal (section II.1) and free suffrage (section II.2). Our focus in the later will be on assessing the issues raised between secret suffrage and end-to-end verifiability in remote electronic voting. This analysis will allow us to conclude that, whereas a trade-off is usually drawn between secret suffrage *vis-à-vis* the integrity and the transparency of elections, it is not just possible but also necessary to envisage ways to observe secret suffrage in remote electronic voting (section III).

[369] For example, this issue has been raised by the Swiss Federal council (2006: 5259) in the following terms:

> « Alors que les transactions et les personnes concernés doivent être consignées avec précision dans le cadre du télébanking en raison des révisions qui pourraient se révéler nécessaires, elles ne doivent absolument pas l'être dans le cadre du vote électronique (protection du secret du vote). Comme le vote électronique se caractérise par son absence de traçabilité et de preuve (« audit trail »), certains experts tirent à boulets rouges sur cette forme de vote. Ils estiment que le vote électronique, contrairement au vote traditionnel dans les urnes ou au vote par correspondance, ne permet pas aux électeurs de vérifier si leur vote est bien parvenu sur le serveur réservé au scrutin et s'il a été comptabilisé dans le cadre du dépouillement. Ils relèvent par ailleurs que l'autorité électorale n'a aucun moyen d'identifier les actes fautifs et de les réprimer pénalement, contrairement à ce qui se passe dans les procédures traditionnelles. »

[370] In addition to verifiability, the Swiss Federal Chancellery (2004: 35) noted that

> « [c]ertains experts ont proposé ce que l'on appelle le « vote par code » pour résoudre le problème de la traçabilité du vote de chaque électeur : au lieu de voter par « oui », « non », ou « blanc », les électeurs tapent un code (par exemple « z3Gv » pour « oui ») sur l'appareil de saisie. Le code correspondant à chaque vote possible leu est envoyé au préalable en même temps que la carte de légitimation. Le système de vote pourrait ensuite répondre de nouveau avec un code pour chaque vote « oui » enregistré, code que l'électeur pourra vérifier avant la clôture du scrutin à l'aide de son tableau de codes. […] Les cantons pilotes ont examiné cette proposition de façon approfondie lors de la conception de leurs systèmes respectifs. Ils ont néanmoins écarté cette variante pour le vote par Internet, jugeant qu'elle n'était pas conviviale »

[371] Therefore, the Swiss Federal Council was not being completely accurate when it claimed that « [l]e vote électronique et le vote traditionnel sont équivalents en termes de risques et donc de sécurité et de traçabilité » (2006: 5260). It has been acknowledged as such from the moment that end-to-end verifiability became a requirement for remote electronic voting in the country, whereas in 2006 the Swiss Federal Council ill-advised such methods, in the following terms (2006: 5260):

> « Même dans le cas du vote par correspondance et du vote traditionnel dans le local de vote, il n'est pas possible d'effectuer une vérification et une traçabilité individuelles. Qui pourrait – ne serait-ce que par voie de recours – constater avec certitude si son vote a été, d'une part, réceptionné et, d'autre part, comptabilisé correctement ? Un bulletin de vote ou un bulletin électoral qui comporterait une indication quelle qu'elle soit, un nom ou un symbole, serait considéré comme étant marqué de signes et serait donc déclaré nul en vertu des art. 12.2.d., 38.1.d. or 49.1.d. LDP. »

I. SECRET TEXTS AND *CIPHERBALLOTS*? ON ANALOGIES FOR SECRET SUFFRAGE IN REMOTE ELECTRONIC VOTING AND THEIR LIMITATIONS

There are grounds to argue that it is not just our approach that is flawed because it relied on an analogy to secret suffrage in remote electronic voting. In fact, a careful analysis of the literature shows that international standards and national experiences with new voting technologies are fraught with these analogies. Both in our analysis of national experiences and international standard we have often found a resort to analogy (either to postal voting or to voting in polling stations) when evaluating, regulating, and analysing the use of remote electronic voting.

At the national level, for example, the whole Swiss project has relied in comparing Internet to postal voting[372] (Swiss Federal Council, 2006: 5261-62). In fact, it was required that remote electronic voting should be as secure as postal voting[373] (Swiss Federal Council, 2013a: 73), and the requirements for secret suffrage in the three cantonal voting systems were analogous to paper-based remote voting channels[374] (Swiss Federal Council, 2013a: 72).

Estonia is no exception. In fact, Priit Vinkel has also noted that "[t]he e-voting procedure has been adapted to the schematic rules of traditional voting" (2016: 43). More specifically, "[t]he technical setup of the internet voting system is derived from the traditional way a person votes from outside of the polling district of their residence, i.e. the postal voting" (Vassil, 2016: 6-7). As a result, and even if the country has reinterpreted secret suffrage according to a teleological approach, analogies to paper-based voting channels are still common. When it comes to confidentiality, for example, the analogy to the envelope voting method (Madise, Vinkel, Maaten, 2006: 22; Maaten and Hall, 2008) is mentioned often. Priit Vinkel summarised it at follows (2016: 51):

> "The double-envelope system […], used in many voting systems (in particular postal voting) around the world, has been implemented as the logical structure for electronic voting. Its similar nature to the postal system allows the voter to relate to the e-system, helping build trust in an otherwise novel idea."

[372] For example, in the 2006 report the Swiss Federal Council acknowledged that « [o]n prend souvent le vote par correspondance comme élément de comparaison pour évaluer les risques inhérents au vote électronique. » (Swiss Federal Council, 2006: 5261-62).

[373] According to the Swiss Federal Council, « [q]ue le vote électronique soit aussi sûr que le vote par correspondance » (2013a: 73). By 2013, however, this approach had been overcome and the specific challenges of remote electronic voting acknowledged, as follows (Swiss Federal Council, 2013a: 73).

> « Cette comparaison […] a cependant ses limites : il est communément admis qu'une éventuelle fraude dans le contexte du vote par correspondance sera limitée alors qu'une éventuelle fraude dans le vote par Internet peut affecter l'ensemble de l'urne électronique à cause de la centralisation du système. En même temps, le traitement électronique des voix par un système fonctionnant correctement est considéré comme beaucoup plus sûr et fiable que le traitement manuel, notoirement imprécis et au sujet duquel la seule certitude qu'on puisse avoir semblé être qu'en réitérant un dépouillement manuel on n'obtient pas deux fois le même résultat »

[374] According to the Swiss Federal Council (2013a: 72),

> « [l]es exigences en matière de secret du vote posées aux trois systèmes de vote par Internet sont analogues à celles posses au vote par correspondance. Des mesures techniques et organisationnelles ont été prises dans ce sens. Les votes se transmettent sous forme cryptée, l'utilisation du droit de vote et le vote lui-même sont enregistrés dans des structures de données séparées. Après impression des cartes d'électeur, le registre utilisé pour contrôler l'utilisation du droit de vote par Internet est anonymisé – c'est-à-dire que les données personnelles (nom, prénom, adresse) sont effacées »

The depiction of the possibility to cast multiple votes as a 'virtual voting booth' may be yet even more striking: "[t]he principle of the 'virtual voting booth' as a guarantee of freedom and the understanding of teleological voting secrecy have become the cornerstones of the Estonian system and are also adopted in other e-voting systems" (Vinkel, 2016: 43; Vinkel and Krimmer, 2016: 181). In France, the CNIL also draws an analogy to remote postal voting when prescribes that there should be no link between the voter and the encrypted ballot once the vote is cast[375] (CNIL, 2019c). The French Recommendation also forbids time-stamping the votes (CNIL, 2019c).

Analogies have been imbued in the analysis of remote electronic voting, from election observation missions to academia. Even the OSCE/ODIHR's missions have adopted such an approach to remote electronic voting. For instance, the Final Report of the Election Assessment Mission to Estonia's 2007 parliamentary elections (OSCE/ODIHR, 2007b: 9) states that:

> "[r]emote electronic voting is similar in many respects to remote postal voting, offering some of the same advantages, such as increased access of voters to the voting process, and some of the same disadvantages, such as the impossibility to observe during the voting process fully and to ensure the fundamental rights of a free and secret vote. In addition, internet voting does not provide for a fully transparent counting procedure."

Likewise, they also echo the approaches mentioned above, such as in the Estonian case, when they state that (OSCE/ODIHR, 2007b: 11)

> "[t]he internet voting process is designed to parallel the paper voting process to the maximum extent possible so as to be familiar and accessible to voters. The system checks the identity of the voter, provides a 'ballot' to the voter, obtains the voter's signature, and finally allows the vote to be cast. Like remote postal voting, the system is designed to protect the anonymity of the voter through a 'double envelope', in which the content of the voter's electronic ballot is not decrypted until it is separated from the voter's identity after the expiration of the advance electronic voting period."

Moreover, they also resort to analogy when analysing specific processes within the election, such as the verification of the system logs. For instance, in the Final Report of the OSCE/ODIHR's Election Expert Team that observer the 2015 *Riigikogu* elections it is noted that the "logs files contain information about which electronic ballots were excluded as required and which were counted. This process can be compared to reconciliation of ballots cast with those counted in different categories" [emphasis added] (OSCE/ODIHR, 2015b: 6).

In academia[376], Sutton Meagher has sustained that "[t]he use of the digital signature during Internet voting is this analogous to the voter's signature on the outer envelope in paper ballot voting" (2009: 358). An interesting resort to the analogy can be find, as well, in Adrew A. Apple's report about the 2006 French elections: "[t]he *assesseurs* cannot see the voter enter an *isolior* (voting booth) because there is no *isoloir*. In fact, the voter can easily sell his vote –or be coerced– because another person can see him [sic] perform the act of voting" (2006: 8). On the other hand, Alexander H. Trechsel et al. has concluded

[375] For a detailed discussion of this requirement, see footnote 359 above.

[376] On their side, Robert Krimmer and Melanie Volkamer concluded that "both electronically (remote e-Voting) and paper based (postal voting) […] channels share common problems in the field of secrecy of the vote in the vote casting state is concerned" (2005: 9). Notwithstanding, they also identified some unique problems of remote electronic voting, such as Trojan horses.

that "postal voting suffers theoretically from the same problems [than Internet voting]" (2007: 15). In a study of secret suffrage and Internet voting for Mexivo, Jordi Barrat i Esteve[377] also concluded that remote electronic voting and postal voting faced similar dangers (2012: 65). At the political level, according to the OSCE/ODIHR, Estonian "parties [have also] stated that remote voting by internet was similar to remote postal voting in this respect" (2007a: 6).

Notwithstanding, possibly the most reveal example can be found in the case of Rec(2004)11, whose foundation was that "e-voting shall be as reliable and secure as democratic elections and referendums which do not involve the use of electronic means"[378] (Council of Europe, 2004a: 2). As we have seen, many authors were quick to point the flaws of such an approach. For example, Douglas Jones (2004) noted that "[t]he requirement that e-voting should be as secure as non-electronic voting is problematic […] because there exist no widely accepted metrics for this. In addition, the risks that e-enabled elections face are different from those encountered by traditional voting methods."[379]

In his analysis of the Council of Europe's Recommendation Rec(2004)11, Jones (2004) already noted that security requirements for remote electronic voting are measured "against requirements for non-electronic voting systems. As there exist no widely accepted metrics for measuring, reasoning by analogy flaws the comparison between the two" (Driza Maurer, 2014: 114). Driza Maurer herself is also of the opinion that "[r]easoning by analogy with postal voting has serious limits and must be used with care" (Driza Maurer, 2014: 114).

Therefore, the constrains of reasoning by analogy were acknowledged during the updated of the Recommendation, and it was actually one of the drivers behind the endeavour. However, the updated Recommendation stills depends largely on analogies to paper-based voting channels. One example can be found in the guidelines for the implementation of standard No 40. This guideline reads (Council of Europe, 2017c) [emphasis added]:

> "From the moment the vote is cast, no one should be able to read or change it or relate the vote to the voter who cast it. This is achieved by the process of sealing the ballot box, and where the ballot box is remote from the voter, by sealing the vote throughout its transmission from voter to ballot box. In some circumstances, sealing has to be done by encryption.
>
> To seal any ballot box, physical and organisational measures are needed. These may include physically locking the box, and ensuring more than one person guards it. In the case of an electronic ballot box, additional measures are necessary, such as access controls, authorisation structures and firewalls.

[377] The author states that "[e]l voto por internet y el voto por postal constituyen casos análogos" (Barrat i Esteve, 2012: 64) and concluded that "tanto el voto postal como el informático plantean problemáticas similares" (Barrat i Esteve, 2012: 64).

[378] We have identified a similar formula in the Estonian General Framework, according to which "[i]-voting must […] be at least as secure as regular voting" (State Electoral Office of Estonia, 2017: 4).

[379] According to Ardita Driza Maurer, "Jones calls them "retail fraud" for non-e-voting and "wholesale fraud" for e-voting referring to the impact that fraud may have on the results" (2013: 15).

> A vote is sealed when its content has been subject to the measures that ensure that it cannot be read, changed or related to the voter who cast it."

These provisions basically translate the processes for the counting of the votes cast on paper in most countries. First, they claim that votes are anonymous from the moment is cast, whereas elsewhere the Recommendation itself mentions that anonymity should be guaranteed before the counting stage (see for example Standard No. 45). These guidelines prescribe specific measures for the "sealing" of the electronic ballot box, which are additional to those used for physical ballot boxes. It is unclear whether the same measures can be applied at all, or whether the recommendation should have prescribed equivalent measures. More important, these provisions also mix anonymity with confidentiality (we have seen that anonymity is not ensured with encryption). Additionally, these provisions use vague wordings such as "sealing", which does not mean anything specifically[380].

It is now evident that regulating remote electronic by analogy to paper-based voting channels, either remote or not, carries important flaws. Nevertheless, it could be argued that such analogies, even if inaccurate, are useful to convey the workings of a new voting channel to the general public. For the Estonian case, Mihkel Solvak (2016: 128) has put it in this way:

> "It is self-evident that conducting democratic free and fair elections is only possible when there is a baseline level of trust in the electoral procedure among the electorate. Building and ensuring that trust is key in legitimizing the outcome of the election. This is usually achieved through open and detailed regulation of election proceedings and the mutual oversight performed by national as well as international actors involved in the electoral process […] For e-voting, however, novel challenges in maintaining that level of trust in election proceedings arise due to the particular nature of the process […] Given that people cannot physically observe how their e-vote is placed into a virtual ballot box, nor observe how this virtual e-vote are then 'physically' counted by the election officials, a non-satisfactory answer to the question 'what happens to my e-vote?' can discourage participation. In the absence of physical evidence in the form of paper ballots, it essentially becomes a question of trust."

Along these lines, Mihkel Solvak and Kristjan Vassil (2016: 172) recommended that:

> "[i]t is therefore probably wise to keep the procedures of electronic vote processing as similar to regular vote counting processes as possible, so the sceptics always see the equivalence of this or that step between the process of on- and off-line voting. This is exactly what has been done in Estonia. We have an electronic voting committee as part of the national voting committee, use the digital equivalent of the double envelope system as used in postal voting worldwide, with the electronic votes are electronically 'opened' and 'counted' on election day with observers present, as is done in any polling station after polls close. All this should make the process as transparent as possible, even though one mode uses the latest in cryptography and the other pen and a ballot paper in voting booth, just as when the secret vote was introduced in the 19th century."

In our opinion, while such an effort may be necessary to convey the working of remote electronic voting, it is different to regulate a voting channel and to make it understandable

[380] In fact, sealing could be misunderstood as providing integrity rather than confidentiality. For example, Martin Keith notes that "[t]he real purpose of the seal is to indirectly state that *the integrity of the information on this piece of paper is assured by the creator of this stamp*" (2020: 99). However, it is clear that this is not what is meant by sealing when it comes to secret suffrage.

to the general public. Several of the examples found on the use of analogies are not aimed at the general public, but their goal is to assess whether remote electronic voting complies with the principles of democratic elections. Whereas analogies may be restored to for voter education campaigns[381], reports by the OSCE/ODIHR, by academia assessing the conduct of a specific election or system, and administrative standards should not use these analogies. At most, they should distinguish between the actual description of remote electronic voting and the strategies used to convey how it works. Therefore, if we take the case of confidentiality, standards of descriptions of the systems should be clear that it is ensured by means of encryption and specify which encryption algorithms. Additionally, they could suggest how to convey the use of encryption to the general public, referring to as sealing instead of encryption.

To sum up, we rephrase Chantal Enguehard who raised a similar flag when analysing the French decrees on remote electronic voting already in 2010[382]: the administrative authority is not in a position to record the findings that it is supposed to report on the minutes, because there is neither attendance list nor ballot box, but representations of these objects in the computer memory[383].

1. Secret suffrage and remote electronic voting: the constraints of the analogy

It may also be claimed that in remote electronic voting reasoning by analogy to paper-based remote voting challenges may help identify some of the risks or threats that Internet voting has to meet. Such claims can be found in some of the more recent developments on remote electronic voting in Switzerland. For example, the Swiss Federal Chancellery (2020b: 36) has echoed the opinions of experts who concluded that:

[381] It has not been our goal to specifically address whether such voter education campaigns work at all. Yet, we still have doubts that trying to answer accurately the answer of 'what happens to my e-vote?' or 'where is my e-vote' in terms of an analogy meet yet create more distrust, or at least less awareness of some risks related to voting online. On this matter, see for instance the work of Josep Maria Reniu (2016) mentioned in footnote 196.

[382] More specifically, she refers to the provision in the decree of 13 March 2008 for the elections to the council of the professional association of nurses establishing that "[t]he technical committee for the organization of the elections may request the communication of the minutes drawn up by the administrative authority attesting that the list of voters is blank, that the ballot boxes are empty...". Before her, François Pellegrini had also noticed that "seen from the outside, Internet voting may seem to be similar to postal voting [...] However, the dematerialization of the ballot constitutes in fact a radical break, with considerable consequences on the voting process, and whose risks should not be underestimated" (2006: 4).

[383] Regarding (in)security in cyberspace, authors like Keith Martin (2020: 21) stress that:

> "cyberspace is inherently not *physical*. Of course, elements of cyberspace such as data centers, computers, routers, and wires are part of the physical world. However, the information relating to, and being produced and processed by, these components is not physical. Information in cyberspace is represented by digital data. You can't pick digital data up, feel it, or stuff it into an envelope.
>
> Because digital data is not physical, very few of the security mechanisms we use in the physical world are appropriate for protecting digital information. It's true that we can securely store a USB memory stick by locking it in a drawer, but the moment we want to use the information on this device, we have to connect it in some way to cyberspace, and then the physical protection is no longer effective."

Our stance is that the same approach towards securing data exchanges in cyberspace, including remote electronic voting, should acknowledge these differences and the constraints of translating the mechanisms envisaged for paper-based voting (in polling stations) to remote electronic voting.

> "the risk itself can be hard to assess. With regards to the risks, points of reference might be found in postal voting or in the systems that would likely allow a threat-agent to reach his [sic] goal to manipulate the outcome of a vote at a lower cost. The risks of not offering internet voting may also be taken into the equation, e.g. disenfranchisement of voters abroad or losing momentum and resources towards more secure solutions, thereby possibly also addressing the risks inherent to postal voting."

For example, about half of the experts in the Swiss expert dialogue were of the opinion that "[t]he risks are not or not much higher with internet voting. One expert clearly highlights the scalability of vote-buying in the absence of a resilient voting protocol. However, he located the parameters as to whether vote-buying happens rather in societal than technical aspects" (Swiss Federal Chancellery, 2020b: 56). From this perspective, there are some 'cross-channel' interaction risks, that is "threat areas that can affect postal and internet voting channels alike, such as voter coercion or vote-buying, a risk that appears most scalable and attractive to foreign adversaries when applied to internet voting […] but has also proven a realistic threat to postal voting even in mature democracies" (Federal Chancellery, 2020b: 76).

Nevertheless, this opinion was not unanimous. In fact, the majority of the experts argued that "[t]he risk is higher with internet voting[384], mainly due to anonymity and increased scalable technical feasibility" (Swiss Federal Chancellery, 2020b: 56). When it comes to secret suffrage, we can identify some specific risks and threats that have no equivalent to postal voting.

a) Threats against individuality and confidentiality

The fact that voters cast their votes by themselves in unsupervised environments has been the main concern about remote electronic voting. Nevertheless, Internet voting is not the only channel in which voters cast their votes from unsupervised environments. For example, in postal voting the same concerns may arise.

However, we argue that there are some challenges that are unique to remote electronic voting or attacks that scale better if voters can cast their votes electronically from unsupervised environments. Furthermore, these attacks also challenge the standard of confidentiality, since they are carried out when and where data exist in unencrypted form. These attacks include, among others, *keyloggers*, *tempest attacks*, viruses and trojans[385].

[384] Interestingly, some experts also stressed the importance of examining

[385] Keith Martin refers to this as endpoint security. Using end-to-end encryption reduces the scope of these attacks, but they cannot be disregarded since end-to-end encryption (Martin, 2020: 191):

> "does not encrypt this data from the point at which you enter it into your keypad [or click it in your screen]. Here, the data might exist in temporary memory, or indeed it might be stored somewhere on your computer. The data could be obtained by anyone standing behind you, watching you as you type. It is potentially available to anyone else who has access to your computer or can run a program on your computer. The data might also be available to anyone who has installed a keylogger on your keyboard to record your keystrokes."

In turn, Simon Singh also mentions attacks based on the so-called tempest attack (1999: 318):

> "A more recent development is the so-called *tempest attack*, which aims to detect the electromagnetic signals emitted by the electronics in a computer's display unit. If Eve [an eavesdropper, an attacker] parks a van outside Alice's house [i.e., a voter], she can see sensitive tempest equipment to identify each individual keystroke that Alice makes on her computer. This would allow Eve to intercept the message as it is typed into the computer, before it is encrypted."

Overall, these threats and challenges are related to applications that allow voters to share their screens while voting; to malware that can monitor the voter's casting devices without them noticing; and fake voters portals that can be setup to misguide voters and steal their voting credentials and data.

Voting receipts: screenshots, screen recordings, and screensharing

As we have seen, standards on individuality prescribe that remote electronic voting systems should not generate any evidence that the voter can use to prove the contents of their vote to a third party. By extension, an Internet voting system should not generate any residual information about the votes cast either. For example, the Swiss Federal Chancellery's report (2004: 35) noted that Geneva's Internet voting system disabled the screen print functionalities during the casting of the vote. Likewise, the voting portal opened on a "pop-up" screen, which did not leave any traces in the Internet browsing history (Swiss Federal Chancellery, 2004: 35). However, it is unlikely that it prevents the use of software that records a screen, or the very screenshot functionalities that come with most devices. In any case, it cannot be prevented at all that a voter records themselves with a second device (for example, a smartphone if they are voting with their computer).

Indeed, this threat is not new. Voters could also record themselves using a smartphone when voting by post. However, with remote electronic voting a coercer or a vote-buyer has more options to actually observe how a voter is voting while voting, even if remotely. For example, a voter selling their vote could be asked to share their screen during the process using a video conferencing tool[386], while the vote buyer is connected remotely. Then the reward would be conditional on the voter following all the steps, from authentication to casting, until the confirmation of the casting is displayed in the screen. Since the monitoring is done remotely, the possibilities to scale this attack increase to other paper-based voting channels.

In principle, the Estonian solution that enables the voter to cast multiple votes and cancel any vote cast electronically under duress (even by casting a paper ballot) would mitigate this threat. However, we have already seen that voters do not have such an option neither in Switzerland[387] nor in France.

A more detailed account of the work conducted in tempest attacks is provided by Steven Levy (2001: 41-44). As we will see, these attacks are partially mitigated if we take into account the provisions on residual information (discussed in section II.1. of the previous chapter) and the confidentiality of the previous choices (also started in the previous chapter, and more specifically in section II.2.c) above). However, the analysis of national experiences has already revealed that mechanisms to comply with these standards are always put in place.

[386] Video conferencing tools… some of the most common examples include Skype, Zoom, Microsoft Teams, bluejeans, jitsi, etc. All these tools allow a user to share their screen.

[387] As it has been explained, cantons in Switzerland created centralized registers to prevent voters from casting more than one vote. In this sense, "[o]nce a voter cast her/his vote, the electronic record is marked accordingly in the voter register to avoid the possibility of multiple voting" (OSCE/ODIHR, 2016: 7). Such systems also prevent voters from "change[ing] a vote after it has been cast" (OSCE/ODIHR, 2012: 17; OSCE/ODIHR, 2016: 6). Aware that this mechanism prevented voters from cancelling a vote that they may have cast while being observed or coerced, the OSCE/OIDHR concluded that "consideration could be given to providing voters […] with means to protect voters against possible coercion and other forms of manipulation. This could include options to allow voters to cancel their previous vote by casting another vote via the internet or in person" (OSCE/ODIHR, 2012: 17; 2016: 8).

Surveillance: trojans, malware, and spyware

A different issue arises if the voter is being monitoring without them knowing. That is the case of trojans, malware and spyware[388]. Such a risk is not difficult to conceive. For example, in its feasibility study on the introduction of remote electronic voting, the Swiss Federal Council noted that voting devices could be compromised in such a way that non authorised parties could see or register the contents of the screen, the data introduced, or the communication exchanges carried out, using connected peripheral devices (Swiss Federal Council, 2002: 637). Such attacks could be triggered from anywhere, meaning that it would not be enough for voters to isolate themselves at the casting phase. More important, the Swiss Federal Council highlighted, the very rapid changes in software and the appearance of ever new forms of viruses would make it necessary to test electronic voting systems over the Internet almost constantly (2002: 637). For the Swiss Federal Council, virus and trojan horses[389] were the main threat in remote electronic voting (2006: 5258).

A device infected with malware or a trojan horse could be tampered in such a way that the choices made by the voters and that the information which allows the identification of the persons entitled to vote are read and stored by a third party (Swiss Federal Council, 2006: 5218). As noted by Keith Martin, "your computer could store what you type[390] and send this information to someone who is conducting surveillance of your activities[391]" (2020: 130). Since the devices used by the voters are not supervised by the election authorities, and voters may not have the necessary knowledge to identify attacks or infected devices, these were considered high risks[392] (Swiss Federal Council, 2006: 5218).

[388] The following scenario described by Simon Singh (1999: 319) shows quite well how these attacks work:

> "Other attacks include the use of viruses and Trojan horses. Eve might design a virus that infects […] software and sits quietly inside Alice's computer. When Alice uses her private key to decrypt a message, the virus would wake up and make a note of it. The next time that Alice connects to the Internet, the virus would surreptitiously send the private key to Eve, thereby allowing her to decipher all subsequent messages sent to Alice. The Trojan horse, another software trick, involves Eve designing a program that appears to act like a genuine […] product, but which actually betrays the user."

The use of asymmetric encryption (as we recommend in section I.2 in this chapter) would mitigate this risk (since it would only be possible to copy the public key). However, such a virus or Trojan horse could always copy and share the plaintext vote before it is encrypted, thus breaching secret suffrage.

[389] The Swiss Federal Council (2006: 5257) defined these threats in this way:

> « Les virus et les chevaux de Troie sont des programmes autonomes pourvus d'une fonction cachée malfaisante. De tels programmes (par exemple, camouflés en d'inoffensifs écrans de veille) peuvent souvent se loger subrepticement dans le système d'exploitation d'un ordinateur et s'y développer, mais aussi permettre à des tiers d'accéder à des donnés personnelles par une porte dérobée, détruire des données importantes ou identifier des mots de passe. »

[390] This kind of malware is known as keylogger (see footnote 385 above).

[391] Computers can also supress and alter information, which makes electronic votes vulnerable to manipulation. This is the reason why individual verifiability mechanisms have been introduced in most cases, as we will discuss in section II.3.b) below.

[392] Nevertheless, some mechanisms were envisaged. According to the Swiss Federal Council (2006: 5258),

> « [t]oujours est-il que les cantons pilotes ont intégré des éléments de sécurité dans la transmission des votes, lesquels concourent à prévenir les manipulations dues à des virus ou à des chevaux de

Concerns about these threats were echoed in subsequent reports. For example, the 2013 report depicted the voting devices as the Achilles heel of remote electronic voting[393] (Swiss Federal Council, 2013a : 75).

Switzerland is no exception in this. For example, Priit Vinkel also concluded that "[p]ersonal computers and the internet remain the weakest links in the system" (2016: 42). In France[394], the ANSSI has also noted that since each voter freely chooses their voting device, the attacks against personal computers remain the most difficult to contain (Buffet, 2020: 45). This threat cannot be downplayed. Furthermore, it is an attack that has no equivalent in paper-based voting channels: papers ballots do not spy on the voters without them knowing (at least not for the time being).

Against this threat, the advantages of casting multiple votes are not so obvious. First, the voter should be aware that they have been spied in other to cast another ballot, a requirement quite difficult to meet. Therefore, it is not clear that such a mechanism would be enough to address the concerns of those voters concerned about the confidentiality of

> Troie. Ainsi, quand un électeur à opère son choix, il reçoit un message lui demandant d'effectuer un dernier contrôle avant de valider son vote. Cette opération ne se fait pas sous la forme d'un texte, mais sous la forme de pictogrammes, que les virus et les chevaux de Troie n'ont guère de chance d'identifier et qui ne peuvent faire l'objet de manipulations que si des conditions extrêmement complexes sont réunies. Dans le canton de Genève, les pictogrammes (« oui », « non », « blanc ») sont en plus placés sur un code à quatre chiffres. Le canton de Zurich travaille quant à lui non pas à l'aide de codes mais de symboles (notamment des symboles représentant des animaux). »

[393] Along these lines, the 2013 report stressed that « [l]'ordinateur privé est considéré comme le talon d'Achille du vote électronique. Il échappe au contrôle des autorités et on considère que la plupart des électeurs n'ont à priori pas les connaissances techniques nécessaires pour le sécuriser de manière adéquate » (Swiss Federal Council, 2013a : 75). By then, the Swiss Federal Council had concluded that « [l]a responsabilité de la sécurité de l'appareil de saisie relève dès lors exclusivement de l'utilisateur ou alors du responsable s'un système de gestion (antivirus, pare-feu, etc.) » (2006: 5251).

The latest version of the Annex to VEleS on Technical and administrative requirements for electronic vote casting offers a detailed account of such threats (Swiss Federal Chancellery, 2018d):

- "3.1.10. Malware on the user platform sends vote to organisation.
- 3.1.11. Vote redirected using DNS spoofing.
- 3.1.12. An attacker reads a vote using MITM [Man in the Middle]

  […]
- 3.1.16. Criminal organisation infiltrates the system with the aim of breaching voting secrecy or obtaining early provisional results."

These provisions identify different threats that, in principle, all concern the security objective of protecting vote secrecy and non-disclosure of early provisional results. In practice, they range from those compromising only the secrecy of the vote () and those were both the very right to vote is breached by preventing a voter from casting their vote (). In this second case, of course the secrecy of the vote is breached as well, but the two threats are sufficiently distinct to be dealt with separately. Additionally, some of these threats are linked to the standard of anonymity and will therefore be discussed in section d). below.

[394] As early as 2006, François Pellegrini had noted how these attacks could be scaled in remote electronic voting (2006 : 10):

> « [g]râce à l'Internet, il peut être très facile de diffuser sur grande échelle des virus capables d'infecter les machines des électeurs, et qui auront pour fonction d'intercepter les frappes des identifiants qu'ils effectuent au clavier, puis d'empêcher la connexion finale au serveur, en redémarrant l'ordinateur de l'électeur ou en bloquant son navigateur, après avoir transmis les informations recueillies à une machine relais piratée pour l'occasion et affiché, comme leurre, une génère indiquant que le vote a bien été pris en compte. Dès lors, le fraudeur pourra en quelques seconds, effectuer le vote de son choix au nom de l'électeur. »

their choices (either because they were not voting alone or because they did not trust the device used to cast their vote to be free from spyware).

Social engineering attacks and fake voting portals

A third kind of attack has raised even more concerns. This attack is not just a threat to secret suffrage (it could even be argued that the secrecy of the vote is not directly affected[395]) and therefore requires a special consideration. It is also a threat that has been present in all three national experiences.

In this attack, voters connect to a voting portal as it were the legitimate one. They enter their voter credentials, mark their vote, and cast it. However, the entity behind the portal is not the legitimate voting server: they are casting a fake vote in a fake website. This enables the attacked to actually disregard their vote and obtain the credentials of the voters to vote on their behalf. It can be executed through different means, including phishing attacks[396], spoofing[397], and DNS poisoning[398]. Several solutions are suggested for this problem, including both technological and social ones. For example, on the

[395] However, since this attack targets the foundations of public key cryptography, we consider it here. After all, "asymmetric encryption relies on the assumption that you have the correct public key before you encrypt anything. If this is in doubt, all bets are off" (Martin, 2020: 88).

[396] At an early stage of the Swiss experience, the Swiss Federal Council (2006: 5257) identified this issue and suggested some solutions in the following terms:

> « L'électeur est confronté à la question de savoir comment être sur qu'il vote sur le « bon » serveur (c'est-à-dire, le serveur officiel). Car de faux serveurs pourraient être crées, le but étant de détourner les caractères d'identification des électeurs. Les informations ainsi récoltées pourraient alors être utilisées à des fins abusives. Cette technique est souvent appelée « phishing » (hameçonnage). Des exemples tirés du télébanking montrent malheureusement que nombre de citoyens, qui n'ont pas encore assez conscience de ce danger, renoncent à utiliser les moyens de vérification, qui leurs sont proposés. Il est à craindre que cela puisse aussi être le cas dans le cadre du vote électronique. C'est la raison pour laquelle ce domaine à risque est ultrasensible. La plupart des solutions qui permettent de prévenir de tels risques visent à contrôler partiellement ou complètement les logiciels installés dans l'appareil de saisie. Une solution serait par exemple d'envoyer un CD-ROM contenant un système d'exploitation et une application pour le vote électronique. Les électeurs n'auraient ensuite plus qu'à lancer le CD-ROM dans l'appareil de saisie avant de voter. Les cantons pilotes ont toutefois décidé d'écarter ce système après l'avoir examiné en profondeur, car ils le jugent non convivial, sans parler du fait qu'il ne pourrait pas être installé tel quel sur tous les appareils disponibles sur le marché. Les trois cantons pilotes offrent malgré tout aux électeurs la possibilité de vérifier le certificat du serveur réservé au scrutin grâce à un numéro imprimé sur la carte de légitimation (empreinte digitale du certificat). Qui plus est, des codes ou des symboles transmis sous forme graphique sont utilisés durant la procédure de vote, que l'électeur peut comparer avec les codes ou les symboles figurant sur sa carte de légitimation. Les risques liés à l'authentification du serveur réservé au scrutin sont jugés moyens, car les mesures de contrôle présents ci-dessus doivent être prises par les électeurs eux-mêmes. »

[397] For the Estonian experience, the OSCE/ODIHR (2007b: 18) noted that

> "The internet voting system cannot prevent voters from using computers which have malware installed that could compromise the security of their vote. The NEC warns voters on the official web page only to use the internet voting system if their computer is free from malware. One potential threat is that malicious software could 'spoof' the Internet address used for voting, causing a voter to believe that he/she is casting a vote on the official website but in reality interacting with another website."

[398] Alternatively, François Pellegrini (2006: 10) described this attack as follows:

> « En falsifiant à distance les informations réseau permettant la communication entre l'ordinateur de l'électeur et les serveurs du système de vote (technique dites de « DNS poisoning ») il est possible de faire croire à l'utilisateur qu'il se connecte sur le bon serveur alors qu'il interagit avec un serveur pirate qui, une fois ses identifiants obtenus, effectuera à sa place le vote, mais pour un autre candidat. »

technological side it has been suggested to use secure connection protocols[399], digital certificates[400], and pictographs[401]. The Swiss alternatives have been described by the OSCE/ODIHR as follows: "[v]oters can verify whether they are casting a vote on the official server by checking the SSL certificate of the voting server presented by the internet browser as well as by comparing unique pictorial symbols displayed on the screen to those printed on their polling card" (2012a: 17). The individual verifiability mechanisms that we will describe in Section II would also help identify if there has been such an attack.

On the social side, several options are identified in the Estonian experience. According to the OSCE/ODIHR (2007b: 18):

> "The NEC stated that they could not prevent malware installed on a voter's computer from interfering with the voting process but had taken steps to limit the likelihood. These steps included advising voters to type in the correct IP web address rather than click on a link to the NEC website posted on another site, and publishing the server certificate in newspapers and on the NEC website so that a voter can verify that he/she is connected with the vote storage server. The voter could also obtain information to verify whether he/she has the proper voting application"

It seems a combination of both technological and awareness-raising solutions seems to be the most effective mitigation strategy. For example, one of the findings of the expert dialogue was that "[a]dvising voters to check the TLS-fingerprint is unlikely to bring much benefit. Two experts recommend to advise voters to enter the URL correctly and check the pad-lock symbol" (Swiss Federal Chancellery, 2020b: 51). Along these lines, the Swiss Federal Chancellery had already concluded that "[v]oters are given the information required to check the authenticity of the website and the server used for vote casting. The informative validity of a successful verification must be supported by the use cryptographic resources in accordance with the best practices" (2018d: 14).

All in all, these challenges shows that the main risks for remote electronic voting are related to the conditions in which votes are cast. To some extent, they are similar to those that a voter may experience in remote postal voting (since they are the result of the voter casting their vote from unsupervised environments). However, they have a unique nature as long as the voting device can be a source of threat itself. The analogy to remote postal voting would be equivalent to the paper ballot spying on the voter, it being able to record the process of being marked, or the possibility for the postal vote to be send to a different address than the expected one. Likewise, the option to re-vote may not be as useful here since an effective resort to multiple voting requires the voter to know that they have been

[399] For example, in the case of Neuchâtel it was reported that « la communication entre le poste de l'utilisateur et le serveur sera garantie par un protocole de communication sécurisée s'étendant à l'ensemble des prestations offertes dans le GSU » (Swiss Federal Chancellery, 2004: 35)

[400] A certificate is the standard tool for linking a public key to its owner (Martin, 2020: 187). According to this author, "[a] public certificate essentially states: *This is to certify the public key of* www.reallycheapwidgets.com *is X*" (Martin, 2020: 187). For example, in the case of Geneva, « l'empreinte du certificat digital lié au site de vote est reproduite sur la carte de légitimité de façon que l'électeur peut s'assurer qu'il est bien en contact avec le site officiel de vote » (Swiss Federal Council, 2006: 5222).

[401] In this regard, the Swiss Federal Chancellery described that in Geneva « [l]e bulletin renvoyé à l'électeur, pour qu'il confirme son choix et s'identifie, est mélangé à une image qui le rend illisible aux pirates informatiques. Cette image, différente pour chaque électeur, lui permet de vérifier qu'il est connecté au site officiel de vote » (2004: 35).

voting under duress. Therefore, it is unlikely that it can work if the voter is being inadvertently spied by its very voting device.

Having said that, it is also important to acknowledge that attacks on the channel or server side are less likely than in remote postal voting, because the technological measures are expected to mitigate the vote from being intercepted after it has been cast (thanks to vote and channel encryption) or once received by the election administration (thanks to key-sharing mechanisms). At the same time, all these challenges are in principle feasible, which does not mean that they are likely. We also presented several attacks to paper-based voting channel that are possible (see section III in chapter 2), but that we estimate difficult to conduct and therefore we assume the risk. The same assessment should be conducted for the risks that are unique or more salient in remote electronic voting[402]. For example, Switzerland has been aware of these risks and the authorities have accepted them. In other cases, it is unclear whether the risks have been assessed at all. In turn, it is important that this assessment is conducted often, since technological advances may male these attacks less costly and therefore more likely.

b) Threats against confidentiality and anonymity

A second set of threats and challenges are related to confidentiality. In the previous chapter it has been concluded that confidentiality is guaranteed by means of public key encryption. However, how resilient is public key cryptography? Can it be considered the silver bullet for confidentiality?

Following, we focus on certain weaknesses of existing public key cryptography algorithms. These algorithms will not be resilient against quantum computers, which may compromise secret suffrage in the long term. Additionally, we also resume the discussion about whether confidentiality should also apply to the very fact that a voter has voted, and how this can be guaranteed or not in remote electronic voting.

Data deletion and post-election data processing

The question arises as what to do with the election data, including the votes that are kept both encrypted and signed, and in some cases anonymised (Estonia) and mixed (Switzerland). Keeping this data creates a risk, since the cryptography used to protect them may be vulnerable to attacks nowadays or in the future.

For example, In Estonia it was already acknowledged in 2011 that "the data and the internet voting equipment need to be destroyed in order to preserve the secrecy of the

[402] For example, during the Swiss' PIT a group of experts described an attack against Swiss Post's remote electronic voting systems that would require the attacker to control each voting client from where a vote is cast, in addition to at least one control component. In spite of this attack being feasible, with the current technology it seems unlikely that an attacker could control all the devices from where voter can be cast. According to Jordi Puiggalí (2019: 322):

> "the main theoretical attack identified by the researchers requires the attacker to control also the vote casting process in the voter device to learn the randomness used to encrypt the vote. Therefore, the attacker needs to control the voter device used to cast each vote that they want to manipulate. Another constraint of the reported attack was that it requires to control the first control component, otherwise it is not feasible. A second theoretical attack was also proposed, but the internal structure of the vote made it not feasible.

vote in view of the ever-increasing computing powers available for a trial-and-error decryption [sic]" (OSCE/ODIHR, 2011b[403]: 12). According to the OSCE/ODIHR's Final Report, the most important parts of the Internet voting system that were destroyed included "[t]he key pair, the encrypted votes, including all back up CDs, the hard disk drives, the SSL server and the secret keys used for signing the Internet voting software" (OSCE/ODIHR, 2011b: 12). However, the mission noted that "[w]hile regulations for the storage and destruction of materials used in the paper ballot voting follow the requirements provided for in the Personal Data Protection Act, the Internet voting remains unregulated in this respect. In particular, details are lacking in the specifications on how personal data should be destroyed" (OSCE/ODIHR, 2011b: 12).

For years later, this assessment was updated in the following terms (OSCE/ODIHR, 2015b: 6)

> "The EVC performed daily updates of the voter register and backed up encrypted ballots on a CD. This was done through direct access to the servers, which the EVC insisted was preferable to establishing a remote connection, even though direct (administrative) access and maintenance during critical operations is not considered a good security practice. The EVC maintained that backing up encrypted votes on an external storage medium is preferable to organizing and securing another location with a direct connection to mirrored servers."

Currently, there are provisions in the Acts that prescribe the destruction of this data" (Unt, Solvak and Vassil, 2016: 82): "the actual votes have been destroyed as stipulated by law."

In Switzerland, "[VEleS] also regulated the destruction of electronic data once the final election results have been approved, along the same principles as to dispose of paper ballots" (OSCE/ODIHR, 2016: 5). Likewise, in France the CNIL's updated Recommendation clearly sets a limit on how long the election data can be stored. According to the Recommendation (Rodríguez-Pérez, 2020: 179)

> "All support files (copies of source and executable codes of programs and the underlying system, voting materials, attendance files, results, backups) must be kept under seal until the means and deadlines for judicial appeal. This conservation must be ensured under the control of the electoral commission under conditions guaranteeing the secrecy of the vote. Obligation must be made to the service provider, if necessary, to transfer all of these media to the person or third party named to ensure the conservation of these media. When no contentious action has been initiated at the exhaustion of the time limits for appeal, these documents must be destroyed under the control of the electoral commission."

Therefore, data that must be deleted includes the copies of source and executable codes of programs and the underlying system, voting materials, attendance files, results, backups. Such data may be stored during the complaints and appeals procedure, "under conditions guaranteeing the secrecy of the vote".

Interestingly, it is not clear how it is prevented that there are copies of this data that are not destroyed. For example, Keith Martin (2020: 229) notes that

[403] For the 2011 elections, the "[m]ost important parts of the Internet voting system were destroyed on 11 April in the presence of the NEC members, the auditor and observers" (OSCE/ODIHR, 2011b[403]: 12).

> "In the event of future breakthroughs in attacks on cryptography, it's not realistic to rely on simply upgrading the encryption algorithm in order to protect existing data. You can re-encrypt old plaintext with the stronger encryption algorithm, but you cannot guarantee that copies of the original ciphertext will not still be available for an attacker to break.
>
> The biggest challenge for designers of cryptographic algorithms is that the cryptography of today *will* be attacked tomorrow."

The issue is a concern if we take into account that votes are cast through an open environment, the Internet. Additionally, copies can be made of the votes cast without anyone noticing. Even if the votes are encrypted, their encryption could be compromised in the future.

Furthermore, it is also important to highlight that "deleting a file does not necessarily destroy it; it merely breaks the digital association between the file itself and the label the laptop uses to locate it. Someone who knows what they're doing can rummage around on the laptop and retrieve the unlabelled 'deleted' file" (Martin, 2020: 191).

Quantum computing and cryptanalysis

The risk of encryption being breached is especially acute when we consider the potential of quantum computing[404]. Some authors, like Keith Martin, speak about a revolution in computing due to advances in quantum physics[405] (2020: 231):

[404] However, the same threat could result from advances in artificial intelligence and algorithms trained to break encryption. Such cases are highlighted by Miles Brundage et al. (2018). For example, Keith Martin (2020: 244) stresses that:

> "I can certainly imagine advanced in automated reasoning and artificial intelligence threatening today's cryptography. A highlight sophisticated computer program might well be able to conduct a more thorough security analysis of a cryptosystem than we can carry out today. It might find subtle flaws, discoverable only by sophisticated investigation. It might be able to find unobvious patterns in encrypted data. But for advances in artificial intelligence to lead to a capability gap, it is necessary to imagine an advanced attack machine being able of doing things the resto f us are totally unaware of. I can't completely rule this out, but I think the advancement of modern science unfolds in a sufficiently open and collaborative environment that it's unlikely anyone can keep this type of capability secret for very long."

[405] There are two underlying theories to quantum physics: superposition and the many-world interpretation. According to Simon Singh, superpositionists argue that "if we do not know what a particle is doing, then it is allowed to do everything possible simultaneously. In the case of the photon, we do not know whether it passed though the left slit or the right slit, so we assume that is passed through both simultaneously. Each possibility is called a state, and because the photon fulfils both possibilities it is said to be in a superposition of states" (1999: 324). This is illustrated in the parable of Schrödinger's cat (1999: 324):

> "Imagine a cat in a bot. There are two possible states for the cat, namely dead or alive. Initially, we know that the cat is definitely in one particular state, because we can see that it is alive. At this point, the cat is not in a superposition of states. Next, we place a vial of cyanide in the vox along with the cat and close the lid […] quantum theory says that the cat is in a superposition of two-states-it is both dead and alive, it satisfies all possibilities. Superposition occurs only when we lose sight of an object, and it is a way of describing an object during a period of ambiguity. When we eventually open the box, we can see whether the cat is alive of read. The act of looking at the cat forces it to be in one particular state, and at that very moment the superposition disappears."

On their side, "[f]ollowers of the many-worlds interpretation belie that whenever an object has the potential to enter one of several possible states, the universe splits into many universes, so each potential is fulfilled in a different universe. This proliferation of universes is referred to as the *multiverse*." (Singh, 1999: 325). On quantum computing see also Steven Levy (2001: 275).

> "*Quantum computers* will, apparently, be able to perform some tasks much more speedily than today's computers do. Quantum computers will have a significant impact on cryptography because some tasks relating to cryptography that are currently computational infeasible on a conventional computer will become computationally feasible. Only a few fledging quantum computers exist today, and their extremely limited capability makes pocket calculator seem like a supercomputer. But quantum computers will only improve, so we need to take quantum computing seriously and prepare for its arrival."

Therefore, and as some experts pointed out in their contributions during the Swiss expert dialogue, "[q]uantum computers or advances in cryptanalysis[406] may at some point subvert the soundness of today's standard building blocks" (Swiss Federal Chancellery, 2020b: 5). To understand why, it is important to understand how current encryption algorithms work.

We have already mentioned that confidentiality is currently achieved by encrypting the vote, and more specifically by using asymmetric or public key cryptography. Without the private key, "decryption [of the votes] should be *extremely hard* to perform" (Martin, 2020: 78). According to Martin Keith, "[a] function suitable for asymmetric encryption is sometimes called a *trapdoor one-way function*. 'One way' refers to the fact that it must be easy to compute but hard to reverse, while 'trapdoor' indicated there must be a way for a genuine recipients to reverse the process (knowledge of the private decryption key being the trapdoor)" (2020: 266-267)[407]. Nowadays, the hardness of asymmetric encryption is based either on prime factors (in the case of RSA[408]) or on the difficulty of working out the discrete logarithm (i.e., elliptic curves).

Breaking encryption is not impossible. But it is unlikely that conventional computers can break standardised asymmetric encryption algorithms in reasonable time[409]. The hardness of the algorithm will thus depend on how much time does it take to find out the key. In this regard, Keith Martin notes that "[g]iven the computers used today, however, the

[406] According to Simon Singh, cryptanalysis is "the science of unscrambling a message without knowledge of the key" (1999: 15). This author explains that "[w]hile the cryptographer develops new methods of secret writing, it is the cryptanalyst who struggles to find weaknesses in these methods in order to break into secret messages" (1999: 15).

[407] See also Simon Singh (1999: 260-261). In turn, Steven Levy provides a historical account on how contemporary cryptographic algorithms were build based on one-way functions (2001: 28-36)

[408] RSA stands for the names of its inventors: Ronald Rivest, Adi Shamir, and Len Adelman (Martin, 2020: 267). According to Keith Martin, "[t]he relationship between a number and its prime factors creates exactly the types of computational tasks […] necessary in order to accomplish asymmetric encryption: going in one direction, it's manageable; going in the other, it's a circuit-board burner" (2020: 81).

[409] For example, it is possible to compute the prime factors of a number. In this regard, "trying to divide by every prime from 2 onward will eventually result in the two prime factors being found" (Martin, 2020: 84-85). Therefore, the robustness of factoring is not based on whether it is possible to solve the mathematical problem, but on how hard it is (and how much time it could take). Simon Singh (1999: 320) offers a more detailed account:

> "A theoretical breakthrough would be a fundamentally new way of finding Alice's private key. Alice's privacy key consists of *p* and *q*, and these are found by factoring the public key, *N.* The standard approach is to check each prime number one at a time to see if it divides into *N,* but we know that this takes an unreasonable amount of time. Cryptanalysis have tried to find a shortcut to factoring, a method that drastically reduces the steps required to find *p* and *q,* but so far all attempts to develop a fast factoring receipt have ended in failure. Mathematicians have been studying factoring for centuries, and modern factoring techniques are not significantly better than ancient techniques. Indeed, it could be the laws of mathematics forbid the existence of a significant shortcut for factoring."

human race is more likely to face extinction, or at least to evolve into different species, before all the possible prime factor of a 900-digit number have been tested" (2020: 85). For this reason, the key length is paramount[410]. A generally accepted standard "for data that needs protection up until the year 2030 suggest using a product of two primes that is more than 3,000 bits long" (Martin 2020: 267).

Quantum computing challenges most of these assumptions[411]. In 1994, Peter Shor found an algorithm that could be implemented by a quantum computer to break contemporary encryption algorithms[412]. Chris Jay Hoofnagle and Simon L. Garfinkel explain Shor's finding as follows (2022: 166-167):

> "Shor's paper showed that if a certain kind of quantum circuit could be built on an as-yet non-existent quantum computer, then laws of quantum mechanics could be combined with number theory in such a way as to solve a particular math problem very efficiently. Solving *that* particular math problem would make it possible to efficiently factor large numbers. And factoring large numbers would have a huge impact on the world, because the world's most sophisticated encryption systems at the time (and still today) depended upon the fact that we are unable as species, on Earth, today, to rapidly factor large numbers."

By contrast, quantum algorithms are not expected to have the same implications for symmetric cryptography[413]. In this regard, Lov Grover found out that "a properly

[410] Keith Martin stresses that "[k]ey length matters because there is an unsophisticated attack that can be launched against every cryptographic algorithm […] An *exhaustive key search*" (2020: 167), also known as brute force attacks. One interesting case about the importance of key length is related to the fact that the first encryption standard prescribed a key length that was not resilient against eavesdropping by the NSA. It has been reported by Simon Singh (1999: 249-250), Steven Levy (2001: 57-65). Similarly, Keith Martin describes the NSA's efforts to place backdoors in cryptographic algorithms (2020: 209-210). On key lengths, see also footnote 284 above.

[411] On the other hand, quantum computing can also provide opportunities for confidentiality by solving the problem of establishing a common secret key in two different locations. This could be achieved by means of quantum key distribution, "a means of transferring a randomly generated key from one location to another over a special quantum channel" (Martin, 2020: 231). According to Simon Singh (1999: 349): "[q]uantum cryptography is an unbreakable system of encryption". The author further adds (Singh, 1999: 349):

> "the claim that quantum cryptography is secure is qualitatively different from all previous claims. Quantum cryptography is not just effectively unbreakable, it is absolutely unbreakable. Quantum theory, the most successful theory in the history of physics, means that it is impossible for Eve to intercept accurately the onetime pad key established between Alice and Bob. Eve cannot even attempt to intercept the onetime pad key without Alice and Bob being warned of her eavesdropping. Indeed, if a message protected by quantum cryptography were ever to be deciphered, it would mean that quantum theory is flawed."

In other words, "the 'magic' channel is a quantum optical channel, instantiated through the likes of either line-of-sight aligned lasers or optical fibbers. The key is encoded as quantum states, and a special property of quantum mechanics means that anyone attempting to read data on the channel will inadvertedly alter these states in a way that can later be detected by the receiver" (Martin, 2020: 235). However, Keith Martin also stresses that "[w]e don't have serious quantum computers today, nor are we likely to have them soon. […] Eventually, maybe, quantum computers will become a bit more mainstream. Only *then* might quantum cryptographic algorithms possibly become useful" (2020: 231).

[412] The reason why Schor's algorithm can be executed by a quantum computer but not by a conventional one has been described in detail by Simon Singh (1999: 327-330).

[413] Keith Martin has summarised the resilience of symmetric cryptography against quantum computers as follows (2020: 234):

constructed quantum computer could speed up all sorts of computations that have a certain mathematical property. The speedup was not as significant as Shor's: instead of turning a problem that is computationally intractable into one that can be solved in just a few hours, Grover's algorithm gives a square-root speedup" (Hoofnagle and Garfinkel, 2022: 210). Therefore, "quantum computers will have a significant impact on modern cryptography, but they won't break *all* the cryptography that we use today" (Martin, 2020: 232). However, we have already seen that one of the building blocks of confidentiality is asymmetric encryption, and the cryptosystems based on factoring and on discrete logarithm are vulnerable to quantum attacks. Therefore, for systems guaranteeing confidentiality based on these two mathematical problems are at stake[414].

Having said that it is not clear neither when quantum computing when be feasible, nor the actual capabilities that quantum computers will have[415]. There are different estimates. For example, in 2016 the NIST estimated that quantum computers would be available in 20 years, that is: by 2036 (Chen et al., 2016: 1). More recent estimates by the EU Agency for Cybersecurity (ENISA), some threat agents could have quantum computers in the next five to 10 years (Beullens et al., 2021: 28). Nevertheless, any data that is published today is vulnerable against quantum attacks. According to Ward Beullens *et al.*, "[w]hat makes matters worse is that any encrypted communication intercepted today can be decrypted by the attacker as soon as he [sic] has access to a large quantum computer, whether in 5, 10 or 20 years from now" (2021: 28). Such a threat – referred to as retrospective decryption – was also acknowledged by the e-voting experts at the Swiss dialogue (Swiss Federal Chancellery, 2020b: 55):

> "Most experts do not see a threat to integrity in the coming years. However, privacy deserves attention, given that data could be collected today and evaluated later, as four experts highlight. One expert notes that one must always assume that the encrypted votes might leak. Two experts highlight that breaking voter privacy would require to establish a link to the voter. This could be managed by withholding the personal data of the voters, that however would have to be done in an effective way"

Finding an answer to this problem requires a novel approach. Regulating by analogy does not work, since similar problems do not exist in paper-based voting channels[416]. One alternative is to resort to quantum-resistant encryption algorithms. Quantum-resistant or post-quantum cryptography are based on mathematical problems that quantum computers may not be able to solve easily. Some examples include lattice-based cryptography,

> "It is currently believed that the best quantum computers can do is reduce the time it takes to perform an exhaustive key search by a margin that is substantial, but not so significant that all the symmetric encryption algorithms we use today would be ineffective. More specifically, it is believed that symmetric-key lengths need to double in order to protect against and attacker with a quantum computer."

[414] According to Keith Martin (2020: 233),

> "[a]lmost all the asymmetric encryption and digital-signatures schemes that we use today are based on the perceived difficulty of two mathematical problems: factoring and finding discrete logarithms. It is known that a sufficiently powerful quantum computer could, unfortunately, both factor and find discrete logarithms efficiently. In other words, a quantum computer would render all our current asymmetric encryption and digital signatures schemes ineffective."

[415] According to Keith Martin, "[w]e *know* it's coming. We *know* it will impact contemporary cryptographic algorithms (to quite varying extents). We *don't know* the time frames. We *don't know* how realistically the theory can be converted into practice" (2020: 164).

[416] Although maybe there are but we are not aware of them. It is possible that with the development of quantum sensing it should be possible even to picture a vote protected inside and envelope, or even a voter casting their vote within a voting booth. For more on quantum sensing see Chris Jay Hoofnagle and Simson L. Garfinkel (2022: 31-76).

supersingular elliptic curves, or codes (Chen *et al.*, 2016). Currently, there are not yet generally accepted quantum-resistant algorithms to build these systems, although there are efforts to standardise them[417]. The problem with these algorithms is that they "need to be capable of running on conventional computers" (Martin, 2020: 233), and they may not be as efficient as the existing standards. At the time of writing, there are just a couple of proposals of remote electronic voting systems based on quantum-resistant public key encryption (del Pino et al., 2017; Costa, Martinez and Morillo, 2017; Costa, Martinez and Morillo, 2018; Costa Mirada, 2021). One of these proposals has been recently implemented by Valeh Farzaliyev et al. (2021). However, the efficiency of their findings makes the actual implementation of this system not feasible for actual politically binding elections.

Furthermore, actual quantum computers may already exist, or they could exist anytime soon. It means that quantum computing is no longer a long-term risk, but a medium-to-short one. For example, in the framework of the Swiss expert dialog one expert noted that "[i]t is unclear whether quantum computers will exist in the near future or if they already exist. Therefore, it is not possible to determine when a post-quantum cryptographic redesign is necessary" (Swiss Federal Chancellery, 2020b: 55). If we take into account that most developments in cryptography have been kept secret[418], this risk cannot be downplayed.

(Anonymised) i-voting system log data

In the previous chapter, we have discussed whether confidentiality should apply also to whether a vote has voted at all. As a result, it is prescribed that the list of persons who have voted should not be made public, although it can be scrutinised by auditors and election observers. Nevertheless, in the case of remote electronic voting this list has to be understood in broader terms.

For example, in Estonia "[t]he study of e-voting has since the 2013 local elections benefited from an additional data source in the form of anonymized e-voting system log data" (Unt, Solvak and Vassil, 2016: 71). According to Ülle Madise, Priit Vinkel and Epp Maaten, "[i]n its different stages the e-voting system produces different logs on received, cancelled, counted, invalid and valid votes. Audit Application enables to establish what happened to an e-vote given by a concrete person without revealing the voter's choice" (2006: 24-25). According to Unt, Solvak and Vassil "[t]he data itself is automatically generated when people e-vote and is foremost used by the election authorities and e-voting system administrators to identify failures and to detect anomalies and possible attacks against the system" (2016: 71-72). The information logged is quite detailed, and includes "each voter's age, gender, the country where the vote was cast, the operation system (Windows, Linux, iOS), the method of identification (ID-card, Digi-ID or mobile-

[417] However, this could change quickly, rendering this statement may be outdated from the time these lines are written until the defence of this PhD. The National Institute for Standards and Technology (NIST) in the United States is currently undergoing the third and last round of its competition for the standardisation of quantum-resistant public key cryptography algorithms, and the final report could be published at any time. An overview of this competition is described in Adrià Rodríguez Pérez (forthcoming).

[418] See for example see for example alternative proposals for public key encryption that were kept secret by the United Kingdom in Simon Singh (1999: 279-292) and Steven Levy (2001: 313-330). Overall, the work of these authors clearly shows how states always have had an interest in keeping secret their developments in cryptography and cryptanalysis.

ID), the time of voting and the session length" (Unt, Solvak and Vassil, 2016: 72). Therefore, looking at these logs may reveal whether someone has voted or not[419]. Since this information should not be made public, the access to the logs should be limited.

The issue is whether there are alternative ways to find out whether someone has voted just looking at the connections with the voting server. Simon Singh described these attacks based on traffic analysis (1999: 318):

> "Even if users employ the RSA [or any other] cypher properly, there is still plenty that codebreakers can do to glean information from intercepted messages. Codebreakers continue to use old-fashioned techniques like traffic analysis; if codebreakers cannot fathom the contents of a message, at least they might be able to find out who is sending it, and whom it is being sent, which itself can be telling."

Therefore, an attacker could position themselves "logically between the two communication partners and via its system [have] full control of the data traffic between two or more network participants" (Swiss Federal Chancellery, 2018d: 11). This kind of attacks would not allow the attacker to view or manipulate the information since it is encrypted, but it could identify whether a voter is casting their vote. The use of channel encryption in addition to vote encryption would mitigate this threat.

2. Regulating secret suffrage and remote electronic voting

All in all, these issues compel us to revisit our understanding of secret suffrage, so its three minimum dimensions (individuality, confidentiality, and anonymity) can be fully observed. In this section, we summarise some key recommendations for the regulation of secret suffrage in remote electronic voting.

a) Individuality: coercion-resistance and multiple voting

According to J. Paul Gibson et al, "[v]oter coercion is a major potential problem with REV-if the voter records their vote in an uncontrolled environment then it is reasonable to ask what is to stop a coercer from being present and obliging the voter to follow their wishes?" (2016: 281). It is unchallenged that one key "problem in regards to i-voting and vote secrecy is the voting environment, which should ensure voter privacy. This cannot be guaranteed by election administration when the voter is voting from the location of their choice using a personal computer" (Koitmäe, Willemson, Vinkel, 2021: 141). Nevertheless, we have seen that an essential guarantee for the standard individuality offered in Estonia is the possibility for voters to cast several votes electronically, or even casting a paper ballot that would override any vote cast online.

However, no such mechanisms exist neither in Switzerland nor in France. Likewise, the Council of Europe's Recommendation on e-voting neither prescribes nor precludes multiple voting. This is undoubtedly a consequence of approaching the issue of individuality in analogy to paper-based remote voting channels. However, we have already showed that both channels raise different challenges for secret suffrage. Therefore, both scenarios need

[419] In principle, is not possible to ascertain what each voter has cast, since logs operate "with anonymize data on the so called outer envelope of the e-vote" (Unt, Solvak and Vassil, 2016: 82).

to be assessed differently. For this reason, it is important to analyse in detail how multiple voting works[420] and which are its advantages against the challenges identified above.

Interestingly, Estonia is the only one of the three countries that have been analysed that offers this possibility. It is not a mere option, but "[i]n case of internet-based voting, the possibility to change a vote is a constitutional obligation"[421] (Madise, 2007. 18). How the system works is quite straightforward, and "[i]n order to guarantee the freedom of voting, e-voters have been granted the right to re-vote electronically an unlimited number of times and replace the vote cast on the Internet by a paper ballot. […] In case of several e-votes the last one is counted; in case of contest between e-vote and paper ballot, the paper ballot is counted" (Madise, 2007: 18).

The main concern behind this guarantee is the fact that voters may be subject to coercion or even be willing to sell their vote. Kristjan Vassil (2016: 9) has summarised the idea in the following terms:

> "An often-debated issue in terms of internet voting is the question of how to ensure vote secrecy in unsupervised environments. Because internet voting does not ensure that voters cast their votes alone, the validity of internet voting must be demonstrated on other grounds. To ensure that the voter is expressing their true will, they are allowed to change their electronic vote by voting repeatedly (electronically) during advance polls or by voting at the polling station during advance polls. This mechanism ensures that the vote buyer or coercer will not know for sure which ballot will be eventually counted rendering vote buying or coercing meaningless"

Nowadays, voters can cast their votes from Monday until Saturday evening, just the day before election day[422].

While the potential of this mechanism to mitigate or even eliminate coercion and vote-buying seem paramount, multiple voting is not a silver bullet. In fact, the advantages of

[420] In addition to multiple voting, the literature also offers alternative coercion-resistance mechanisms. According to Kristjan Krips and Jan Willemson, these include fake credentials (the JCJ/Civitas family), re-randomisable ciphertexts (BeleniosFR, in the Helios family), cryptographic tracking numbers (Selene), conditional linkability (Eos), and panic passwords (Selections) (2019). However, and since they have not been implemented in any of our three case studies, it does not seem adequate to evaluate their legal feasibility.

[421] Ülle Madise describes this in the following terms (2007: 19): "[a]ccording to the opinion of the Supreme Court […] the state has to create the necessary prerequisites in order to carry out free polling and to protect voters from the undesired pressure while making a voting decision."

[422] Initially, and based on the ruling of the Supreme Court, remote electronic voters could not cast their votes on election day. This option has changed recently with a series of amendments to the *Riigikogu* Elections Act that entered first into force for the 2021 local elections. Before that, voters still have several options to cast multiple ballots (Vassil, 2016: 9):

- "Time framework of e-voting: e-votes may be cast during seven days, from the 10th until the 4th day before the Election Day.
- Possibility to recast an e-vote: during the e-voting period a voter can e-vote as often as they wish, but only the last e-vote is counted.
- Primacy of ballot paper voting: if a voter who has already e-voted goes to the polling station during the advance polls and casts their vote using a paper ballot, then the e-vote is cancelled. After this, the voter cannot recast their vote electronically or using a paper ballot.
- Similarity of e-voting to regular voting: e-voting adheres to the elections acts and general election principles and customs. Thus, it is uniform and secret, only eligible voters may vote, every person may cast only one vote and it should be impossible for voters to know which way someone voted. The collecting of voters must be secure, reliable and verifiable"

this option are limited[423]. For example, it is not much used in Estonia, which calls its effectiveness into question. Multiple voting also carries additional costs for election administrations when it comes to handling votes cast through multiple channels, and its very approach can seem at first contrary to other electoral principles, such as equal suffrage. Unsurprisingly, the analogy with paper-based voting channels has been also drawn with a view to justify the constitutionality of multiple voting in Estonia, which may hamper its full potential[424].

First, Estonian analysis show that use of multiple voting is not widespread. For example, for the 2005 local elections "[t]he general statistics shows that the number of amended e-votes was only 364 […], including repeated votes given for demonstration by the members of the e-voting organizing-team" (Madise and Martens, 2006: 23). In 2007, this number doubled, but compared to the overall number of votes cast electronically it only represented the 2.5% (OSCE/ODIHR, 2007b: 17). More recently, Taavi Unt, Mihkel Solvak, and Kristjan Vassil have found that re-voting "is [still] extremely rare; the overwhelming majority of e-voters, approximately 98% of those who cast a binding vote, e-voted exactly once. Between 1.5 and 2.1% e-vote twice and during each studied year [2013-2015] only 0.14 to 0.17% (i.e. a few hundred) e-voted voted three or more times" (2016: 82).

For this reason, it is unclear whether such an option actually works to mitigate coercion[425]. Nevertheless, regardless of the numbers it may be still useful to lower the effectiveness of coercion or buying votes. Since the potential vote manipulator has no guarantee that their machinations will deliver the desired results, this advantage still remains in theory.

Another question that arises here is whether this option to cast multiple ballots does not breach the principle of "one voter, one vote" enshrined in the principle of equal suffrage. The issue was at the heart of the Supreme Court's ruling on the constitutionality of remote electronic voting. When ruling about the constitutionality of multiple voting, it was argued that (Supreme Court of Estonia, 2005) [emphasis added]:

[423] In this regard, remote electronic voting sceptics have also argued that this solution does not by itself guarantee adequate levels of secrecy (Birch and Watt, 2004: 62). For example, Jo Saglie and Signe Bock Segaard acknowledge that "[t]hese measures may not work equally well in all social contexts. First, if someone influences a family member's vote, the voter who is subject to pressure may not always have an opportunity to cast a new vote" (2016: 157).

[424] In its 2005 ruling, the Supreme Court of Estonia held that [emphasis added]:

> "[w]ithin the system of electronic voting the taking of only one vote per voter is guaranteed by a system similar to the so called system of two envelopes, used upon voting outside the polling division of one's residence during advance polls. Upon voting by electronic means a voter makes his or her choice, which shall be encoded (placed in a so called inner envelope). Thereafter the voter shall approve the choice by his or her digital signature, which means that personal data is added to the encoded vote (so-called outer envelope). The personal data and the encoded vote shall be stored together until the counting of votes on the election day, with the aim of ascertaining that the person has given only one vote. The personal data of a voter and the vote given by the voter shall be separated after the fact that the voter has given only one vote has been checked and repeated votes have been eliminated. It is possible to open the so-called inner envelope only after the personal data added to encoded vote have been separated with the help of a key given only to the members of the National Electoral Committee, after the polling divisions have been closed. Thus, the system of electronic voting guarantees that only one vote per voter shall be taken into account, ensuring, at the same time, that the voting remains secret."

[425] What is clear that no such advantage exists if the challenge comes from voters being secretly monitored while voting (as we described in Section I.1.a) above). If voters are not aware that they are being observed while voting, they may not cancel their votes, and therefore the incentive to monitor them using malware and spyware remains. In fact, in light of the number of voters who actually re-vote there is a clear interest in continuing to monitor them.

> "[t]he principle of uniformity does not mean that all votes should vote using exactly the same channel. All those who use different channels of voting are, in fact, in a somewhat different situation, and so far this has not been deemed to be in conflict with the principles of democratic elections […] [p]roceeding from the principle of uniformity that state shall take measures to prevent the purchasing of votes, otherwise it would be possible to obtain more than one vote either in consideration for benefits or under the influence of a threat. Purchasing of an electronic vote becomes less reasonable only when an electronic vote can be changed by another electronic vote or by a ballot paper."

However, the very fact that this practice has not been widely adopted may be the consequence of such concerns. For example, Ülle Madise describes how "the possibility to replace a vote given electronically, or e-vote, with another e-vote or a paper ballot with the aim of ensuring the principle of free suffrage cause perplexity amongst the audience of the report presented at the Worldwide Forum on e-Democracy in Paris in 2001 and even in 2005"[426] (2007: 7-8).

In addition to these concerns, enabling the option to re-vote also carries procedural complexities. For example, "Estonian election procedures require that election officials compare the list of voters who voted online with a list of voters who voted at the polling place prior to initiating the vote tally at the end of an election. If one individual appears on both lists, the officials cancel the electronic vote to prevent anyone from voting twice. Although voters may change their vote as many times as they wish, the system prevents multiple votes" (Meagher, 2009: 373-374). In this regard, "[e]lection officials [have to] compare the list of voters who voted electronically and those who voted a normal [sic] paper ballot to ensure that no one has voted multiple times. If there are any names that appear on both lists, officials go through a process to delete the vote cast electronically" (Meagher, 2009: 358-359).

Lastly, it is also important to stress that in 2007 the "OSCE/ODIHR EAM noted that one technical aspect of the system undermines the objective of the recast possibility. Namely, the vote storage server records the time that each voter casts his/her last electronic vote. This log, which is available to political parties and observers, could potentially be misused to know whether a voter did in fact recast his/her vote electronically"[427] (2007b: 17). More importantly, the analysis conducted in 2020 found a risk and that this possibility could be used by "an attacker submitting a vote using a compromised e-ID environment without the voter noticing" (Heiberg, Krips and Willemson, 2020: 84), for instance by changing

[426] Therefore, it should not come as a surprise that the wording of the Council of Europe's 2004 Recommendation on e-voting actually precluded this practice. This is noted by Douglas Jones (2004: 2), who criticised the legal standard that the e-voting system shall prevent changing of a vote once the vote has been cast. While it is obvious that the system nor any unauthorised party should change those votes to preserve the integrity of the election, Douglas Jones already noted that "[p]articularly with remote electronic voting, it may be appropriate to allow voters to change their votes. One of the most frequently cited objections to remote voting (including both electronic and postal variants), is that a voter could vote in the presence of someone who is attempting to coerce a particular vote. The potential for voter coercion can be reduced by making all ballots provisional, with the rule that casting a replacement ballot voids all ballots previously cast by the same voter" (2004: 2). The exception here was Norway, where multiple voting was also offered during the pilots in 2011 and 2013. According to Ülle Madie, "at an International seminar held in Bregenz in 2006, Norwegian scholars, who remarked *inter alia* that they had arrived at similar principles before obtaining detailed knowledge about the Estonian Internet voting system expressed clear support for the vote replacement aspect of this idea" (2007: 8).

[427] In this sense, the OSCE/ODIHR EAM recommended "that the time voting is not recorded" (2007: 17). However, the time when each vote is cast must be recorded in order to exclude all the votes but the last one cast by the same voter when they have cast multiple votes.

"the originally submitted vote by re-voting, and also when the voter did not intent to vote at all" (Heiberg, Krips and Willemson, 2020: 84). While this attack would not breach the secrecy of the voter's previous vote (or their abstention thereof) it is a challenge that also needs to be taken into account since it could jeopardise their right to vote[428]. In any case, "as of 2021 i-voters will have the option to re-vote on paper during the election Sunday as well" (Heiberg, Krips and Willemson, 2020: 91) which would render such attacks even more unlikely should the voters be aware that they have been affected by them.

All in all, this brings us to the importance of awareness[429]. In Estonia it has been acknowledged that "[t]he individual has to be aware of risks, i.e. technical risks, and he or she has the right to decide whether or not to use the Internet voting opportunity"[430] (Madise, 2007: 18). For multiple voting to be effective, they should be aware that risks do not come only from coercers, group voting, or vote-buying, but there are technological risks as well: they can be monitored while voting if their voting device is infected with malware, their computer may take advantage of the re-vote possibility and cancel their vote by casting another one later on, etc. If the ultimate responsibility rests on each and every voter, their decision to vote online cannot be considered free if they are not aware of these challenges.

b) Confidentiality: asymmetric, quantum-resistant vote encryption with key-sharing schemes

Based on the above, it seems wise to enshrine at the level of the law the guarantees that preserve the principle of confidentiality. In this regard, we have seen that in all three cases confidentiality it is used by means of cryptography, and more specifically by means or asymmetric or public key encryption. The use of public key encryption ensures that only

[428] Notwithstanding, and as the authors suggest, this can be easily prevented by enabling a feedback channel (such as SMS) that would alert voters when a vote (or another one, in case that they have already voted) is cast using their credentials (Heiberg, Krips and Willemson, 2020: 91-92).On the other hand, the authors also note that such a measure could also make coercion attacks (such as vote-buying) easier.

[429] A usual mantra among the tech community and cybersecurity experts is "that humans are the 'weakest link' in any security system, including cryptosystems" (Martin, 2020: 192). In the case of remote electronic voting, there are several studies on the usability of remote electronic systems for the lay voter that discuss whether they can be made aware of tampering. According to Keith Martin, "[o]ne slight risk with making cryptography so seamless is that bypassing the human prevents a level of interaction between person and machine that might be *desirable* from a security perspective" (2020: 193). Related to this, it is also important to ascertain that there are some trust assumptions behind computing. In the same way that Switzerland may claim that voters are trusted to vote in secret in postal voting, they are also trusted to perform certain computer activities. In this sense, Keith Martin (2020: 245) reminds us that:

> "Cryptography *also* relies on trust. For cryptography to work, we need to trust that certain mathematical computations are hard to perform on a computer. We need to trust that an attacker's computing power does not exceed anticipated levels. We need to trust that users of cryptography will behave in expected ways and not, for example, share their cryptographic keys on their social media accounts."

[430] In a similar way, the Swiss Federal Chancellery's requires that "voters are given the information required to check the authenticity of the website and the server used for vote-casting".

the election administration can decrypt the votes[431]. The question is which encryption algorithms and implementation can fully satisfy the requirements for confidentiality.

Furthermore, public key encryption should go hand in hand with specific provisions on secure key management, thus ensuring that malicious actors cannot misuse the key and decrypt the votes earlier than expected (this behaviour, as we will see below, could also compromise anonymity). In this regard, the use of public key encryption opens the door to the use of key-sharing mechanisms, and in most experiences the law itself specifies how many shares of this key are needed to decrypt the election results.

Last, but not least, the threat of quantum computing also poses the question whether legal provision on secret suffrage on remote electronic voting should also prescribe the use of post-quantum cryptography.

Cryptographic standards

In the case of remote electronic voting, it has been argued that symmetric encryption is not enough: it must be specified that confidentiality is ensured by means of public key cryptography. Furthermore, encryption must be based on generally accepted cryptographic standards. Not all implementations of public key cryptography are secure. A standard[432] is something that experts have evaluated and approved for widespread use (Martin, 2020: 61). A standardised cryptographic algorithm is scrutinized much more than any other algorithm[433] (Martin, 2020: 68). In this regard, Keith Martin (2020: 161) concludes that

> "[t]he lesson for us today is simple. When it comes to choosing a cryptographic algorithm, whether for confidentiality, data integrity, or entity authentication, choose the state of the art. Cryptographic algorithms are the core component of any cryptosystem, and there is no excuse for not using the best available algorithms. If a widely respected algorithm is being used and a cryptosystem fails, then the problem will almost certainly lie elsewhere."

[431] With this we do not preclude the resort to hybrid encryption, where both symmetric and asymmetric encryption are used: a message is encrypted using symmetric cryptography, and the symmetric key is then encrypted using public key cryptography. According to Keith Martin, "[e]xamples of important internet standards that all use hybrid encryption include *Transport Layer Security* (*TLS*) for secure web connection, *Internet Protocol Security* (*IPSec*) for establishing virtual private networks to enable activities such as working from home, *Secure Shell* (*SSH*) for secure file transfer, and *Secure Multipurpose Internet Mail Extensions* (*S/MIME*) for secure email" (2020: 269). By this we do not mean, however, that the use of only these standards is sufficient to ensure the confidentiality of votes cast.

[432] According to Keith Martin, the establishment of the *Data Encryption Standard* (DES) as the first encryption standard in the seventies was "unprecedented and facilitated the use of DES by commercial organizations in the United States, and de factor in many other countries around the world" (2020: 61). See also Simon Singh (1999: 249-251) and Steven Levy (2001: 37-65)

[433] Furthermore, standardised cryptographic algorithms are based on well-known mathematical problems (i.e., one-way trapdoor functions). According to Keith Martin (2020: 87):

> "the security of asymmetric encryption is connected to the computational problem around which the algorithm is designed. If the problem is well understood and widely believed to be difficult, which is the case for seeking prime factors, then confidence can be placed in the security of the associated asymmetric encryption algorithm. But it, for some reason, the computation problems turns out not to be as hard as everyone hoped, the algorithm is doomed."

Therefore, the use of standardised cryptographic standards is paramount[434]. At the end of the day, the hardness of a cryptographic algorithms depends on the belief that the reverse of one-way trapdoor functions such as factoring cannot be resolved efficiently. In the case of factoring, Keith Martin (2020: 161) notes that:

> "The claim that determining prime factors is hard can be based only on what we know, not on what we don't know. A more accurate version of this claim is that, even with the smartest techniques known today, determining prime factors seems to be hard. This doesn't mean that some child genius, or indeed artificial intelligence, of the future won't come up with a new method of determining prime factors."

In turn, the perceived level of difficulty "relies on assumptions about how much computing power an attacker can expend on the problem" (Martin, 2020: 164). For all these reasons, "cryptographic algorithm design tends to be extremely conservative, assuming the existence of much more powerful attackers than there are probably ever likely to be out there. Better safe than sorry" (Martin, 2020: 164). This is another reason to use standard cryptographic algorithms. Furthermore, standards also advise on ways in which algorithms should be used, and not only specify these algorithms (Martin, 2020: 164).

Likewise, standard procedures should also be used for the implementation of this standards, and for the conduct of certain tasks (such as data deletion). In addition to the cryptographic algorithms, the size or lengths of the keys should be specified as well[435]. One important aspect of encrypting the vote is that it should be non-deterministic, in such a way that the votes with the same answer or candidate are encrypted differently. Likewise, all ciphertext should be *padded* in order to be encoded with the same size (or otherwise the length of the ciphertext could be used to guess the contents). These are issues that should be specified in the cryptographic standards. An additional standard that should be taken into account are those for key management, that we discuss in the following section.

Key management and secret-sharing

Keith Martin reminds us that "[s]crambling the data is the *only* thing encryption does" (2020: 158). However, encryption does not control who has access to the decryption key[436] (2020: 158). Therefore, remote electronic provisions on secret suffrage should also touch upon key management[437].

[434] In fact, one principle in cryptography is that "[t]he security of a cryptosystem must not depend on keeping secret the crypto-algorithm. The security depends only on keeping secret the key" (Singh, 1999: 12)

[435] On key lengths, see footnote 284 above.

[436] And encryption neither plays a role in the protection of the data before it is encrypted or after it is decrypted (Martin, 2020: 158). For this reason, it is important to identify how is this data protected before encryption (as we have assessed in section I.1.a) above) and how is preserved in the long term (something we have covered in section I.1.b) above).

[437] According to Keith Martin, "[t]he main goals of key management are to keep secret keys secret, and to make sure we're using the right keys for the right things. Key management is arguably the hardest aspect of making cryptography work in real systems, because it's the interface between the cryptographic technology itself and the organizations and people who need to use it" (2020: 182).

According to Keith Martin, "[t]he best way of storing a cryptographic key is in secure hardware. Smartcards such as bank cards and SIM cards are lightweight examples. More heavyweight technologies for storing keys are *hardware security modules*, which are dedicated pieces of equipment for storing and managing keys" (2020: 192). In the three experiences, the shares of the keys are stored in smartcards. In turn, these smartcards are protected with passwords that are only known by the persons that guard them. While the support of the keys may be something too specific to be set at the level of the law, higher-level regulations could at least mandate that these issues are considered.

Furthermore, the distribution of responsibilities does not have to be limited to key-sharing. For example, the Swiss Federal Chancellery stressed in a recent report that "[e]-voting systems must be spread across multiple computers that are set up differently, some of which may not be connected to the internet. Technical and organisational measures must be in place to ensure that no individual can access critical data or votes without the involvement of another person (multiple-assessor verification)"[438] (2020c: 4).

c) Anonymous tallying

Regarding anonymity, the main conclusion is that in remote electronic voting the fulfilment of this standard is conditional to certain technological and procedural requirements. This fit wells with the definition of conditional anonymity offered by Douglas Jones, who distinguished between absolute and conditional anonymity in the following terms (2004: 3):

> "two perspectives on ballot secrecy, one that is absolutist, and one that is conditional on the correct functioning of the election apparatus (human and technical) […] their consequences for system design are quite different, and they also have very different behavioural consequences. Provisional ballots, for example, require that the voter's identity be attached until the end of the voting period, an option that is compatible only with the a [sic] conditional and not an absolute interpretation of ballot secrecy."

For Ülle Madise, "[t]he voter's right to anonymity during the counting of the votes is guaranteed to the extent to which this can be secured in the case of absentee ballots by mail: the so-called 'system of two envelopes' used for absentee ballots by mail is both reliable and easy to understand for e-voters" (2007: 16). And whereas we do not agree that analogies to postal voting are the best way to approach the issue, it is true that the national implementations of remote electronic voting have been inspired by already

[438] In a similar way, the Swiss Federal Council (2013a : 71) prescribed

> « Des mesures organisationnelles assurent la protection des données et leur destruction au moment voulu et excluent l'accès non autorisé à l'urne électronique et au registre d'utilisation du droit de vote : l'accès n'est autorisé que dans des cas précis, selon des règles précises (une autorisation préalable est nécessaire, le principe des quatre yeux s'applique, un système de surveillance est mis en place) et par des personnes bien précises (règles sur l'engagement du personnel qui travaille dans les infrastructures sensibles de l'État, engagement de ces derniers à respectes des accords spécifiques à ce sujet, etc.). Pour ce qui concerne les prestataires privés du vote électronique, ils sont également censés appliques les règles qui découlent des engagements contractuels qu'ils ont signés avec les cantons et la Confédération. Les électeurs sont informés des mesures à prendre pour sauvegarder le secret du vote (comme p. ex nettoyer la cache du navigateur. »

existing remote voting channels: postal voting[439]. In fact, it can be argued that anonymity is conditional to any voting method[440].

Therefore, the question is which mechanisms ensure a strong compliance with the standard of anonymity. Here is when the analogy to postal voting has limitations: it is not enough to separate the encrypted vote from the signature, proper anonymisation is needed. For example, mixing the votes as done in Switzerland (and sometimes in Estonia) or using the homomorphic properties of the encryption system as in France are necessary measures. Since these processes are of utmost importance to ensure anonymity, they should be clearly specified at the level of the law or the lower regulations. Our assessment of the three national experiences shows that such procedures are not clearly prescribed, which leaves the door open to insecure anonymisation procedures (such as the mere storing of the data separately, or the anonymisation based only in removing the digital signatures from the votes).

The key-sharing mechanisms as those prescribed for confidentiality should be required as well (otherwise, votes could be decrypted before being anonymous, and both confidentiality and anonymity would be breached). The Swiss case goes a further step here and prescribes that server-side operations (which include the anonymisation of the votes) be split into four different control components. When it comes to the system with control components, the Swiss Federal Council envisaged the following anonymization and decryption processes: each of the control components acts as a different node of the mix-net by shuffling and re-encrypting the votes. All the control components are then involved in the decryption of the votes. More specifically, control components (Swiss Federal Council, 2013c: 6):

> "1. The control components form a local network.
>
> 2. The voting system transmits all votes from the electronic ballot box to the first control components.

[439] Likewise, Chantal Enghehart has noted that « [c]omme tous les systèmes de vote par correspondance, les systèmes de vote par Internet reçoivent les votes des électeurs accompagnés de leur identité. Ces informations permettent de tenir à jour un registre des émargements afin de respecter le principe de l'unicité (un électeur, un vote) » (2010). In the Swiss case, the Swiss expert group noted that « le numéro de la carte de légitimation […] sert de moyen d'identification anonyme (« nom d'utilisateur anonyme »). […] Il n'est pas nécessaire de recourir à d'autres données personnelles. Le numéro de la carte de légitimation sert simultanément à l'authentification (« nom d'utilisateur anonyme et mot de passe tout en un ») » (2018: 26).

[440] For Douglas Jones, "[t]he choice between these two models of voter privacy should be viewed as a matter of public policy, not of voting technology" (2004: 3). We partially agree, as long as the same criteria is applied to any voting method. In this regard, the author notes that (Jones, 2004: 3):

> "[t]echnological arguments that purport to show that a given technology for conditional privacy is strong enough to be trustworthy should be taken as arguments to change the law to permit a conditional model, not as arguments for the use of technology offering conditional privacy in jurisdictions where the law calls for absolute privacy."

In practice, however, anonymity is always conditional. This is clearly the case when it comes to postal voting (as we have argued). But the same could be said about paper ballots in polling stations. As we have noted in chapter 2, anonymous voting in this case is conditional to the voter following some key steps (taking more than one paper ballot before voting, marking their choices inside the voting booth, not recording themselves while voting, or not making any signs to their ballots that could be observed by third parties during the count). Therefore, we can only agree with Douglas Jones as long as his use of "technology" is broadly understood to include both digital as based as paper-based voting methods.

3. The electronic ballot box performs re-encryptions, mixes the votes, calculates proofs and sends all values to the voting system.
4. The voting system transmits the re-encrypted and shuffled votes to the next control components, etc.
5. The voting system transmits the shuffled votes to the control components. The latter use their private key parts for decryption and to generate a proof that the decryption parts are correct. All values are signed and delivered to the voting system,
6. The voting system calculates the unencrypted votes using the partial decryptions."

Lastly, remote electronic voting regulations could also prevent the votes from being decrypted if the number of votes cast is too low and knowing aggregate results could compromise secret suffrage. Again, this is not something unique to remote electronic voting. Nevertheless, and in contrast to paper-based voting channel, the advantage of remote electronic voting is that aggregating encrypted votes is easier (and even more so if votes have been encrypted with homomorphic cryptographic algorithms). However, it could also be the case that no additional aggregation levels are feasible, and the number of votes to be tallied is still low. In those cases, procedural guarantees should be prescribed so these results are not publicly accessible.

II. THE PRINCIPLES FOR DEMOCRATIC ELECTIONS AND THEIR TRADE-OFFS: BALANCING THEM IN REMOTE ELECTRONIC VOTING

At this stage, one issue remains unsolved: secret suffrage is not the only principle for democratic elections. This is relevant because, as some authors have argued, the different principles for democratic elections may conflict with each other. For example, the fact that the vote is secret means –at least to certain extent– that not all the elements of the election can be properly observed or audited[441]. As a result, the integrity of the election is ascertained based on the observation of the voting and tallying procedure. However, when remote electronic voting is used, such processed can be no longer observed through the naked eye. In turn, compliance with the procedures enforcing the principle of secret suffrage need to be observed as well.

The very Recommendation of the Council of Europe acknowledges, in its Explanatory Memorandum, that "[t]here may be exceptions to the principles; restrictions to the conditions for implementing the principles may apply. Furthermore, in an e-voting context, it may be necessary to have a stricter application of one principle and a looser application of another" (Council of Europe, 2017b: para. 18). This is neither new nor unique to remote electronic voting. In fact, we have already seen how the mechanisms that have been introduced to ensure the secrecy of the vote have sometimes negatively impacted on other electoral principles, such as universal suffrage (since it may become more difficult for some

[441] Bernard Lang has summarised this conundrum as follows: « [l]e secret du vote ou l'intégrité de son expression sont chacun facile à assurer séparément, au détriment de l'autre : en ne transmettant pas le vote, ou en affichant publiquement le vote et son auteur (pour prendre des cas limites caricaturaux). C'est la combinaison des deux qui est complexe » (2006). Along these lines, the author raises the following question: « Si la perfection n'est pas atteignable, y a-t-il de la marge pour un compromis entre ces deux objectifs nécessaires, compte tenu de circonstances spécifiques, par exemple dans le cas des français de l'étranger ? » (Lang, 2006).

voters to exercise their rights, namely those abroad or voters with disabilities). The introduction of alternative voting channels (such as postal voting, or proxy voting, as discussed in chapter 2) has aimed at rebalancing the fulfilment of each of these principles. We argue that the introduction of remote electronic voting, and some of the (potential) challenges to secret suffrage, need to be understood from this perspective. In what follows, section 2 and section 3 deal with how secret suffrage has been balanced with universal and free suffrage, respectively[442].

Notwithstanding, the need for such balancing is not absolute. Not all the electoral principles present trade-offs between them. In fact, the key to identifying the proper balance entails finding a compromise where their fulfilment is maximised. For these reason, section 3 of this chapter will challenge some dichotomies, specifically those usually established between secret and free suffrage. We argue that the integrity of the elections, its accountability and its transparency, should also observe compliance with secret suffrage. Once again, this is not new: one of the key trends in the introduction of secret suffrage – as described in chapter 2 – was on how to supervise that ballots were cast in secret.

1. Secret and universal suffrage: when remote electronic voting enables secret suffrage

As we have seen, most of the cases analysed here introduced remote electronic voting as a means to making voting more convenient and accessible. Therefore, it could be argued that remote electronic voting contributes to the fulfilment of the principle of universal suffrage. Universal suffrage can be broadly understood as "that all human beings have the right to vote and to stand for election" (Venice Commission, 2002a: 1.1). Therefore, by making it possible for specific voters to actually exercise their right, remote electronic voting and universal suffrage go hand in hand[443]. For example, according to Priit Vinkel and Robert Krimmer (2016: 179),

[442] In the case of re-voting, as implemented in Estonia, the same could be said for secret, free, and equal suffrage. In this regard, the possibility to change an e-vote has been considered an "infringement of the right to equality and of university" (Madise, 2008: 18). However, we see no such conflict here, as only one of those votes is finally included in the tally. Furthermore, and while this option is offered to e-voters only, in Estonia everyone is eligible to vote online, which does not create any discrimination between eligible e-voters and non-eligible e-voters. Therefore, we will not consider such balancing in this chapter. Should the reader be interested in those alleged trade-offs, it is suggested to read the work of Ülle Madise (2007) and Priit Vinkel (2015).

[443] At the same time, it has been suggested that electronic voting may disenfranchise specific voting groups. For example, it has been argued that voting electronically requires high digital literacy skills and that therefore some voters with scarce digital knowledge may not feel comfortable casting their votes electronically. This argument hardly holds for these three case studies, where remote electronic voting is offered as an additional voting channel and does not prevent a voter from using alternative paper-based methods, such as postal voting or voting in polling stations. Furthermore, there are several recent studies that also challenge the assumption that remote electronic voting is not accessible. For example, in Estonia any correlation between age and use of online voting gradually disappeared after the third e-enabled election and lost any predictive power by the fourth election (Vassil et al., 2016). In Canada, Nicole Goodman has found that middle–aged and older voters are more likely to vote online that younger ones, and that being familiar with and use the Internet are not as powerful preconditions for remote electronic voting as it is generally assumed (). In the Swiss case, a study concluded that older voters are most likely to remain faithful to

> "[i]ntroducing remote electoral methods (also, e.g., postal voting) serves the citizen in providing an easily accessible and comfortable means of voting. In addition, remote voting is also considered a viable alternative for disenfranchised voters whose participation in elections has always been dependent on the methods they are offered – voters living or residing permanently abroad, voters who are living in conditions which make it difficult for them to attend elections for geographical reasons and voters with disabilities. All these voters need to make extra efforts in participating in the democratic process, and in all these cases, the principle of universality (or general elections) prevails over the possible concerns connected with the way of voting."

Convenience is undoubtedly an advantage of remote electronic voting: the option to cast any vote from anywhere, together with the fact that the vote cast is immediately received by the voting server (in contrast to postal voting) is one of this technology's main appeals. For this reason, remote electronic voting has been mostly favoured by voters abroad. This is the case in Switzerland, where associations of voters abroad have unequivocally supported the adoption of this voting channel[444]. Notwithstanding, from the perspective of secret suffrage this is not the most important voter group for which the introduction of remote electronic voting maximises both secret and universal suffrage.

Another voter group that benefits even more from remote electronic voting are voters with disabilities, and especially those who are blind or visually impaired, and voters with reduced mobility. These voters tend to need assistance in order to cast their vote independently when the only option are handwritten paper ballots. For example, the Swiss Federal Council stressed in its very first report that electronic voting could facilitate participation in elections and votes for many voters, with special focus on the blind and the visually impaired, whose opportunity to vote independently and in confidence with paper-based channels is limited[445] (Swiss Federal Council, 2002: 652). For this reason, the Report in 2006 targeted voters with disabilities as the second priority group, after voters

internet voting than 'digital natives' (i.e., younger voters) (Mendez and Serdült, 2017). More recently, another study covering 30 ballots between 2008 and 2016 in Geneva has found that "e-voting increases participation more for old than for young cohorts […] the convenience of internet voting especially appeals to people suffering from illness or mobility problems. This presumably accounts for the positive effects of e-voting availability on (very) old abstainers and occasional voters" (Petitpas, Jaquet, and Sciarini, 2021: 7).

[444] In one of the recent consultations by the Swiss Federal Chancellery (2019c: 19), one of the organisations by Swiss abroad stated that:

> « L'OSE approuve sans ambiguïté le vote électronique et sa mise en exploitation. Elle considère que le vote électronique est indispensable, car il est important pour la démocratie suisse que tous les électeurs puissent prendre part aux processus de décision politique, où que se situe leur domicile. L'OSE rappelle qu'il arrive souvent que les Suissesses et les Suisses de l'étranger ne puissent exercer leurs droits politiques parce que le matériel de vote leur parvient trop tard. Elle salue la phase d'essai longue et concluante à laquelle a été soumis le vote électronique et se déclare favorable à la mise en exploitation de ce dernier. Les avantages du vote électronique ne doivent pas pour autant faire oublier que la sécurité doit primer la vitesse. L'OSCE considère cependant que cet impératif est pris suffisamment en compte par la procédure d'autorisation et, par exemple, par l'obligation de procéder à un test public d'intrusion. »

[445] Along these lines, the recent survey by the Swiss Federal Chancellery also concluded that associations of persons with disabilities continue to support remote electronic voting. As summarised in the consultation's final report (Swiss Federal Chancellery, 2019c: 19),

> « [l]es organisations représentatives des personnes handicapées […] sont de manière générale favorables aussi bien à la mise en place du vote électronique qu'au projet. Elles soulignent qu'il faut garantir aux personnes handicapées la possibilité de participer librement au processus politique et que les canaux de vote actuels ne le font pas sans restriction. Les personnes handicapées sont souvent dépendantes de l'aide d'autrui, et ne peuvent donc exercer leurs droits politiques de manière autonome et dans le respect du secret du vote. Pour les organisations précitées, le vote électronique constitue le meilleur moyen d'assurer à ces personnes une accessibilité pleine et entière, pour autant que celle-ci soit effectivement garantie. »

abroad[446]. In the opinion of the Swiss Federal Council, voters with disabilities were being given an unprecedented opportunity[447] to vote without assistance, thereby guaranteeing the secrecy of their vote[448] (2013a: 103).

The same applies to the other two national experiences[449]. For example, for the 2015 elections in Estonia, the OSCE/ODIHR noted that "[v]oting online was available from 19 to 25 February through software that voters could download from the EVC website which included enhanced support for the visually impaired" (2015b: 5). More recently, the OSCE/ODIHR has also stated that "the Internet voting application was configured for use with special screen readers, which were used by some 200 voters" (OSCE/ODIHR, 2019b: 56).

In the French case, the updated Recommendation of the CNIL prescribes that remote electronic voting systems should be accessible to everyone, and especially to persons with disabilities and in particular those with visual impairment[450] (2019a: 3-4). In the case of public administration bodies, the Recommendation refers to the *référentiel général d'accessibilité pour les administrations* (RGAA) as a requirement. The CNIL also encourages other organisations to abide by the provisions of this toolkit.

[446] According to the 2013 report, there were two main reasons why voters abroad could benefit more than voters with disabilities from remote electronic voting in the Swiss case: first, because there was no electoral roll specific for voters with disabilities, in contrast to the electoral roll for voters abroad; and, second, because the limits fully applied to voters residing in Switzerland (regardless of whether they had a disability), while such limits had been removed for voters abroad (Swiss Federal Council, 2013a: 103).

[447] According to the Swiss Federal Council (2013a: 103),

> « [l]e rapport 2006 du Conseil fédéral sur le vote électronique accordait le deuxième rang de priorité aux électeurs handicapés, et en particulier aux handicapés de la vue qui devaient ainsi obtenir la possibilité inédite de voter sans aide extérieure, ce qui garantit le secret de leur vote. Le 1er janvier 2008 est ainsi entrée en vigueur une disposition selon laquelle la mise en œuvre du vote électronique sur le plan technique doit tenir compte des besoins des électeurs handicapés, notamment de la vue, pour autant que cela ne porte atteinte ni à la sécurité ni au secret du vote de manière disproportionnée. A cet égard, il convient aussi de mentionner la loi du 13 décembre 2012 sur l'égalité pour les handicapés, et plus particulièrement son art. 14, al. 2, qui prévoit que dans la mesure où les autorités offrent leurs prestations sur Internet, l'accès à ces prestations ne doit pas être rendu difficile aux handicapés de la vue. »

[448] To what extent these systems have actually met the accessibility requirements is a different issue. For example, the foundation « Zugang fur Alle » were able to test the demonstration version of the Zurich system in 2012 and posted a video of this experience online (Swiss Federal Council, 2013a: 103). For the following elections, the OSCE/ODIHR also noted that "[t]he Geneva system also provides for access by persons with disabilities, while the Neuchâtel system envisions such provisions to be in place in the future" (OSCE/ODIHR, 2016: 8). Notwithstanding, and as we have seen in footnote 445 above, voters with disabilities continue to support the introduction of remote electronic voting.

[449] Elsewhere, the case of New South Wales in Australia is paramount.

[450] In contrast, for non-electronic voting channels the OSCE/ODIHR mission that observed the 2012 parliamentary elections concluded that "[p]olling stations were generally accessible for disabled people, but no special means were provided for visually impaired voters who could thus not vote in secrecy" (2012c: 2). Previous EAM had also recommended establishing a means of voting in secret by eligible prison inmates (OSCE/ODIHR, 2012c: 3).

2. Secret or free suffrage: do end-to-end verifiable remote electronic voting technologies challenge secret suffrage?

The second principle that needs to be assessed against secret suffrage in remote electronic voting is free suffrage. According to Ülle Madise and Tarvi Martens (2016: 17),

> "[o]ne of the primary arguments has been that the security requirements of e-voting are extremely difficult to satisfy due to the conflicting requirements of confidentiality and auditability. The confidentiality requirement states that votes must remain anonymous; the auditability requirements – that every action in the system must be recorded."

If voting is secret –the argument goes– there are no means to observe or audit an e-enabled election, ensuring that the results are genuine. Likewise, auditability mechanisms aimed at enhancing transparency may end up compromising the principle of secret suffrage. The issue gains salience in view of the introduction of individual verifiability. Individual verifiability allows voters to verify that their vote has been cast-as-intended and recorded-as-cast. By means of verifiability mechanisms, it is possible for voters to identify systematic manipulations with sufficient plausibility. Verifiability has become established in the scientific literature in the last decade and an end-to-end verifiable system was first used in Norway in 2011. Since then, several countries have made of end-to-end verifiability a requirement for remote electronic voting, including Switzerland and Estonia.

We have already seen some definitions of end-to-end verifiability, but it is good to recall here its three main dimensions[451]:

- Cast-as-intended: the vote is cast according to the voter's intent.
- Recorded-as-cast: the vote has been registered by the voting server unmodified.
- Counted-as-recorded: the vote has been included in the final tally as it was registered by the voting server.

Whilst in principle verifiability mechanisms should not breach the secrecy of the vote (Swiss Federal Council, 2013a: 108), there is room to think that they actually do. For example, cast-as-intended mechanisms give voters some proof of the contents of the vote they have cast[452]. Since votes are cast from unsupervised environments, the mere fact that the voter can ascertain that their vote has been received by the voting server

[451] These definitions are based in the Swiss Federal Council's 2013 Report (2013a: 110). However, most definitions are quite similar. For example, the Council of Europe's definitions (which we will describe later on) are aligned with the Swiss Federal Council's. Likewise, it is aligned with the definitions by Rojan Gharadaghy and Melanie Volkamer (2010), that we have introduced in chapter 1. In turn, the OSCE/ODIHR's Handbook for election observation defines end-to-end verifiability as "a functionality of NVT systems that allows for the validation of results on a universal and/or individual basis" (2014: 7). More specifically, the OSCE/ODIHR distinguishes between (2014: 7):

> "[s]ystems with universal verifiability [that] provide means for an independent third party to establish that the result of an election was reported honestly and without manipulation through either manual or mathematical checks. On an individual level, voters are provided with the opportunity to verify that their votes were cast as intended, stored as cast, and (ideally) counted as recorded."

[452] For example, when analysing the individual verifiability mechanism used in Norway in 2011 (which was based also in return codes), Jordi Barrat et al. notices "concerns about the anonymity of the vote when return codes are in use. It is worth questioning how the application can send specific data about the value of a voter's ballot while maintaining the anonymity of the vote" (2012: 40). However, these authors conclude that by combining individual verifiability with a multiple voting scheme, this issue could be considered solved since "potential coercers will never know whether the code links to a counted ballot" (Barrat et al., 2012: 44).

(recorded-as-cast verifiability) – and sometimes even that it has been included in the final tally – is equivalent to providing evidence of the vote that has been cast by them. This, in principle, would breach the principle of secret suffrage. More specifically, individual verifiability would breach the standard of individuality, since they provide the voter with proof of the content of the vote cast for use by third parties[453]. On this subject, Joseph R. Kiniry *et al.* have concluded that "no usable [end-to-end verifiable internet voting] E2E-VIV protocol in existing scientific literature has receipt freedom when the voting computer is untrusted" [454] (U.S. Vote Foundation and Galois, 2015: 32).

In its 2013 report, the Swiss Federal Council argued that the introduction of verifiability properties in the so-called second-generation remote electronic voting systems[455] should be grounded in scientific evidence and explainable to the public by analogy[456] to paper-based voting channels (Swiss Federal Council, 2013a: 11). In the 2018 report by the Swiss Federal Chancellery, it was stressed that any such mechanisms should preserve the principle of secret suffrage[457].

[453] Against the requirement enshrined in standard No. 23 of the Council of Europe's Recommendation on e-voting, that sets that "[a]n e-voting system shall not provide the voter with proof of the content of the vote cast for use by third parties" (2017a: 6). The paper by Jordi Barrat et al. discusses whether cast-as-intended mechanisms can be considered to be in line with the provisions of the previous recommendations (2012: 40-43). In the updated Recommendation, the Explanatory Memorandum already clarifies that "individual verifiability can be implemented provided adequate safeguards exist to prevent coercion or vote-buying" (Council of Europe, 2017b: para. 70).

[454] It is also important to note that this report was written in 2015, when most of the systems analysed were not yet offering end-to-end verifiability. Furthermore, it does not analyse in detail neither the Swiss nor the Estonian Internet voting systems. For instance, by 2015 Switzerland and Estonia were only offering individual verifiability.

[455] As we have already seen in chapter 3, the Swiss approach called for a gradual introduction of verifiability. First, with individual verifiability mechanisms (so remote electronic could be used by 50% of the electorate); and second, with complete verifiability, which additionally included universal verifiability with control components (so it could be used by all the electorate). This approach is summarised as follows (Swiss Federal Council, 2013a: 109):

> « La première approche consiste à placer la partie fiable chez les électeurs (côté clients), Les ordinateurs privés n'étant pas a priori dignes de confiance, il faut fournir aux électeurs un appareil spécial qui leur donne la certitude que leur vois sera respecté. La fiabilité de ces appareils pourra être vérifié par des votes tests. La seconde consiste à la placer chez les exploitants de système (côté serveur). Plusieurs composants de contrôle entrent en jeu ici, dont le nombre dépend de leurs caractéristiques techniques. »

[456] The analogy goes back to the second report on remote electronic voting. The Swiss Federal Council's reasoning back then was that (2006: 5275):

> « Comme c'est le cas pour le vote traditionnel, lorsqu'on glisse son bulletin dans l'urne ou qu'on vote par correspondance, on ne pourra jamais exclure complètement, dans le cas du vote électronique, le fait que des votes soient falsifiés, manipulés ou qu'ils ne puissent pas être exprimés, que ce soit par hasard ou de façon illicite, ou le fait que le vote de certaines personnes soit observé par des personnes qui n'en ont pas le droit. »

Three years later, the Swiss Federal Chancellery noted instead that « [u]n autre aspect de la sécurité fait actuellement l'objet de travaux de recherche de la part de l'[école polytechnique fédérale de Zurich] EPFZ. Il s'agit de répondre à la question suivante : de quelle manière le [vote électronique] VE peut-il être effectué de manière sûre, sachant qu'une majorité d'ordinateurs privés sont infectés ? » (2011: 3).

[457] According to the Swiss Federal Chancellery (2018c: 13),

> « le secret du vote doit être préservé. Les votes, depuis le moment où ils sont saisis jusqu'à celui de leur déchiffrement par un procédé cryptographique après qu'ils ont été mélangés, ne doivent figurer à aucun moment sous une forme non chiffrée. La vérifiabilité va au-delà des exigences applicables aux autres procédures de vote : l'ensemble du processus de votation ou d'élection, depuis le vote jusqu'au dépouillement, doit pouvoir être contrôlé tout en respectant le secret du vote. »

For the Estonian case, Sven Heiberg, Kristjan Krips, and Jan Willemson have more recently concluded that "the Estonian Internet voting scheme does not provide full E2E verifiability, but instead balances the verifiability and coercion resistance requirements using a combination of verification, server-side auditability and option of re-voting" (2020: 95). At the same time, they also note that "the search for a better balance is on-going and the question of introducing some form of E2E verifiability without increasing the coercibility level of the protocol too much is one of the main directions of future research"[458] (Heiberg, Krips and Willemson, 2020: 95).

Interestingly, this may be the reason why individual cast-as-intended verifiability is not a requirement in the French case. The French Electoral Code only prescribes that, after casting their vote, an electronic receipt is displayed on the voting system allowing the voter to check online that their vote has been taken into account (art. R176-3-9). In the case of the CNIL, the Recommendation prescribes mechanisms that ensure the transparency of the operations for voters (security objective 2-07) (CNIL, 2019a: 5). The solution proposed to achieve this security objective does clarifies that the voter should be able to ascertain that their vote has been received by the voting server and that it contains their choices. Notwithstanding, it is proposed to offer this feature by allowing the voter to cast different test ballots that they should be able to decrypt to verify their contents, but that are not the actual votes cast[459] (CNIL, 2019c). This one seems a compromise not to breach secret suffrage, since the vote that is actually cast is never verified (neither it is verified that the vote that has reached the voting server contains the desired options). At level 3, universal verifiability mechanisms are also prescribed (security objective 1-02).

Therefore, it could be argued that end-to-end verifiability raises a latent ambiguity. We have already introduced Lawrence Lessig's idea of latent ambiguities in chapter 1. Here, it is important to recall that latent ambiguities are raised when digital technologies compel us to choose between two values, when the choice was clear for their original (i.e., analog) context. As summaries by Lawrence Lessig, "[i]n the original context, the rule was clear […], but in the current context, the rule depends upon which value the Constitution was

[458] In turn, Heiberg, Krips and Willemson conclude that "[t]here are still residual risks that E2E verifiability does not address" (2020: 95). In the Estonian case, "[f]or example, if a citizen never intended to vote, but due to hostile take-over of her e-ID, the attacker manages to submit a vote on her behalf, the voter would not learn about this fact even if there is strong E2E verifiability in place" (Heiberg, Krips and Willemson, 2020: 95).

[459] The so-called Benaloh Challenge (see footnote 63 below). More specifically, the solution suggested by the CNIL consists in (2019c)

> « Rassurer autant que possible les votants qui n'ont pas accès à l'expertise de la solution de vote, garante du bon fonctionnement du dispositif et de la sincérité et intégrité du vote dans son ensemble. Il s'agit de permettre aux électeurs de s'assurer que leur bulletin a été pris en compte dans l'urne et que les bulletins de vote sont construits de manière correcte.
>
> Pour ce faire :
>
> Chaque récépissé de vote contient une information unique, totalement décorrélée de l'identité du votant (empreinte numérique, numéro aléatoire, « preuve à divulgation nulle de connaissance », etc.) qui est calculée au moment où le votant valide son choix de vote. La plateforme de vote électronique est destinataire de l'information et la publie afin de la rendre accessible à tous les électeurs. Chaque électeur peut ainsi avoir la garantie que son bulletin est bien dans l'urne.
>
> De plus, la solution de vote permet aux votants d'accéder à un espace de test où il est possible d'effectuer différents votes de tests et de voir ce qui ressort de l'ouverture du bulletin sur le serveur, le but étant de s'assurer que les bulletins sont correctement construits. »

However, such mechanisms have not (yet) been put in place for public political elections in France.

meant to protect. The question is now ambiguous between (at least) two different answers. Either answer is possible, depending upon the value, so now we must choose one or the other" (2006: 25). The latent ambiguity in these cases would be between the values of secret and free suffrage. But what values are enshrined in the principle of free suffrage?

Overall, free suffrage can be understood as the ability for voters to form an opinion and to express their wishes (Venice Commission, 2002a: 3.1-3.2). Secret suffrage also imposes an obligation on election administrations to combat fraud (Venice Commission, 2002a: 3.2). Therefore, free suffrage is closely linked to transparency. For the case of (remote) electronic voting, the Council of Europe's Recommendation on e-voting broadly states in Standard No. 10 that "[t]he voter's intention shall not be affected by the voting system, or by any undue influence" (Council of Europe, 2017a). Additionally, according to Standard No. 14, "[t]he e-voting system shall advise the voter if he or she casts and invalid e-vote" (Council of Europe, 2017a).

The updated recommendation also prescribes end-to-end verifiability. For example, regarding individual verifiability, standard No. 15 sets that "[t]he voter shall be able to verify that his or her intention is accurately represented in the vote and that the sealed vote has entered the electronic ballot box without being altered. Any undue influence that has modified the vote shall be detectable" (Council of Europe, 2017a). In turn, standard No. 16 establishes that "[t]he voter shall receive confirmation by the system that the vote has been cast successfully and that the whole voting procedure has been completed" (Council of Europe, 2017a).

Lastly, standards No. 17 and 18 deal with universal verifiability. One the one hand, standard No. 17 reads that "[t]he e-voting system shall provide sound evidence that each authentic vote is accurately included in the respective election results. The evidence should be verifiable by means that are independent from the e-voting system" (Council of Europe, 2017a). On the other, eligibility checks are described in standard No. 18. This standard reads that "[t]he system shall provide sound evidence that only eligible voters' votes have been included in the respective final result. The evidence should be verifiable by means that are independent from the e-voting system" (Council of Europe, 2017a). Universal verifiability is therefore understood not just as counted-as-recorded verifiability (standard No. 18), but also in terms of making sure that votes counted have been cast by eligible voters (standard No. 17). The commonality between these two verifications is that they should be verifiable by independent means (that is why referred to them as universal verifiability, whereas in individual verifiability it is the voter themselves who verify).

We have also seen how certain provisions in the Explanatory Memorandum and the Guidelines dealing with free suffrage set some limitations for these mechanisms to fulfil secret suffrage (see for example section I.1.a) in chapter 4). However, we must now assess with more detail whether and to what extent does putting in practice these mechanisms may challenge the standards of secret suffrage. To do so, we will start with vote correctness, understood as the mechanisms that guarantee that the vote cast is valid (that is, the requirement in standard No. 14 in the Council of Europe's Recommendation) (section a). Second, we will study individual verifiability (cast-as-intended and/or recorded-as-cast) as it has been introduced in Switzerland, France, and Estonia to ascertain whether the specific mechanisms may breach any of the minimum standards of secret suffrage (section b). Lastly, our focus will be on universal verifiability mechanisms that help third parties to audit whether all votes validly cast have been duly counted and to identify whether there have been attempts of ballot box stuffing (section c).

a) Conformity checks (a.k.a. vote correctness)

For the case of (remote) electronic voting, the Council of Europe's Recommendation on e-voting broadly states in standard No. 10 that "[t]he voter's intention shall not be affected by the voting system, or by any undue influence" (Council of Europe, 2017a). Additionally, according to standard No. 14, "[t]he e-voting system shall advise the voter if he or she casts and invalid e-vote" (Council of Europe, 2017a). The Explanatory Memorandum further details the provisions of standard No. 14 by specifying that (Council of Europe, 2017b: para. 54),

> "[t]he present standard does not require that the invalid voting possibility is introduced as a voting option. It only requires that, whenever an invalid vote is received by the e-voting system for whatever reason, the voter that issued that vote shall be informed accordingly. The aim is to avoid unintentional invalid e-votes. It applies in all cases, whether the e-voting system allows or disallows invalid votes. Of course, it only applies to votes cast electronically."

Interestingly, this requirement can be understood in different ways. First, it may convey that the marks made by the voter are valid according to the electoral rules. Another interpretation is that the vote has been properly encrypted, and that it will be possible for the voting server to decrypt those options. We have seen that in some cases votes have been erroneously encrypted – wilfully or due to technical reasons – and they have not been included in the final tally (see for example the Estonian case in 2011 or the French one in 2012, both described above). The Explanatory Memorandum seems to point towards the later understanding of this requirement, by specifying that voters should be informed about the validity of their vote when it is received by the e-voting system. In principle, the cast-as-intended verifiability mechanisms that we will describe later allow a voter to ascertain that their vote has been properly constructed, but what happens if voters do not verify their votes (in Estonia it is not compulsory to do it) or when it is not possible to verify the contents of the votes cast (such as in France)?

One alternative is vote correctness. In 2013, the Swiss Federal Council noticed that in Neuchâtel it was not possible to confirm whether a vote contained the valid options or whether it was properly encrypted until the decryption and counting stages, when it would be too late to warn them about the issue (Swiss Federal Council, 2013a: 72). In contrast, other cantons had opted for a ballot conformity check that allowed them to detect and reject any ballot that did not match the required format already during the voting period. In such cases, the system immediately informed the voter during the voting session. According to this approach, the electronic ballot should only contain the possible choices allowed for the ballot in question (Swiss Federal Council, 2013a: 72).

The issue raised here is how this conformity check is conducted: if the system decrypts and reads the contents of the vote at the casting stage, secret suffrage would be breached. The vote is still not anonymous and can be linked to the voter (otherwise they could not be informed of the non-conformity), which means that the voting server could clearly link the contents of the vote cast to the voter who has cast them, and it could store a proof that could be even used by third parties. However, in the opinion of the Swiss Federal Council (2013a: 72), the three systems complied with the federal obligations on secret suffrage and the different approaches fit the margin of appreciation that the cantons had.

Nowadays there is a general obligation to conduct this conformity checks (requirement 2.6.3., Annex to VEleS)[460]. This conformity check is achieved by using the cryptographic properties of homomorphic encryption, without having to reveal the contents of the vote (as we will explain in the next section, dealing with individual verifiability). Since France uses homomorphic tallying, the correctness of the vote is also ascertained from the moment the vote is cast, again without breaching secret suffrage: in homomorphic tallying it is necessary to validate that the vote includes correct answers, and this is done over the encrypted vote, thus complying with the standards of individuality, confidentiality, and anonymity. Otherwise, this anonymous tallying method would not work. In contrast, in Estonia it is necessary for the voter to individually verify their vote in order to confirm that it has been properly encrypted and with the right option.

In principle, none of these mechanisms challenges the secrecy of the vote. These processes are independent from the voter, and (with the exception of the Estonian case) they do not need to take any further steps. Conformity checks would therefore not currently raise any issue regarding secret suffrage, and they help guarantee one of the dimensions of free suffrage.

b) Individual verifiability: can verifiable remote electronic voting be free of coercion?

Individual verifiability mechanism, in contrast, can be said to generate receipts of the vote cast and therefore could challenge secret suffrage's standard of individuality. It should be recalled that according to this standard, enshrined as Standard No. 23 in the updated Recommendation on e-voting, "[a]n e-voting system shall not provide the voter with proof of the content of the vote cast for use by third parties" (Council of Europe, 2017a). It is important to stress that the goal of individual verifiability is not to provide a proof of the content of their vote, but to prevent the vote from being tampered with during the casting or the transmission stages.

According to the Council of Europe's recommendation on e-voting and the general understanding of this mechanism, individual verifiability has two main dimensions. The first dimension is cast-as-intended verifiability. It is enshrined in standard No. 15 of the Council of Europe's recommendation as the means by which "[t]he voter shall be able to verify that his or her intention is accurately represented in the vote […]. Any undue influence that has modified the vote shall be detectable" (Council of Europe, 2017a).

[460] It is important to stress that this requirement applies to all systems, including those that do not offer individual verifiability. In this regard, the requirement reads that "[i]f the vote has been cast in conformity with the system, the system stores the vote in the electronic ballot box and informs the voter that the vote has been cast successfully. Votes not cast in conformity with the system are not stored in the electronic ballot box" (Annex to VEleS). In a footnote, the Annex also specifies that (Swiss Federal Chancellery, 2018d: 9):

> "[a] vote is properly cast if a ballot paper has been completed in a pre-determined way. How and whether votes that have not been properly cast should ultimately be taken into account may be defined in advance. For example, it may be decided that where there is a question on the ballot paper, only the responses 'yes', 'no' or no response at all can influence the result of the vote. A response such as 'I don't want to vote' would not constitute a properly cast vote in this case. Whether it is even possible to place votes not properly cast in the electronic ballot box, whether they are ignored at the count or whether then may even be shown in the end result must be decided in advance."

Second, there is recorded-as-cast verifiability. It is also expressed in standard No. 15, as a requirement that "[t]he voter shall be able to verify […] that the sealed vote has entered the electronic ballot box without being altered. Any undue influence that has modified the vote shall be detectable" (Council of Europe, 2017a). In a similar way, Standard No. 16 also prescribed that "[t]he voter shall receive confirmation by the system that the vote has been cast successfully and that the whole voting procedure has been completed" (Council of Europe, 2017a).

The question raised here is whether individual verifiability (both cast-as-intended and recorded-as-cast) may somehow compromise the standards of secret suffrage. For example, the OSCE/ODIHR has noted that (2014: 47-48)

> "[i]n some Internet voting systems, mechanisms are provided for individual verifiability. In principle, this means that the voter is able to check – combining several pieces of information – if the cast vote was recorded correctly according to her or his intentions. Any single piece of information should not reveal the content of the vote, which would violate the secrecy of the vote if it provided the voter with a way to prove to third parties how she or he voted."

At the end of the day, if by means of individual verifiability it is rendered visible to the voter any manipulation of their vote during transmission (and on the client platform[461]), what can prevent that they misuse this mechanism to show the contents of their vote to a third party?

The Swiss Federal Council acknowledged this apparent ambiguity in its 2013 report, but it concluded that no such contradiction actually existed[462]. The conclusions reached in the Estonian case are quite different. For example, it has been noted that "the more information we give to the voter about their vote, the more the secrecy of the vote is undermined. In order to ensure freedom of the vote, it should not be possible to use this information against the voter" (Koitmäe, Willemson, Vinkel, 2021: 141). For Sven Heiberg, Kristjan Krips, and Jan Willemson, "breaching privacy of the vote […] is an inherent risk present with any kind of verification that has to be accepted. This is similar to the present Estonian vote verification" (2020: 88).

The reason that may explain why a different conclusion has been reached in the two countries is due to their different approaches towards individual verifiability. Therefore, a

[461] It is important to stress that, in Switzerland, individual verifiability is broadly understood as those mechanisms that « permet[ent] au votant de déterminer si son suffrage a été enregistré correctement par le système, c'est-à-dire tel qui l'a exprimé. Le votant peut ainsi s'assurer que son suffrage n'a pas été modifié de façon abusive sur la plateforme de vote ou sur Internet » (Swiss Federal Chancellery, 2020c: 4).

[462] By contrast, the report stressed that the challenges to secret suffrage laid in the kind of vulnerabilities that we have described in the section I.1.b) above. According to the Swiss Federal Council (2013a: 110):

> « Vouloir instaurer la vérifiabilité tout en garantissant le secret du vote (jusqu'au dépouillement) peut paraître contradictoire à première vue. La pratique montre que ça ne l'est pas. L'une et l'autre dépendent du bon fonctionnement de la partie fiable, ce qui implique que le décryptage n'est autorisé à aucun moment jusqu'au dépouillement (cryptage de bout en bout). Il y a toutefois une différence en ce qui concerne les éléments de la partie fiable : le respect du secret du vote dépend aussi de la fiabilité de la plate-forme client, qui appartient à la partie fiable, avec les composants de contrôle et les autres éléments évoques ci-dessus. Les tentatives de violer le secret du vote sur la plate-forme client n'échoueront donc que si cette plate-forme est suffisamment protégée et indemne de toute attaque de maliciel. »

more detailed account of how individual verifiability is achieved in the different national experience seems necessary. Here, it is important to describe the use of verification codes in Switzerland, and the verification app used in Estonia[463]. Both systems provide cast-as-intended and recorded-as-cast verifiability, but do not allow a voter to ascertain that their vote has been included in the final tally. In contrast, voting receipts like the ones offered in France do not allow a voter to verify the contents of their vote, but does generate a proof that the vote has been counted. Only in Switzerland the combination of verification codes and voting receipts allows a voter to ascertain that their vote has been cast-as-intended, recorded-as-cast, and included in the finally tally.

Verification codes (cast-as-intended and recorded-as-cast verifiability)

In Switzerland, there was a concern that viruses and malware in the voter's casting device could manipulate the choices made by the voter. For example, malware could change their affirmative stance in a matter put to a vote for a negative one (or the other way around)[464]. For this reason, it was envisioned to use verification codes in order to ascertain that the vote received by the server contained the choices actually made by the voter. By using verification codes[465] jointly computed by the voting client and the voting server, individual verifiability (both cast-as-intended and recorded-as-cast) could be achieved.

In order to vote, each voter receives a voting card with a list of codes that allows them to verify that their encrypted vote has reached the voting server with their choices unmodified (Swiss Federal Council, 2013a: 111). This card includes: an encrypted

[463] There are other proposals for individual vote verification, such as the cast or challenge mechanisms (also called Benaloh challenge). In this mechanism the voter marks their choices and then the vote is encrypted. To verify the contents of their vote, the voter then can "challenge" the voting device and decrypt the vote instead of casting it. The vote challenged is not the vote that is going to be actually cast, which is a shortcoming. However, the voter can challenge their device several times in order to ascertain that the voting device is not compromised and only when they are satisfied, they would actually cast their vote. This approach has not been used in any of the three national experiences analysed here, although it seems to be the preferred solution for the CNIL, as we have seen in footnote 459 above. For an overview of individual verifiability mechanisms in public political elections, we suggest the paper by Jordi Puiggalí *et al.* (2017).

[464] These concerns were raised as soon as 2006. In this regard, the Swiss Federal Council (2006: 5257) noted that

> « [l]a saisie du vote sur l'appareil prévu à cet effet, qui précède directement la transmission, est une opération à haut risque. À ce stade, des virus ou des chevaux de Troie pourraient tenter de manipuler les votes à l'insu des électeurs en substituant par exemple des votes « oui » à des votes « non ». Dans ce cas de figure, les procédés cryptographiques ne sont d'aucun secours. Ce domaine doit dès lors lui aussi être qualifié d'ultrasensible. »

This is an actual concern, quite unique to digital technologies (although certain inks could also behave in this way by becoming invisible and therefore unmarking a voter's choice in a paper ballot). However, this looks much more likely when it comes to digital technologies. for Keith Martin (2020: 130-131):

> "[t]he fact that a computer could behave differently from the way a human user expects, or indeed conduct tasks that the human user is unaware of, is something attackers often exploit. We cannot prevent this gap between humans and devices, so we have to manage it somehow. One method that you will undoubtedly have encountered is the *captcha* (a term that derives from the phrase 'completely automated public Turing test to tell computers and humans apart'). Captchas are used to test the presence of a human by setting tasks that machines are currently less effective at, such as deciding which alphabetic characters are suggested by an almost illegible squiggle, or which of a series of photographs features a building that could plausibly be a shop."

[465] For a more detailed description on how verification codes work, we suggest reading the paper by David Galindo, Sandra Guasch, and Jordi Puiggalí (2015).

identifier; a control code per candidate or per possible answer, randomly ordered; a confirmation code; and a finalisation code.

Because the system has to comply with the principle of the secrecy of the vote, only the voter themselves can do the verification (Swiss Federal Council, 2013a: 110; Swiss Federal Chancellery, 2018c: 13). The voter starts the session by typing their encrypted identifier, selecting their options, and casting their vote (which is encrypted in the voter's device and digitally signed). Once the vote is cast, the voting device and the voting server jointly compute a code that is displayed by the voting application, without revealing the actual encrypted options. Then the voter checks this code against the list of codes in the voting card: if the code displayed is the one that corresponds to the voting option that they have selected, they have to type their confirmation code (Swiss Federal Chancellery, 2018c 13). Therefore, this verification method is compulsory for the vote to be confirmed (although the voter can always confirm their vote without looking at the actual code returned by the system[466]).

In this scenario, the confidentiality of the choices depends on codes being kept secret (Swiss Federal Chancellery, 2018c 13). This is achieved in part by the voter not sharing their voting card, but also by adopting specific requirements for the generation and distribution of the cards. According to the Swiss Federal Chancellery's 2018 report, special requirements are therefore needed to generate the codes and, in particular, to print them. Furthermore, these codes should be sent through a different channel than the one used to vote (i.e., the electronic) and they are currently being sent by post. Otherwise, malicious software installed on the equipment used to vote could read them and reveal the voting options (Swiss Federal Chancellery, 2018c 13).

Therefore, this system complies with the principles of secret suffrage as long as there are specific requirements for the print office[467] responsible for generating, printing, and

[466] In this case, it is assumed that « [l]e système vérifiable doit donc impérativement lui donner la possibilité – facultative – de procéder lui-même à la vérification. En supposant qu'un nombre suffisant de votants en useront, il sera possible de découvrir les manipulations systématiques » (Swiss Federal Council, 2013a: 110; Swiss Federal Chancellery, 2018c: 13)

[467] It is important to highlight that, given the broad use of postal voting in the country, strict security requirement for print offices were set from the outset. For example, already in the 2006 report, the Swiss Federal Council noted that « [l]'établissement des cartes de légitimation est délégué a des imprimeries qui doivent satisfaire à des exigences de sécurité élevées. Les cartes de légitimation contiennent notamment les données d'accès permettant de s'identifier sur le serveur réservé au scrutin. Dans les trois cantons, les codes d'accès sont imprimés sur la carte de légitimation. » (Swiss Federal Council, 2006: 5252). As we have seen, in Neuchâtel, according to the Swiss Federal Chancellery (2004: 35),

> « [t]outes les cartes de légitimation sont générées ainsi que le registre d'électeurs disposant d'un accès au GSU pour autoriser le vote électronique. C'est durant ce processus que sont générées également les codes de validation et de confirmation, imprimés sur les cartes de légitimation. Les cartes de légitimation sont ensuite transférées au centre d'impression cantonal pour y être imprimées. Pour des raisons de sécurité, le papier utilisé comporte un hologramme représentant l'écusson du canton de Neuchâtel. »

However, each canton relied on a different approach. According to the Swiss Federal Council (2006: 5252-53),

> « [l]es électeurs ont en outre besoin d'un mot de passe pour l'opération d'authentification. En l'occurrence, les trois cantons ont opté pour des approches différentes : celui de Genève a choisi de dissimuler le mot de passe sous un film à gratter ; celui de Zurich a opté pour un système similaire, à la différence près que le mot de passe est caché sous un champ Hydalam ; celui de Neuchâtel, enfin, a décidé de ne donner la possibilité de voter par voie électronique qu'aux électeurs qui se sont inscrits au GSU. Ces personnes reçoivent par courrier séparé le mot de passe leur

delivering the voting cards to each voter. Nevertheless, in 2011 the OSCE/ODIHR's EAM noted that most steps of the printing of voting cards, including access to unprotected voter credentials, were being conducted by a single person with minimal oversight (2012: 17). For this reason, in its subsequent report, the Swiss Federal Council stepped up the consideration of the print office to an essential partner[468] (Swiss Federal Council, 2013a: 45). In this regard, the Swiss Federal Chancellery and the cantons jointly adopted a set of requirements for print offices (Swiss Federal Chancellery, 2013a). The goal was that printing services could be still considered a reliable component of the electronic voting system in terms of verifiability and secrecy of the vote, at least in the mid-term (Swiss Federal Council, 2013b: 3). More recently, the Swiss Federal Chancellery has reached a similar conclusion (2020b: 15):

> "The effectiveness of individual verifiability hinges on return-codes, the confirmation code and the finalization code being secret and impossible to predict. In practice, the tasks of the Printing Office are divided. The generation of the codes and other parameters are performed in the cantonal premises. The physical printing is done by a printing company. The printing-office holds the codes in plain-text. At the latest when the codes are being printed, there can be no cryptographic means to protect these codes from being divulges. The codes have to be protected by organizational means."

Cast and decrypt (cast-as-intended and recorded-as-cast verifiability)

In Estonia, individual verifiability (both cast-as-intended and recorded-as-cast) is based on a different approach: the vote is cast into the voting server, and then the voter can download it and decrypt it to ascertain that it has reach the voting server and that it includes the selected options. To prevent any misuses, this verification can be conducted only after the vote has been cast, for a 30-min period, and a maximum of three times[469]

> permettant de se connecter au GSU. Qui plus est, les électeurs neuchâtelois reçoivent une carte à numéros qui est comparable aux listes de codes à biffer en usage dans le telebanking » (Swiss Federal Council, 2006: 5252-53).

[468] According to the Swiss Federal Council (2013a: 45),

> « [l]'imprimerie est un partenaire incontournable. La plupart des cantons font imprimer le matériel de vote par des entreprises privés, sauf Neuchâtel et quelques cantons du consortium, où cette tâche est assurée par une imprimerie de l'État. Étant donné le rôle particulièrement important de l'imprimerie en ce qui concerne le secret associé aux codes de vote électronique et la diversité des pratiques cantonales en matière de certification des imprimeries, la Chancellerie fédérale a adopté, en collaboration avec les cantons, un catalogue de critères obligatoires pour l'impression des cartes d'électeur pour le vote électronique. Ce catalogue traduit en exigences spécifiquement applicables aux imprimeries les exigences générales de l'Ordonnance en Droits Politiques. »

[469] A detailed account of this verifiability mechanisms is offered by Mihkel Solvak (2016: 129):

> "E-vote verification is possible using a smart device that runs on Android, Windows Phone or iOs, has a camera to read a QR-code and internet connectivity. Verifying and individual e-vote is fairly straightforward. After casting an e-vote on a computer, the voting application displays a note with a QR-code. The voter can simply close the application and be done with voting, or they can take a separate smart device, download the verification app from Google Play, App Store or Windows Phone Store and use this app to read the displayed QR-code. Once the code is read and the smart device has communicated with the central server and received the encrypted vote, it will display a note on whether the e-vote cast from the computer was received by the server and upon requests shows the candidate name and number for whom the vote was cast. The verification app then closes automatically after 30 second. The app does not show any personal information of the voter and only one vote can be verified with it at a time. Each e-vote can be verified up to three times, but no later than 30 minutes after the vote was cast. If there is a conflict between the given vote and the information displayed on the separate smart device, either the computer used to cast the vote is compromised or there are more sophisticated problems with the e-voting system. In any case, the voter should report the conflict to the election authority and can revote with another device or vote on paper at the polling station."

(Solvak, 2016: 129). The system neither displays whose vote is being verified. Lastly, the voter has no way to know whether that specific vote is included in the final tally, nor can they prove to a third party (a coercer or a vote-buyer) that the vote shown is indeed theirs or the last one that they will cast.

Nevertheless, one of the conclusions reach by the OSCE/ODIHR's EET that observed the 2015 *Riigikogu* elections was that "[v]oters who voted online so close to the end of Internet voting as not to be able to change their votes could potentially demonstrate for whom they voted by showing their cast ballot as displayed on the computer screen or a mobile phone" (OSCE/ODIHR, 2015b: 4). According to the ETT's final report, this was because voters who vote online were "ineligible to cast paper ballots on election day"[470] (OSCE/ODIHR, 2015b: 4). While this was already prevented by having an extended advanced voting period to vote in paper than the one to vote online even during the advanced voting period (Heiberg, Krips and Willemson, 2020: 91), we have already seen that the Estonian authorities currently allow online voters to vote on election day as well and thus to cancel their online vote. Therefore, voters always have the choice to cancel their vote cast online by going to a polling station and casting a paper ballot.

Notwithstanding, the system still has some shortcomings. For example, according to Mihkel Solvak "[l]ooking at smart device access and QR-code familiarity in combination shows that only about 11% of eligible voters fulfil both of these prerequisites"[471] (2016: 131). Furthermore, this author argues that "the possible positive effect upon trust towards e-voting as such is probably limited. The technical solution is simply somewhat excluding" (Solvak, 2016: 131). Furthermore, the OSCE/ODIHR's EET for the 2019 *Riigikogu* elections concluded that "an internal attacker with privileged access to digital ballots could break the vote secrecy of any voter who published an image of the QR code online, even after the expiry of the code's validity [and that] this contradicts national legislation and international standards pertaining to vote secrecy" (OSCE/ODIHR, 2019b: 8).

Even more important, it should be noted that with this system "the voter is not able to check whether the ballot that reached the voting system will be counted in the tally as such an ability would also made vote selling easier"[472] (Heiberg, Krips and Willemson, 2020: 93). According to these authors, "[t]he current verification system is optimised for being coercion resistant and thus verification does not reveal if a re-vote has been cast" (Heiberg, Krips and Willemson, 2020: 93). This is important because already in 2013, a possible attack was found where a compromised computer could cast another vote without

[470] Interestingly, this was the result of a legal requirement aimed at complying with the principle of equal suffrage, as we have discussed above.

[471] According to According to Arne Koitmäe, Jan Willemson, and Priit Vinkel (2021: 145)

> "a smart device application is used for verification, but it does not help in the case when the voter is unaware that someone has cast a vote on their behalf. Since this method requires action on the voter's side, it hasn't achieved wide usage. The share of i-votes verified by the voters has remained between 4-5 per cent of all i-votes since 2014. It can be used to detect certain mass attacks against i-voting (e.g. when malware is trying to manipulate active voting sessions), but not all of them (e.g. when malware itself initiates the sessions without voter participation)."

[472] According to Sven Heiberg, Kristjan Krips, and Jan Willemson (2020: 95), "[o]ne of the strongest measures suggested against such a threat is end-to-end (E2E) verifiability that would allow every voter to verify that her vote has been correctly counted in the final tally. Unfortunately, such a strong notion of verifiability potentially conflicts with voter privacy and coercion-resistance."

the voter knowing, thus cancelling the genuine vote with a tampered one[473], "where ID-card is left attached to the working terminal for extended periods of time, e.g. as a login token" (Heiberg, Krips, and Willemson, 2020: 84). In the end, the risk of being disenfranchised may be higher than the risk of actually being coerced into voting in a certain way[474].

Voting receipts (recorded-as-cast verifiability)

As we have seen, neither verification codes nor cast and decrypt mechanisms ensure that the vote cast and individually verified has been included in the final tally. At the end of the day, the voter verifies that the vote has been received by the voting server, but it could be deleted from the "electronic ballot box" or excluded from the tally without them noticing. For this reason, it is also possible to publish a list of receipts for the votes that have been included in the tally. If the vote has been counted, the corresponding receipt should appear in the list.

This option is feasible both in Switzerland and France, even if in France there is no cast-as-intended verifiability. Nevertheless, the CNIL's updated Recommendation does prescribe that upon casting their vote, the voter should receive a confirmation that their vote has been cast and should be able to keep evidence of this confirmation (CNIL, 2019a: 5). In the Swiss case, the receipts have also been used since the early stages in the introduction of remote electronic voting. For example, in Neuchâtel a list with the receipts corresponding to the votes included in the tally was published at the end of the election already in the first trials[475] (Swiss Federal Council, 2006: 5228).

[473] This vulnerability has been described as the Ghost Click Attack by Drew Springall *et al*. (2014). This a clear example of a conflict between secret and free suffrage: because voters can cast multiple ballots (to enhance individuality and confidentiality) but they cannot known which one of the votes will be finally included in the tally (to comply with the requirement for receipt-freeness), their vote can be cancelled at any time without they knowing.

[474] There are several alternatives that have been envisaged to mitigate this risk. Among them, there is the option to provide a feedback channel, as we will approach in our discussion of voting receipts below. Yet another alternative would be to ask the voter to input a confirmation cast code during the voting phase, that should be different each time they vote, and could be delivered to them not using electronic means. For example, in France voters receive a PIN with an SMS at the time of voting that they need to input to confirm the vote cast. In spite of this mechanism having raised certain issues when voting from abroad (because of the signal or how SMS are delivered in some countries) this would not be an issue in Estonia, at least for those voters casting a vote from their country. For an overview of this methods, we suggest the paper by Adrià Rodríguez-Pérez, Jordi Cucurull, and Jordi Puiggalí (2022).

[475] More recently, the Swiss Federal Council also concluded that the recorded-as-cast verification could be entrusted to third parties (2013a: 110):

> « les autorités et les employés des bureaux de vote jouissant d'une confiance importante, cette vérification peut être confié à des tiers dignes de confiance (appelées vérificateurs). La désignation de ces tiers (commission électorale, observateurs électoraux ou volontaires, p. ex.) dépend des bases juridiques, du contexte politique et des besoins de la société. Les données nécessaires aux vérificateurs pour répondre aux recorded-as-cast et counted-as-recorded peuvent aussi être publiées si nécessaire. »

However, third parties can only verify if the votes received by the server have been included in the final tally (i.e., identifying any deletion of the votes that have been stored in the server). It is unclear how a third-party could verify whether a vote cast has been received by the server, which still leaves in the hands of the voter themselves to do part of the verification.

In Estonia, however, the system does not offer any way to confirm that the vote has been tallied or counted as intended[476] (Koitmäe, Willemson, Vinkel, 2021: 147). However, and "in order to convince voters that their votes had been correctly registered, they were provided with the option to check whether their e-vote had been reflected on the polling list on Election Day" (Vinkel, 2016: 54). According to Priit Vinkel, "[i]n addition to the verification itself, a second option for confirming the arrival of an e-vote has been made possible during the e-voting period. If the voter decided to replace the e-vote with a new one, they were notified in the voting app of the previously recorded e-vote being stored in the central system" (2016: 54). According to Arne Koitmäe, Jan Willemson, and Priit Vinkel (2021: 141):

> "A well-implemented i-voting system can use cryptography to guarantee that the ballot is sent and received as intended, with its integrity untouched. An observer or an auditor can make sure that all the votes cast are accounted for, that the votes included in the tally are the same as cast, and that the votes were tabulated correctly. However, voters themselves cannot fully verify i-voting results and people need to have absolute faith in the accuracy, honesty and security of the whole electoral system."

The problem with receipts is that, and since in remote electronic voting the casting of the vote takes place in uncontrolled environments, it may not be necessary to have a proof of the contents of the vote to coerce or buy someone's vote. It would be enough with being with the voter at the time of voting (face-to-face or remotely, as we have described in section I.1.a) above) and use a voting receipt as evidence that that specific vote has been included in the final tally.

c) Universal verifiability: public bulletin boards, blockchain technology, and (again) long-term privacy

The introduction of universal verifiability mechanisms could be said to compromise the principle of secret suffrage as well. For example, according to the OSCE/ODIHR, "[f]or Internet voting systems, universal verifiability is difficult to provide without jeopardizing the secrecy of the vote, especially in cases where ballots are very complex" (2014: 47). Alternatively, the need for universal verifiability may be seen as the result of the votes being encrypted to preserve confidentiality and to ascertain the integrity of the votes following the anonymisation and decryption procedures[477]. In the opinion of the Swiss

[476] According to Arne Koitmäe, Jan Willemson, and Priit Vinkel (2021: 147), the Estonian system offers the following feedback:

> "– Confirmation that the vote collecting service has received the i-vote and received it as intended. In Estonia this is currently implemented by the smart device verification app.
>
> – Confirmation that the i-vote was included in the set of i-votes that are going to be tallied. Since the list of i-voters is created by the Internet voting system, a voter can check if their i-vote is included in this list, but this action is very inconvenient to the voters […].
>
> – Confirmation that the i-vote was amongst the i-votes tallied. Currently no feedback for the voter exists here, but the integrity of the i-vote set is verified by the EMB and auditors.
>
> – Confirmation that the vote was counted as intended. Currently no feedback for the voter exists here, but the result can be verified by the tallying proof by the EMB, auditors and by anyone who has created an auditing application."

[477] For example, Jordi Puiggalí (2019) notes that

> "[t]he Mixing process is used to anonymize the votes before decryption, shuffling and re-encrypting the votes using the election public key. Since the process prevents to correlate the output shuffled and re-encrypted votes from the input ones, an attacker could use this property to substitute the

expert group[478], the introduction of cryptographic mechanisms aimed at guaranteeing universal verifiability helps overcome the apparent contradiction between transparency and the guarantee of secret suffrage (2018: 10).

In 2011, the Swiss Federal Chancellery argued that verifiability was the easiest and cheapest mechanism to verify the results of remote electronic voting and to prove to stakeholders (citizens, electoral commissions, politicians, etc.) that the results were genuine[479] (2011: 5). In the opinion of the Chancellery, universal verifiability complements individual verifiability in the steps that follow the validation of the vote by the voter themselves (Swiss Federal Chancellery, 2018c: 14). For this reason, the combination of individual and universal verifiability is often referred to as complete verifiability[480] (instead of the more common reference to end-to-end verifiability). Such steps include the validation of the digital signatures of the votes cast (similar to the reconciliation procedures in remote postal voting), the anonymisation procedures, the reconstruction of the private key, and the decryption of the votes.

> output votes by other encrypted ones. To prevent this, the voting sVote system implemented a universal verifiable proof that shows that the Mixnet did not modify any content of the votes during the process."

[478] According to the Swiss expert group (2018: 10) [emphasis added],

> « [d]ans le souci de protéger le secret du vote, on fait en sorte que les suffrages ne se trouvent jamais sous une forme non cryptée et qu'ils ne puissent pas être décryptés entre le moment où le vote intervient et le décryptage des suffrages mélangés selon un procédé cryptographique. Pour dissiper la contradiction apparente entre la transparence et le maintien du secret du vote, il fait recourir à des procédés cryptographiques conçus spécialement pour le vote électronique. […] L'avancé des recherches permet aujourd'hui de concevoir des systèmes basés sur ces procédés. »

[479] More specifically, the introduction of verifiability was assessed by the Swiss Federal Chancellery (2011: 5) in the following terms [emphasis in the original]:

> « De par son caractère technique complexe, le [vote électronique] VE souffre de l'image de black-box : contrairement au vote à l'urne ou au vote par correspondance, seul quelques spécialistes sont capables de comprendre le fonctionnement de ce nouveau canal. Ceci provoque une méfiance certaine. Plus de transparence, en particulier plus de vérifiabilité des résultats du VE devraient combler ce décalage de confiance par rapport aux canaux conventionnels et contribuer à l'augmentation de l'acceptation du VE. La vérifiabilité constitue en même temps la fin et le moyen. D'après les connaissances actuelles, la vérifiabilité est *le moyen le plus simple et le moins cher* de vérifier les résultats du VE et de prouver aux intéressés (citoyens, commissions électorales, politiciens, etc.) que *les résultats du VE sont corrects.* »

[480] According to the Swiss Federal Chancellery (2020c: 4), complete verifiability is understood as:

> « La vérifiabilité complète garantit que les disfonctionnements systématiques dans tout le processus de vote ou d'élection à la suite d'erreurs logicielles, d'erreurs humaines ou de tentatives de manipulation seront identifiés grâce à des moyens indépendants. Dans le souci de protéger le secret du vote, ont fait en sorte que les suffrages ne se trouvent jamais sous une forme non chiffrée et qu'ils ne puissent pas être décryptés entre le moment où le vote intervient et le déchiffrement des suffrages mélangés selon un procédés cryptographiques. Pour dissiper la contradiction apparente entre la transparence et le maintien du secret du vote, il fait recourir à des procédés cryptographiques conçus spécialement pour le vote électronique. »

In the Estonian case, individual and universal verifiability are also understood as complementary, trying to address different issues. For example, Mihkel Solvak argues that (2016: 128)

> "[o]ne ingredient for such trust is ensuring vote verifiability at the institutional level, but another is at the level of the individual voter. The former is needed to guarantee the integrity of the election process and to keep different actors from challenging the outcome, the latter is needed to encourage people to cast their vote online in the first place. Individual verifiability should in theory therefore ensure that the otherwise unobservable virtual voting process happened as intended. Though it does not resolve the non-observability problem, at the very least it should mitigate it somewhat by giving added insurance that due process occurred and we should see increased trust levels among users as a result."

More specifically, the verification of the anonymisation procedures is based on mathematical proofs known as Zero-Knowledge proofs[481]. Zero-Knowledge proofs allow third parties to verify that no manipulation has taken place without disclosing any information that could compromise secret suffrage. By means of such verification it is possible to ascertain that the results of the election are genuine by comparing the shuffled, unshuffled, and the decrypted votes, together with the cryptographic proofs (Swiss Federal Chancellery, 2018c: 14). Therefore, and in contrast to the assumption that free and universal suffrage are contradictory, universally verifiability ensures the integrity and transparency of the results while preserving secret suffrage (since the votes are encrypted and the key is shared between different parties).

Likewise, the Estonian system offers the option of verifiable mix-net. According to the State Electoral Office of Estonia (2017: 18):

> "Mixing consists of random shuffling and cryptographic reencryption of votes. A precondition for using the latter technique is the use of a homomorphic cryptosystem in the encrypting of votes. Mixing must be carried out so that the decryption of both the input and the output would give the same result. As a side-result of the process, a mix-proof is issued which can be used, with the help of the Audit Application, to prove the correctness of the process."

In the latest elections observed by the OSCE/ODIHR, it was reported that "[a] team of external auditors was dispatched to assist the SEO with establishing vote secrecy during the computation of preliminary Internet voting results and the integrity of final Internet voting results by verifying the correctness of the cryptographic shuffle and decryption proofs" [emphasis added] (2019b: 9). Therefore, universal verifiability contributes to the observation of secret suffrage, and does not compromise it.

In addition to universal verifiability, the traceability of operations is also paramount. As we have seen, auditors and observers need different evidence to ascertain that election results are genuine: unshuffled and shuffled votes, decrypted votes, and proofs are some examples. The audit of this evidence is known as forensics. During the Swiss Expert Dialogue, "[h]alf of the experts mention[ed] the need to have a system designed for digital forensics, notably tools and immutable logs […] The tools should be available to efficiently identify, authenticate, classify, analyze, integrate, interpret and evaluate digital traces" (Swiss Federal Chancellery, 2020b: 66). In their opinion, "[f]orensic readiness requires trustworthy traceability […] and detailed logs in order to investigate unusual or suspected events" (Swiss Federal Chancellery, 2020b: 66).

In contrast to our previous conclusion, auditing the logs and evidence generated by a remote electronic voting system could indeed compromise secret suffrage, or at least some of their dimensions. For example, if the logs register who has voted, the confidentiality about who has voted could be breached. According to the experts in the Swiss dialogue, "[a] system designed for digital forensics might present a trade-off with respect to its

[481] The genesis of zero-knowledge proofs is described by Steven Levy (2001: 165-166) as follows:

> "In 1986, Shamir and two of his colleagues at the Weizmann Institute came up with another innovative and potentially valuable technology, known as 'zero-knowledge proofs of identity.' Using one-way functions, these allowed Alice to verify that she knew a number (typically something that identified here, like a social security or credit-card number) without revealing that number to the interrogator."

privacy guarantees" (Swiss Federal Chancellery, 2020b: 67). Therefore, the experts also concluded that "it is critically important that none of the tools allowing to expose secrets are installed or running on the trust-critical components of the voting system. They always have to be a part of a voting system whose operations are unobservable so that vote secrecy and verifiability can be maintained" (Swiss Federal Chancellery, 2020b: 71).

A similar issue is raised regarding the proposal to set up the so-called Public Bulletin Boards for remote electronic voting systems. In principle, the verifications for universal verifiability and traceability are limited and can only be conducted by specific appointed auditors and observers (who, in turn, need to have specialised knowledge about cryptography and ICT). For this reason, some have suggested the adoption of Public Bulletin Boards who would allow everyone to ascertain the integrity of the election results. However, during the Swiss Expert Dialogue half of the experts who addressed this issue considered that when discussing the added value of a Public Bulletin Board "long-term privacy risks need to be addressed" (Swiss Federal Chancellery, 2020b: 25). The same would happen if the forensic system is based on a blockchain[482], a technology that some experts in the dialogue suggested using[483].

As we have seen in section I.1.b) above, even if the data logged by the Bulletin Board and the blockchain is encrypted, it could become vulnerable against attacks by quantum computers in the long term (and may be even vulnerable to advances in computation that may allow for quick prime number factorisation). In this regard, it was noted that (Swiss Federal Chancellery, 2020b: 30):

> "Some Public Board designs publish encryption of votes. Here, secrecy of votes relies on the same set of assumptions which guarantee secret communication over the internet. Yet, these assumptions may be invalidated, and votes may be decrypted if quantum computers become a reality. If the board contains voter identifying information (e.g., required for auditing purposes) then the link between voters and their vote may be revealed. These designs may potentially be strengthened by using encryption schemes which are secure even against quantum computers – such schemes are under development by the cryptographic community. Other designs may hide the link between voters and their encrypted ballots so even if ballots get decrypted individual choices stay

[482] As we have explained elsewhere (Rodríguez-Pérez, 2021)

> "Blockchain is the underlying technology used by Bitcoin and other cryptocurrencies. It is used as a public ledger, or record of activity, of all the economic transactions involving the currency. The ledger is not centralized (stored in a single location), which prevents it from being altered by a single authority.
>
> [..]
>
> In a public or "permissionless" blockchain, the different users transfer amounts of the cryptocurrency and miners validate and register them in the ledger. Each of these transactions contains a reference to one or more former transactions — the inputs — and the amount transferred and who received it — the output. The input proves that the user making the transfer has enough cryptocurrency to afford it, and the output verifies the quantity of the transfer and its receivers."

In a previous study, we found that one of the concerns with the use of blockchains in remote electronic voting is precisely that the data registered in the blockchain cannot be protected against future attacks by quantum computers (Cucurull et al., 2019). Since this data cannot be modified (public ledgers are tamper-resistant given their distributed nature), it is not possible to encrypt the data again using quantum-resistant cryptography in the future. However, public ledgers may be still useful for audit purposes if no sensitive data is logged in the blockchain itself, as it has been suggested by Jordi Puiggalí and Jordi Cucurull (2016).

[483] For example, some experts suggested that "[t]he logs could be secured by a blockchain technology or other crypto methods like Merkle trees […] (e.g. ledger-based traceability using blockchain technology)" (Swiss Federal Chancellery, 2020b: 66).

> secret. Finally, other designs aim to achieve "everlasting privacy". Instead of publishing encryptions of votes, such schemes publish only a so-called "perfectly hiding commitment", which registers the vote on the bulletin board, analogous to a hash of the encrypted vote, but which probably contains no information about the vote's content that could ever be decrypted or revealed no matter how powerful the attacker is. Of course, the overall guarantees for vote privacy still rely on the security of the resto of the building blocks"

Interestingly, trust is seen here as an enabler of both transparency and secret suffrage, and not as opposite goals that trade each other off (Swiss Federal Chancellery, 2020b: 30):

> "[i]f a Public Board raises doubts about this guarantee [i.e., secret suffrage], then it undermines not only trust in the Public Board but also in the internet voting channel and voting as a whole. The use of a Public Board raises some concerns regarding vote privacy. Depending on the cryptographic techniques used, advances in cryptanalysis, or due to bugs, the information on the board may reveal how a voter voted. We can only speculate on the potential motivations for future attackers to attempt decryption of deanonymization of past votes, and what harms such attacks could lead to, such as voter embarrassment or coercion. Nevertheless, it is important to understand the risks and trade-offs associated to using a Public Board, and different designs thereof."

To sum up, this section has shown that it must be necessary to (re)balance some of the electoral principles in remote electronic voting, specifically when verifiable remote electronic voting systems are used. The key aspect here is not so much about the specific balance drawn between the different principles (i.e., free and secret suffrage), but rather on how this balancing has been reached[484]. The Explanatory Memorandum to the Recommendation already notes that (Council of Europe, 2017b: para. 18)

> "[t]hese decisions [on exceptions and restrictions to the principles and conditions for implementing them, or on their stricter or looser application] are taken by the competent national authority (the Parliament, the supreme judge, the electoral management body or a governmental agency) and depend on the country's specific context. It is important that such decisions are taken in conformity with basic requirements such as being taken by the competent authority, having a basis in law, being of general interest, respecting proportionality, among others. The overall aim of democratic elections and referendums must be respected."

Therefore, it is important that legal frameworks for remote electronic voting draw the proper balance between principles. This balancing should result from the decisions made by election administrations, in spite of the final decision being left for technical implementations. Nevertheless, calls for a trade-off between may be in fact hasty. At best, they are trade-offs that apply to any voting channel (i.e., to postal voting where there is no traceability, or to voting in polling stations where the traceability is based on the observation of the procedures, which fall short of reaching the levels of verifiability achieved by end-to-end verifiable remote electronic voting).

[484] In line with Lawrence Lessig, we can argue that our "aim is not to make that choice [between two very different conceptions of the value at stake], but instead simple to throw at least two options into relief" (2006: 155). In our case, those options are the ones reached by each of the three national experiences.

Again, we are of the opinion that drawing analogies with paper-based voting channels to assess complying with electoral principles is short-sighted. Our argument is that such compliance should be assessed against the specific risks and challenges that are specific to each voting channel. Likewise, it is possible to argue that there are specific ways in which the actual observation of voting procedures ensures the standards of secret suffrage. In the case of remote electronic voting, public procedures and audits contribute to the observation and supervision of secret suffrage.

3. Publicly voting in secret: false dichotomies and the public nature of secret suffrage

As a matter of fact, a more accurate assessment of the principles of free and secret suffrage reveals that they go hand in hand. Not only when it comes to remote electronic voting, but in any voting channel. In truth, we have seen that the goal of secret suffrage is precisely to shield voters from pleasures they may experience to vote in a certain way, thus enabling free suffrage. Likewise, the gradual adoption of secret ballots showed that the measures themselves (pre-printed ballots, envelopes, voting booths, etc.) should be accompanied with mechanisms to observe that they were being properly used. For example, by ascertaining that the voter entered alone in the voting both to mark their choices individually and confidentially[485], or that the counting procedures prevented anyone from linking a vote cast to the person who has cast them by declaring invalid any ballot with distinctive marks (at least in some jurisdictions).

Along these lines, in the European code of conduct on secret balloting the Parliamentary Assembly of the Council of Europe stresses "that supervision of the secrecy must be as strict as possible" (PACE, 2007a: para. 10). Likewise (PACE, 2007a: para. 5),

> "[t]he Assembly draws attention to its own role in free and fair elections. The many election observation exercises it has conducted in Council of Europe member states have all enabled it to reassert its commitment to the process of democratic consultation and its desire to promote full compliance with the principles and rules governing democratic elections, including respect for secret voting"

But how it can be observed whether encryption preserves the confidentiality of the vote or whether the anonymisation procedures are dully followed by the electoral authorities? The second sub-question that we have introduced in chapter 4 (section I.2) based on Vinkel's analysis of the constitutionally of remote electronic voting "can be answered with a 'yes' only if sufficient measures are in place to check whether the IT solutions work properly. This leads to the requirement that auditing, verification and evaluation of the results be stipulated in law and electoral regulations" (Vinkel, 2016: 41). In this regard, the authors notes that "compliance of the Estonian e-voting system with the ICCPR (1976) has given positive results as well, but also emphasized the importance of special procedures to facilitate auditing and observation of e-voting" (Vinkel, 2016: 42).

This evidences the need to observe secret suffrage, also in remote electronic voting. This observation is something different to the verifiability that we have discussed above,

[485] Such procedures may exist even in the case of postal voting. For example, the Parliamentary Assembly of the Council of Europe reports about the witnesses of secrecy of the vote in Sweden, who "sign either the outer envelope in which a postal vote is mailed or a statement attesting that the vote was both individual and secret " (PACE, 2007b: 6).

since it is also broader. It is important to note how the Swiss experience shows that verifiability and transparency are to be seen as two different principles[486]. In this sense, the Swiss expert group on electronic voting defined both verifiability and transparency as follows (2018: 38):

- Verifiability and traceability: the correct conduct of electronic voting and the accuracy of the results are checked by means that are independent from the system. This can include the complete verifiability mechanisms (individual and universal), that have been discussed in section II.2. above).
- Transparency: the operation of electronic voting systems and the main processes should be documented so that everyone can easily learn about them. Therefore, transparency is broader than verifiability and traceability, since it must include as well how citizens understand secret suffrage (individuality, confidentiality, anonymity) as well as end-to-end verifiability.

Nevertheless, the question of how to observe these processes remain unanswered. In this last section of the PhD, we assess two different approaches towards observing secret suffrage in remote electronic voting. First, procedures and ceremonies to ascertain that certain steps, such as the anonymisation of the vote, are dully followed. Second, the audit and certification of remote electronic voting systems, which more recently have scaled to include the publication of the source code and the conduct of public intrusion tests. As we will argue, these two processes should not be seen as alternatives, but need to complement each other in order to ensure that secret suffrage is observed in remote electronic voting.

a) Procedures, ceremonies, and verifiers: observing compliance with secret suffrage

The first solution to the observation of secret suffrage is drawn (unsurprisingly) from analogies to paper-based voting channels. If compliance with secret suffrage in paper-based voting channels is based on the actual observation by third parties of the key procedures (voter identification, ballot marking and casting, reconciliation, counting, etc.), why not replicate this procedure for remote electronic voting as well?

In Switzerland, for example, the election commissions set up with the cantons were entrusted with these functions. These commissions and committees were setup by analogy to paper-based voting polling committees[487]. For the Swiss Federal Council[488], the solution

[486] See, for instance, how the Swiss expert group on electronic voting referred to verifiability (meaning traceability and secret suffrage), accessibility and transparency towards the public as the three main characteristics of electronic voting (Swiss expert group, 2018: 14).

[487] According to the Swiss Federal Council (2006: 5258),

> « [d]ans le cadre du vote traditionnel, le contrôle démocratique est opéré par les commissions électorales et par les scrutateurs issus des rangs des électeurs. Dans le cadre du vote électronique, ces acteurs doivent être remplacés de façon appropriée, durant la phase de vote, par des procédures faisant l'objet d'une surveillance. Les cantons pilotes de Genève et de Neuchâtel ont donc constitué à cette fin des commissions spéciales composées de représentants des partis politiques et/ou des groupes représentés au parlement cantonal. Ces commissions participent à l'ouverture de l'urne électronique et au dépouillement des suffrages électroniques. Dans le canton de Zurich, des commissions de ce type sont constituées dans chaque commune. »

[488] According to the Swiss Federal Council (2006: 5260),

to the problem of observation of supervision could be solved with the setup of these commissions where political parties were represented and who kept the secrets necessary for the decryption of the votes (2006: 5260). At the end of the day, the same issues had been raised with the generalization of postal voting and this solution could be applied to both remote voting channels[489] (Swiss Federal Chancellery, 2004: 34).

During the extended pilot phase, several cantons adopted this system. By 2012, "[i]n at least two cantons, Central Election Commissions have been established. In Geneva, the CEC's role is to monitor electoral operations, while in Zurich the cantonal statistics office is designated as a CEC and assumes responsibility for the organization of the election." (OSCE/ODIHR, 2012a: 8). The cantons whose systems were hosted by Geneva could appoint representatives to this commission for the decryption of their ballot box[490] (Swiss Federal Council, 2013a: 42). Neuchâtel had also set up a central electoral commission[491] (Swiss Federal Council, 2013a: 85), but Neuchâtel did not offer remote electronic voting during the 2011 federal elections and therefore the OSCE/ODIHR could not observe their work. In contrast, Saint-Gallen set up different bodies depending on the process: a cantonal polling station committee for the federal elections, and a commission for Swiss voters abroad for federal and cantonal votes[492] (Swiss Federal Council, 2013a: 42). As we have seen, nowadays the federal legal framework prescribes both the role of these

> « [l]a solution du problème [de traçabilité et preuve] passe impérativement par une procédure qui satisfasse à l'exigence d'une traçabilité individuelle par un contrôle démocratique de la procédure de vote. Les cantons pilots recourent à des commissions électorales composées de représentants des partis politiques, qui suivent le déroulement du scrutin électronique et qui génèrent et conservent les mots de passe nécessaires aux opérations de cryptage et de décryptage. »

In addition to the committees, the cantons also set up fiction communes. « Cette commune-test est traitée par le système comme une commune politique à part entière du canton. Les suffrages exprimés dans la commune-test subissent le même processus que tous les suffrages électroniques, c'est-à-dire le processus allant de la remise jusqu'au décryptage » (Swiss Federal Council, 2005 : 5258).

[489] According to the Swiss Federal Chancellery (2004: 34),

> « [l]a loi genevoise permet aux citoyens d'assister à l'ouverture des urnes dans les bureaux de vote. Pour le vote postal, cette possibilité a été transposée sur des contrôleurs désignés par les partis en nommés par le gouvernement. La même approche a été retenue pour le vote en ligne. »

[490] According to the Swiss Federal Council (2013a: 42),

> « [d]ans le canton de Genève, la loi cantonale d'exécution des droits politiques définit la forme de la commission électorale centrale (CEC). Elle est notamment chargée du contrôle des procédures et de la documentation du système, du cryptage et du décryptage de l'urne et de la supervision des procédures ; elle a par ailleurs la possibilité de demander des audits. Ses rapports sont publiés. En outre, et afin de contrôler le vote électronique, la commission, composée de représentants de tous les partis actifs au Grand Conseil et d'experts, a créé une sous-commission technique. Les cantons hébergés par Genève peuvent faire intervenir leurs propres représentants lors du cryptage et du décryptage de l'urne électronique. Ils ont délégué le contrôle général du vote électronique à la CEC genevoise. »

[491] According to the Swiss Federal Council (2013a: 42),

> « [l]a commission électorale telle qu'elle existe dans deux cantons (Neuchâtel et Genève) a été identifiée comme un pratique exemplaire par la Confédération et les cantons dans la feuille de route de même que par les observateurs de l'OSCE dans leur rapport de janvier 2012. Il s'agit d'une instance de supervision des opérations qui détient une partie des clés du système, a accès à la documentation sur le système et dispose de pouvoirs de contrôle étendus dans un canton. La commission électorale permet une observation significative du vote par Internet. »

[492] According to the Swiss Federal Council (2013a: 42),

> « [d]ans le canton de Saint-Gall, on met en place un bureau de vote cantonal pour les élections du Conseil national et du Grand Conseil. Pour chaque votation et élection fédérale, on met en place une commission pour le vote des Suisses de l'étranger, qui se compose d'au moins cinq membres désignés par le gouvernement, chaque groupe parlementaire représenté au Grand Conseil fournissant un membre. »

bodies[493], together with the use of advance mathematical methods to ascertain that the results are genuine[494] (Swiss Federal Council, 2013a: 42).

The question revolved around the degree of openness of these commissions. For example, following the 2011 elections the OSCE/ODIHR recommended that "[e]ssential procedures, such as the decryption of internet votes, could also take place at public meetings" (2012: 18). In the opinion of the observers, "[o]verall, there did not appear to be a meaningful possibility for the general public to observe or oversee internet voting procedures" (OSCE/ODIHR, 2012a: 20). By contrast, the Swiss Federal Council noticed that these commissions had foreseen the participation of political representatives, although each one was regulated in a different way[495] (Swiss Federal Council, 2013a: 31). For example, in Neuchâtel the participants are technical specialists and the operations are carried out by the system administrators in the presence of the electoral commission (Swiss Federal Council, 2013a: 85).

By 2015, and "[d]espite a previous OSCE/ODIHR recommendation, the creation of electronic 'keys' to protect encrypted data was [still] not performed in public" (OSCE/ODIHR, 2016: 9). For example, the OSCE/ODIHR warned that "[t]he Geneva and Neuchâtel election commissions were present during the process. In Geneva[496], it was not possible for the general public to attend the meeting on the grounds that election commission represent the public" (2016: 9). More recently, the Swiss expert noticed that federal law does not specify who is responsible for verifying that the results have been established correctly[497] (2018: 20). In contrast, it only determines the type of verification

[493] In the Appendix to VEleS, the following requirements deal with the role of the electoral boards (Swiss Federal Chancellery, 2018d: 9):

> "2.7.1. After the electronic vote casting system is closed, the Cantonal Voting Officer activates the decryption of the votes held in the electronic ballot box, at the earliest on Polling Sunday.
>
> 2.7.3. The Cantonal Voting Officer records the decryption process and tallying in writing.
>
> […]
>
> 2.7.7. The decryption and the tallying of the votes are carried out in the presence of independent bodies or parties. As a result, they can confirm that the procedure has been duly carried out."

[494] According to the Swiss Federal Council (2013a: 42),

> « [l]e droit fédéral prescrit l'utilisation de méthodes mathématiques modernes, garantissant à la fois le secret et la traçabilité du vote, qui doivent permettre de vérifier le processus de vote du début à la fin. Si toutes les vérifications aboutissent à un résultat correct, il est possible d'affirmer que le scrutin n'a pas été manipulé. Il peut par exemple être établi que tous les votes exprimés ont correctement été pris en compte lors du dépouillement. Cette double exigence de traçabilité et de secret du vote est un élément essentiel du vote électronique en Suisse. »

[495] The Ordinance on Political Rights only foresees the participation of representatives during the counting of remote electronic voting. As a result, « [l]es réglementations cantonales traitent quant à elles cette question de différentes façons : la plupart des cantons proposant le vote électronique ne l'ont pas réglée expressément. D'autres ont étendu les compétences du bureau de vote au canal électronique. » (Swiss Federal Council, 2013a: 31).

[496] Additionally, the OSCE/ODIHR also mentions that "[t]he Geneva election commission decrypted the votes of the Geneva, Luzern and Basel-Stadt elections. Representatives from Luzern and Basel-Stadt election commissions observed this process via a live webcam. External observers would have been permitted if present in Geneva and Neuchâtel and all procedures could be followed on a large screen in the room." (OSCE/ODIHR, 2016: 9)

[497] In the opinion of the Swiss expert group (2018: 20),

> « [l]e droit fédéral dispose que des « vérificateurs » seront chargés d'examiner les preuves qui attestent que les résultats ont été établis correctement. Il n'est pas précisé quelles personnes seront amenées à jouer ce rôle. Les électeurs doivent pouvoir supposer qu'en cas de doute, les vérificateurs signaleraient les éventuelles anomalies Leur crédibilité est essentielle. Les cantons et les fournisseurs des systèmes seront appelés à définir les processus de vérification de telle façon que les « vérificateurs » puissent établir avec certitude si le scrutin s'est déroulé correctement. »

that should be possible. In the opinion of the group Swiss Federal Chancellery, the decision on who is responsible is left to the cantons, so they can come up with mechanisms aligned with their specific political and societal circumstances[498] (Swiss Federal Chancellery, 2018c: 14).

In France, the Electoral Code specifies the procedures of the *bureau de vote électronique* with great level of detail. More specifically, the Electoral Code specifies that it must meet (at least) on three occasions, and describes the steps that it should follow each time. Before the start of the voting period, article R176-3-8 prescribes the meeting of the *bureau* for the ceremony in which the key is created and split between the different members. In this occasion, the *bureau* is also entrusted with certifying that no voter has been marked as having cast a ballot and that the ballot box is empty (article R176-3-8). The *bureau* must meet as well when the voting period ends, on Wednesday before election day. In this occasion, the *bureau* monitors how the system administrators extract and record the contents of the ballot box, the *listes d'émargement* and the system logs, and store them in "sealed supports" (art. R176-3-10). The *bureau* has to ascertain that the number of votes stored in the ballot box correspond to the number of voters in the electoral roll and its President is entrusted with keeping the supports. On election day, the *bureau* meets to reconstruct the key and launch the anonymisation and decryption of the votes (art. R177-5).

The procedure actually dates back to the first experiences with remote electronic voting, and we can see that they are quite similar to the typical procedures in a polling station (even if they are carried out in three different days). Andrew W. Appel (2006: 2) has offered a rather cartoonish description of one of the first events:

> "The election is conducted on machines built by EADS and operated by Experian in a room in Aix-en-Provence, and monitored remotely by the *assesseurs* in a room in Paris. From Paris, the *assesseurs* see a video image, purportedly from a camera in Aix, showing an *urne* – but not a physical *urne*, but a room full of computers. They see also a web browser in Paris purporting to show data from the computers in Aix: the number of votes already in the virtual *urne* database, the number of voters who are registered, the number of votes who have already voted."

But how can the *bureau* ascertain that the "ballot box" is actually empty[499]? Or that all the voters marked in the *émargement list* have actually cast their vote? In the opinion of François Pellegrini, however, there is no reason to trust that the election result actually displayed on the screen at the time of the digital count correspond to votes that the voters

[498] According to the Swiss Federal Chancellery (2018c: 14),

> « [l]e droit fédéral ne précise pas qui doit vérifier que les résultats ont été établis correctement. La réponse est laissée aux cantons. Ils peuvent ainsi tenir compte de leurs spécificités politiques et sociétales. Le droit fédéral détermine le type de contrôle qui doit être possible. L'attribution de la compétence de vérifier les résultats relève de l'autonomie des cantons en matière d'organisation. Les contrôles peuvent être confiés par exemple à une commission électorale ou à des observateurs. »

[499] For this author, « [l]es membres du bureau de vote par voie électronique constatent que l' « urne électronique » est vide et déclarent alors le vote ouvert. Il importe de bien préciser que vous constatez que l'écran de contrôle mis à votre disposition indique que l'urne électronique est vide, et de ne surtout pas affirmer qu'elle est effectivement vide » (Pellegrini, 2006 : 9).

(wanted to) cast[500] (2006: 9). For this author, it is necessary to trust the technological intermediaries who have developed the software, installed, and deployed it (Pellegrini, 2006: 9). As also described by Andrew A. Apple (2006: 9).

> "when the *assesseurs* of the *Election des Conseillers à l'Assemblé des Français de l'Étranger* see a computer screen in Paris saying "0 votes in the ballot-box", they are not seeing a ballot box. They are seeing a representation, in Paris, that purports to be a communication form a Supervision machine in Aix, that purports in turn to be connected to an *Urne* machine in Aix, that purports in turn to be running a certain software. The *assesseurs* do not even see a representation or image of that software, since it is held as a trade secret"

For this author, "examining the computer program would be useful in assuring that it accurately interprets de vote" (Apple, 2006: 9).

Procedures in Estonia are based on similar procedures. As it has been reported by Priit Vinkel (2016: 53),

> "[a]ccording to Estonian electoral law, all procedures related to elections are public. Observers have access to the meetings of all elections committees and can follow all electoral activities, including the voting procedures, counting and tallying of results. Internet voting has been no different. All significant documents describing the e-voting system have been made available to the public […], including observers. In order to enhance the observers' knowledge of the system they are invited to take part in a training course before each election. Besides the political parties, auditors and other persons interested in the e-voting system can take part in the training. Observers are also invited to participate in test elections during the set-up phase."

Nevertheless, the OSCE/ODIHR's NAM deployed ahead of the 2007 *Riigikogu* elections noted that, during the 2005 local government council elections "there appeared to be almost no oversight of the internet voting process by political parties or civil society" (OSCE/ODIHR, 2007b: 2). On the other hand (OSCE/ODIHR, 2007b: 14).,

> "[f]or the 4 March [2007] parliamentary elections, counting was conducted in the Parliament building by NEC operators in presence of the NEC, auditors, press, and domestic and foreign observers. After the votes were decrypted and counted, the auditor announced that everything had been done in accordance with the procedure. While the OSCE/ODIHR EAN was present for the counting process, it was – as with any electronic counting – not possible to observe the actual counting of the votes, since this took place within the Counting Server."

During the process, "[t]he installed voting software was checked to ensure that it was identical to the software received by comparing the checksum on the version installed on the servers with the checksum provided by Cybernetica AS" (OSCE/ODIHR, 2007b: 16).

[500] According to M. Pellegrini (2006: 9),

> « [r]ien ne peut permettre aux assesseurs de penser, ni tout autant de penser le contraire d'ailleurs, que l'image qu'ils ont vue en permanence est celle de la salle informatique d'Aix, et qu'elle reproduisait fidèlement ce qu'il s'y passait. Il est tout à fait possible qu'ait été inséré, dans la chaîne de transmission, un dispositif de mémoire d'images permettant à certains moments de rediffuser des images déjà acquises pendant que des manipulations physiques avaient lieu dans la salle informatique. De même, rien ne permet de penser, ni là encore de penser le contraire, que le résultat de l'élection qui sera effectivement affiché sur l'écran au moment du dépouillement numérique correspondra bien à la réalité des suffrages que voulaient exprimer les électeurs devant leurs ordinateurs. »

The event was also open. In this regard, "all political parties and accredited observers were invited to observe the administration of internet voting in every phase of the process. This included the opportunity to review the documentation of the system, the source code of the software, and all of the setup procedures in the process" (OSCE/ODIHR, 2007b: 19). Notwithstanding, the OSCE/ODIHR's mission also noticed that "no political parties exercised their right to have access to the process and to observe the setup procedures, nor did NGOs or civic associations attempt to observe the process in a comprehensive manner" (2007b: 19). Similar procedures were reported for the 2011[501] and 2015[502] elections. Furthermore, the author had the opportunity to attend the decryption and counting ceremony for the 2019 *Riigikogu* elections.

Overall, Mihkel Solvak and Kristjan Vassil explain how "Estonia decided to create a separate administrative level institution, the E-voting committee, to operate the e-voting system. This ensured clear responsibility and created an actor inherently tasked with safeguarding and developing the system" (2016: 164). Interestingly, it was the constitutional debate – that mainly focused secret suffrage and Internet voting – that provided input into the procedures that needed to surround remote electronic voting (Solvak and Vassil, 2016: 164).

b) (Public) testing and auditing remote electronic voting technology

Once again, drawing analogies to paper-based elections when it comes to supervising secret suffrage has its shortcomings. Commissions and ceremonies may well demonstrate that the operators of the remote electronic voting system conduct their operations as expected. However, it is still not clear whether secret suffrage is complied with: are vote encrypted end-to-end? Is the encryption algorithm used strong enough? Are the decrypted votes properly anonymised?

It is important to remember that the only thing that encryption do is to scramble the data (Martin, 2020: 158). However, "encryption does not come with a guarantee that the encryption algorithm used has been correctly coded or integrated into the technology it is trying to protect" (Martin, 2020: 158). Therefore, it is not only important to come up with a sound cryptographic algorithm, but implementation also matters. According to Bruce Schneier (1997), there is a chasm between design and implementation:

> "Just because a protocol is logically secure doesn't mean it will stay secure when a designer starts defining message structures and passing bits around. Close isn't close enough; these systems must be implemented exactly, perfectly, or they will fail"

Keith Martin (2020: 245-246) reminds us that:

[501] According to the OSCE/ODIHR (2011b: 10)

> "The Internet voting system was set up at the premises of the NEC between 15 and 18 February. On the last day, the cryptographic keys used for encrypting and decrypting the votes were generated and handed over to members of the NEC. This stage also included an end-to-end test of the casting and counting of a small number of test votes. The NEC, observers and representatives of political parties were in attendance to check that the system was configured correctly."

[502] In this occasion, the OSCE/ODIHR further adds that "[a]ccording to the NEC, to further transparency of the process, video recordings of EVC meetings and all procedures related to internet voting will be available online. In addition, while observers or party/candidate agents are permitted to observe all stages of Internet voting, the NEC requires they attend its week-long training session on Internet voting."

> "the design processes of cryptographic algorithms cannot always be trusted. Nor can the implementation of cryptography on the technologies we use today, or the ways un which keys are managed. If there is no belief in the reliability of cryptography, what hope it there of establishing meaningful trust in cyberspace?
>
> Establishing trust in cryptography is challenging. A significant barrier is the sheer complexity of what we need to trust in order to trust cryptography. It's not just about algorithms; it's necessary to trust the entire system in which cryptography is used, including the manufacturers of the technologies and the operators of the networks on which cryptography is deployed. All this is made yet more complex by the fact different people trust and mistrust different sets of things."

The question here is whether naked-eye observation is meaningful at all. As Douglas Jones put it: "[w]here voters are hand counted, observers can see what is being done. When votes are tabulated using computers, all the observers can see is a box with some attached fans and blinking lights, and perhaps the back of the technician or programmer sitting at the keyboard typing unknown commands into the system" (2004: 7). It is possible not to have to trust the technological intermediaries who have developed the software, installed, and deployed it, as noted by François Pellegrini (2006: 9)?

When it comes to remote electronic voting, analysing the system itself becomes paramount, also for the supervision of secret suffrage[503]. In the Swiss case, for example, this guarantee is understood as the process of certification, meaning that the electronic voting system and their exploitation are being subject to an independent service (i.e., accredited certification). Nevertheless, it is possible to approach certification in different ways: by testing and auditing the systems, by analysing (and even opening to the public) the source code, and even by conducting public intrusion tests and *bug bounty* programmes.

From certification and audit…

According to the OSCE/ODIHR, "[t]esting is a crucial exercise to find any deficiencies in the system" (2011b: 10). In this regard, Priit Vinkel has noted that "[t]he first feature is validating the electronic voting system, with certification or verification procedures, and testing and auditing all considered" (Vinkel, 2016: 51). Therefore, some form of testing is envisaged in all the national experiences.

For example, regarding the Swiss case, the OSCE/ODIHR has acknowledged that "[i]n line with good practice, the law requires cantons to test all components of their system before every election. The canton of Geneva performs an additional end-to-end test of the casting and counting of a small number of votes prior to each use of the system[504]. For

[503] Additionally, it has been noted that (Gibson et al, 2016: 281):

> "[e]nd-to-end verifiable systems also typically use sophisticated cryptographic techniques for providing privacy (though this is not part of the definition of end-to end verifiability). Such protocols should guarantee that voters do not need to blindly trust any component of the system; all components can be scrutinised so that their computation can be verified if their trustworthiness is in doubt"

[504] In fact, testing in the canton of Geneva dates back to the first trials with remote electronic voting. Interestingly, independent auditors verified that anonymisation mechanisms had been properly

[the 2011 elections] the test too place on 15 September" (2012: 19). More specifically, they noted that (OSCE/ODIHR, 2012a: 19)

> "While the consortium system underwent comprehensive external review after its initial deployment in 2006 and again following an update in 2008, no external audits were performed after a 2010 update of the system. The canton of Geneva has undertaken four separate external security audits of its internet voting system in 2002, 2003, 2007 and 2010. The results of these audits, and the improvements the cantons have made to their systems as a result, have not been made public."

Moreover, they also warned that "[m]ost key documents and explanations were not readily available to the public" (OSCE/ODIHR, 2012a: 20).

In this regard, the Federal Ordinance on Political Rights "requires that internet voting systems, and any changes made to them, be certified by an independent body recognized by the Federal Chancellery" (OSCE/ODIHR, 2012a: 19). The requirements that such a body should met where specified with the adoption of VEleS and the update of the Federal Ordinance on Political Rights[505]. As we have explained elsewhere (Puiggalí and Rodríguez-Pérez, 2018: 90), the certification process in Switzerland has had four main objectives: (1) certify the cryptographic protocol verifiability's compliance; certify the software security and functionality; (3) certify the security of the infrastructure and its resilience against instructions; and (4) certify the requirements for printing offices.

Currently, art. 27*l*.2 of the Federal Ordinance on Political Rights prescribes that external auditors must (a) confirm that the security requirements set by the Federal Chancellery are met, and (b) check whether the security measures and the electronic voting system correspond to the latest technical developments[506]. Among others, it was noticed that a careful analysis of the cryptographic protocol and the source code of the systems was

implemented: « [t]ous les programmes traitant les votes doivent pouvoir être vérifiés par des experts externes à l'État de Genève et totalement indépendants du partenaire qui sera retenu. Ces experts doivent notamment pouvoir s'assurer que l'identité des votants ne soit pas enregistrée dans le fichier des votes » [emphasis added] (Swiss Federal Chancellery, 2004: 34). In fact, it was acknowledged that remote electronic voting was also under the transparency obligations imposed on public administrations. In this regard, the Swiss Federal Council (2013a: 29) stressed from the outset that:

> « Le vote électronique relève également de la loi du 17 décembre 2004 sur la transparence (LTrans). […] La LTrans et son ordonnance du 24 mai 2006 (OTrans) prévoient le principe d'accès aux documents de l'administration fédérale. Le principe du secret est abandonné au profit du principe de transparence. Compte tenu de l'importance capitale du projet pour la démocratie directe, on a vu fleurir ces dernières années les demandes d'accès aux documents traitant du vote électronique »

[505] Before that, the OSCE/ODIHR had criticised that (2012: 19)

> "no such body exists and the required certification has not taken place. Currently, cantons self-declare their adherence to the provisions of the election law and provide a description of their system. Although the Federal Chancellery informed the OSCE/ODIHR EAM that plans are underway to meet this requirement, the current lack of certification in [sic] not in line with federal law and may damage public trust in internet voting. A further concern is that even if an independent body were created, there are no clear, written technical standards or requirements on which to base certification."

[506] According to the Swiss Federal Council (2013a : 112),

> « [c]onformément à l'art. 27l.2 de l'ODP, un service externe indépendant, reconnu par la Chancellerie fédérale, doit confirmer que les systèmes satisfont aux exigences en matière de sécurité et de fonctionnement. Des audits – longs et couteux – dans ce sens ont été réalisés par le passé, mais il n'était pas possible d'y procéder à chaque modification d'un système. »

necessary also to ensure that they were guaranteeing secret suffrage[507] (Swiss Federal Council, 2013b: 2). These external auditors have taken two main shapes (Puiggalí and Rodríguez-Pérez, 2018: 87-88):

- *Groupes d'accompagnement*, which in practice have been made up by representatives from four different cantons using a different voting system; and
- Institutions accredited by the Swiss Accreditation Service (SAS) or certification agencies. "These specialized institutions (i.e., certification laboratories), should first pass an accreditation process through the Swiss Chancellery to get the seal of certification authorities of the VEleS regulation"[508] (Puiggalí and Rodríguez-Pérez, 2018: 88).

Following the legal update, the OSCE/ODIHR changed its assessment of the experience. For example, the EET that observed the 2015 elections concluded that "[i]ndependent certification is a key measure to promote accountability" (OSCE/ODIHR, 2016: 9). They also noted that certification is based on a detailed criteria provided in the Section 5 of the Annex to VEleS, "including aspects related to cryptography, functionality, security of the technical infrastructure and operations, protection against attempts to infiltrate the infrastructure, and requirements for offices for printing polling cards" (OSCE/ODIHR, 2016: 9). However, these findings were not public (2016: 6),

> "[t]he working group drafted reports providing suggestions for improvement to each Internet voting system, which included the two used in these elections as well as the Consortium system. The report was not made publicly available, at odds with international standards. The Neuchâtel system did not present any problems, and it was recommended to insert explanatory texts regarding the Internet voting and available functions. Following the review, Geneva undertook additional testing for its system beyond federal requirements"

In this regard, the EET noticed that "the audit criteria and findings for the Geneva system are publicly accessible, while auditing documents for the Neuchâtel system are not, contrary to international good practice" (OSCE/ODIHR, 2016: 2). More specifically (OSCE/ODIHR, 2016: 10),

[507] More specifically, the Swiss Federal Council (2013b: 2) concluded that [emphasis added]

> « [l]e protocole cryptographique décrit, au plan conceptuel, les communications (en partie cryptographiques) échangées entre les différents utilisateurs du système, par exemple entre les ordinateurs des électeurs, les serveurs du système de vote électronique, les composants de contrôle et l'imprimerie. L'analyse du protocole doit garantir […] que la vérifiabilité et le secret du vote sont donnés au plan conceptuel au sens des exigences. Cette vérification ne doit pas être effectuée par un service accrédité. En lieu de cela, la Chancellerie Fédérale prend connaissance des propositions des cantons et les évalue. Lorsqu'elle est d'accord avec l'organe proposé, le canton peut confier l'analyse à ce dernier. »

Interestingly, the Swiss Federal Council also concluded that both verifiability and secret suffrage were complementary and depended on the trust in the control components. In this regard (Swiss Federal Council, 2013b: 2) [emphasis added],

> « La vérifiabilité et le secret du vote dépendent de la fiabilité des composants de contrôle utilisés […] Leur fonctionnement correct est pour cette raison d'une importance cruciale. An audit doit garantir que les composants de contrôle envoient uniquement les messages décrits dans le protocole cryptographique et que les électeurs ou les vérificateurs […] puissent détecter toute utilisation illicite. »

[508] So far, only KPMG has been accredited as a VEleS certification authority (Puiggalí and Rodríguez-Pérez, 2018: 93). Interestingly, KPMG had to involve experts in the evaluation of security and symbolic proofs from ETH Zurich in the certification process of Swiss Post's remote electronic voting system at level 2 (Puiggalí and Rodríguez-Pérez, 2018: 93).

> "Auditing is also envisaged in the law. In Geneva, independent audits have been carried out in different parts of the system by independent agencies every three years, with the next expected in 2016. The OSCE/ODIHR EET was informed that the audit criteria and findings for this system are publicly accessible. While external audits have been conducted in Neuchâtel, it has mostly relied on procedures of the Federal Chancellery to conduct internal audits. The auditing documents for the Neuchâtel system, including findings, are not publicly available, contrary to international good practice[509]."

More recently, the certification procedures have been subject to a review. The Swiss expert group concluded that certification by external auditors should remain as a key requirement[510] (2018: 37). Along these lines, the Swiss Federal Chancellery also concluded that monitoring the compliance with the legal requirements should be entrusted to an external certification service[511] (Swiss Federal Chancellery, 2018c: 15) and that the certification of the systems should be valid only for a certain period of time[512] (Swiss Federal Chancellery, 2018c: 15).

In Estonia, "[i]ndependent IT auditing that covers all aspects of the system can prove its soundness" (Vinkel, 2016: 42) as well. According to Priit Vinkel, "[t]he proper performance of an IT system should be verified and audited before, during and after voting" (2016: 42) and "[s]ystem-testing prior to elections by contracted testers, auditors, observers and the public is also an important factor in order to control functionality and accuracy" (2016: 51). In this sense, "[t]he law also regulated that before every implementation, the e-voting system must be tested and audited" (Vinkel, 2016: 45). According to this author (Vinkel, 2016: 51),

> "the Estonian e-voting system was developed with the principle that all components of the system should be transparent for auditing purposes: procedures are fully documented, with critical procedures logged, audited, observed and videotaped (since 2013 also published on YouTube) as they are conducted. A separate procedural audit by Certified Information Systems (CISA) auditors is procured by the EMB for every election. The scope of the audits is to ensure the validity of performed procedures in terms of the guidelines contained in the handbooks and technical documentation of e-voting. Additionally, auditors review and monitor security sensitive aspects of the process, such

[509] It is the understanding of the OSCE/ODIHR that governments have a duty to publicly share any reports about the conduct of elections, in line with the international commitments of the States. In this regard, the conclusions of the United Nations Human Rights Committee are mentioned often: "[t]o give effect to the right of access to information, States parties should proactively put in the public domain Government information of public interest. States parties should make every effort to ensure easy, prompt, effective and practical access to such information" (2011: paragraph 19).

[510] According to the Swiss expert group (2018: 37),

> « [l]a certification du système de l'exploitation par un service externe à l'administration restera un des principaux moyens de garantir le respect des exigences techniques de sécurité. Le principe de la certification accréditée sera maintenu après la mise en exploitation. Conformément au droit en vigueur, le système et l'exploitation doivent être certifiés par un service accrédité par le SAS […]. Le protocole cryptographique […] doit aussi être contrôlé par un service indépendant. »

[511] According to the Swiss Federal Chancellery (2018c: 15),

> « [l]'autorisation d'utiliser le vote électronique présuppose que toutes les exigences du droit fédéral sont remplies. Contrôler que c'est effectivement le cas pour le système et les processus fonctionnels mis en œuvre ne doit pas incomber en premier lieu à l'administration fédérale. Ce contrôle détaillé bien plutôt être confié à un service de certification externe, accrédité par le Service d'accréditation suisse (SAS). Le transfert des tâches de contrôle à un service de certification externe accroît l'indépendance institutionnelle de la vérification et contribue ainsi à l'assurance de qualité. »

[512] According to the Swiss Federal Chancellery, « [l]es certificats ne sont valables que pour une durée limitée et doivent en règle générale être renouvelés tous les trois ans. Dans l'intervalle, le service de certification effectue en outre régulièrement des contrôles intermédiaires » (2018c: 15).

> as updated the voter list, preparation of hardware and its installation, loading of election data, maintenance of renewed election data, and the process of counting the votes."

Testing also dates back to early on in the introduction of Internet voting, although there were no specific requirements on certification. In this regard, Sutton Meagher reports that (2009: 378-379),

> "Before Estonia held its 2005 election, the NEC tested the electoral system, and an independent outside expert reviewed the source code. Although this was not an entirely open process, it still provided a level of security to ensure that the software was going to work properly. Before the March 2007 election, the Estonian government hired an outside consulting company to audit Estonia's voting technology and the auditors found no problems."

On the other hand, however, the OSCE/ODIHR warned that "[t]he [internet voting] system was tested prior to the local elections by the NEC, but there has been no subsequent separate testing. There is no provision for certification of the system[513]" (OSCE/ODIHR, 2007a: 6). In also concluded that "the National Election Committee made considerable efforts to minimize the inherent risks, testing and auditing of the system could have been more comprehensive" (OSCE/ODIHR, 2007b: 2). The situation remained in 2011. According to the OSCE/ODIHR's NAM, "[t]here are currently no provisions for the formal certification of the system by an independent external organization. The NEC, however, plans to conduct three rounds of testing: one by the software developers, a second by the NEC itself and a third one by a group of hackers specially hired by the NEC" (2011a: 6).

The mission that observed the elections conduced that (OSCE/ODIHR, 2011b: 10):

> "Similar to previous elections, the NEC conducted extensive testing of the Internet voting system before setting it up. Firstly, the Internet voting project manager tested the software delivered by the vendor. This was, however, carried out without formal reporting. After that, the Cyber Defence League (CDL) conducted an exercise in January 2011 to test the software under given threat scenarios, and produced a report for the NEC that was made available to observers but not to the public. In February, the CDL tested the functionality of the Internet infrastructure under extreme conditions and decided to create a "whitelist" that contained Internet addresses from where legitimate voters could be expected (including embassies abroad)"

However, and as in the Swiss case, the findings of the testing were not widely shared. For example, the OSCE/ODIHR mission noticed that "a programmer, who was contracted by the NEC, verified the software code. The identity of the programmer and his [sic] report to the NEC was kept secret" (OSCE/ODIHR, 2011b: 10). In this regard, they concluded that "[t]he NEC made a substantial effort to test various components of the Internet voting, including by members of the public. However, reporting on the performed tests was often informal and kept secret" (OSCE/ODIHR, 2011b: 10). In a similar way, for the 2015 elections, it was stressed that "[t]he comprehensive testing of software and hardware before the arrival of the OSCE/ODIHR EET was not conducted in the presence of election

[513] As noted by the OSCE/ODIHR's EAM, "[t]he *Riigikogu* Elections Act does not provide specifications or minimum prerequisites of the internet voting system, nor the obligation to certify or test the system" (2007b: 14). The EAM was of the opinion that "[t]he internet voting system was not officially certified by an independent body. The NEC stated that it had organized informal review of the software by representatives from banks, universities, state officials and ICT specialists at various times. The results of these reviews were not made public" (OSCE/ODIHR, 2007b: 15).

observers or auditors. No detailed formal procedures were prescribed for software development and testing" (OSCE/ODIHR, 2015b: 5).

In France, the updates Recommendation by the CNIL also prescribes that in case of external audit, it should be possible to prove, among others, that the keys for encryption and decryption are only known to those that should guard them and that the votes are anonymous (2019a: 5).

… to the publication of the source code

Possibly with a view to overcome the limitations identified by the OSCE/ODIHR in terms of publicly sharing the findings of audit and certification reports, governments took a step further and started to open their procedures. Nowadays, it is possible to argue that "[i]t is a common requirement that the source code of an information system is available for public audit" (Vinkel, 2016: 52). In fact, there have always been supporters who "lauded open-source software because it increases transparency in the voting process and makes independent testing of the election software straightforward" (Meagher, 2008: 378).

Actually, it is possible to observe a wider trend in the publication of source code[514]. In this regard, and if it has come to expect the details of cryptographic algorithms and protocols[515] to be published, scrutinized, and approved for public use (Martin, 2020: 209), why should remote electronic voting be an exception?

For example, the OSCE/ODIHR's EAM during the 2011 *Riigikogu* elections (OSCE/ODIHR, 2011b: 14) already

> "noted that there has been an increased degree of interest in observing the Internet voting on the part of the political parties and civil society. The NEC organized training sessions for domestic observers to familiarize them with the operation manual. Observers were allowed to view the source code of the voter application only after signing a non-disclosure agreement, which limited the observers' ability to comment on the source code and, therefore, transparency of the system."

In fact, even for previous elections Sutton Meagher had reported that "The software used in the Estonian Internet election is Linux-based, which has a source code that is open to the public[516]. Open source software makes it easier for the public and observers to

[514] This also applies to remote electronic voting. According to Jordi Puiggalí, already "[i]n 2011, within the context of the Norwegian Municipal Elections, the first case of source code publication took place, namely the Norwegian voting system, also developed by Scytl" (2019: 312).

[515] According to Keith Martin, "a cryptographic protocol […] dictates the precise procedure everyone needs to follow for the cryptographic tools used in the protocol to deliver the desired security. In fact, a cryptographic protocol is essentially a cryptographic algorithm whose operations are carried out by a number of different entities" (2020: 149).

[516] According to Sutton Meagher, "Election observers in Estonia have the opportunity to review the source code and the architecture of the electoral system, which is essential for a thorough audit of an election with Internet voting. In Internet elections, observers still have the same goals as they do in a paper ballot election, but their specific duties are different" (2008: 379). However, the OSCE/ODIHR only reported that "[p]rior to the local elections an individual expert contracted by the NEC reviewed the source code developed by the contracting company" (OSCE/ODIHR, 2007a:

access the software and check for vulnerabilities" (2008: 378). During the following elections, the OSCE/ODIHR acknowledged that "the NEC has facilitated a number of tests and other scrutiny exercises for the Internet voting system. This includes publishing the source code and initiating discussions with outside experts on potential vulnerabilities" (OSCE/ODIHR, 2015a: 6-7). However, the publication included only the server-side of the source code, and "the NEC explained that certain parts of it were not published for security reasons" (OSCE/ODIHR, 2015a: 7). Moreover, the OSCE/ODIHR's mission also reported that "[t]he EVC also used calculation and comparison of hash values of the source code files to demonstrate that the software installed on the server was the same as published in the repository" (OSCE/ODIHR, 2015b: 5).

A similar trend in observed in Switzerland. In the Swiss case, the publication of the source code became a requirement for the certification of a solution offering complete verifiability in 2018, following the findings of the Swiss expert group[517] (2018: 20). However, Geneva had already allowed for the inspection of their source code even before it became a requirement[518]. In this regard, while observing the 2015 federal elections the OSCE/ODIHR noticed that (2016: 10)

> "Publication of the source code is currently not a federal requirement. In a positive step, Geneva now allows citizens to review the source code of its system at its administration office, while the source code of the Neuchâtel system has not yet been made available. In addition, the parliament of Geneva is to review and amendment to the cantonal Act of Exercising Political Rights which, if adopted, would allow for the source code to be made publicly available in a manner that would be generally understandable."

The publication of the source code became a requirement with the decision of the Swiss Federal council of April 5, 2017 (Swiss expert group, 2018: 20). This requirement was later enshrined with the amendment of VEleS[519], in the following way (art. 7*a* VEleS):

> "1 The source code for the system software must be made public.
>
> 2 Publication shall take place when the system has the property of complete verifiability in terms of Article 5, and:

6). This is more in line with the argument provided by Priit Vinkel, according to whom (2016: 52-52)

> "[i]n Estonia, however, the source code of the e-voting solution was not universally available until 2013, but one could access it by signing a non-disclosure agreement with the EMB. However, after the legal debates of 2012, the source code of all central servers of the voting system, as well as the software of the vote verification application, have been made freely available on the internet."

[517] According to the Swiss expert group, « [l]e protocole cryptographique utilisé pour mettre en œuvre la vérifiabilité complète doit lui aussi être vérifié par une autorité indépendante […]. D'autre part, le code source des systèmes offrant une vérifiabilité complète sera publiquement accessible » (2018: 20).

[518] According to the Swiss Federal Council (2013a: 61),

> « [l]a loi cantonale sur les droits politiques permet aux citoyens genevois l'accès au code source de l'application pour autant qu'ils justifient « d'un intérêt scientifique et purement idéal ». Le Conseil d'État a donné à deux reprises son aval à un tel accès, à des représentants du Parti Pirate genevois et à un étudiant et à un collaborateur de la Haute école spécialisée bernoise. »

[519] According to the Swiss Federal Chancellery (2018c: 15):

> « [l]'art. 7a et 7b de l'OVotE exigent des cantons qu'ils publient le code source du système complètement vérifiable destiné au vote électronique, accompagné d'une documentation suffisante. Le code source permet de voir comment le système enregistre et traite les votes. Le principe de transparence est important et doit être inscrit dans la loi. Les informations permettent aux spécialistes d'évaluer la sécurité et la qualité d'un système. »

> a. following the examination in accordance with Article 7 paragraph 2 if more than 30 per cent of the cantonal electorate are to be authorised to participate in a trial;
>
> b. following the examination in terms of Article 7 paragraph 3 if no more than 30 per cent of the cantonal electorate are to be authorised to participate in a trial.
>
> 3 There is no requirement to publish the source code of the following:
>
> a. third-party components such as operating systems, databases, web and application servers, rights management systems, firewalls or routers, provided these are freely available and regularly updated;
>
> b. portals of authorities that are linked to a system."

In turn, art. 7*b* prescribes that "[t]he source code must be prepared and documented according to the best practices", that "[i]t must be easily obtainable, free of charge, on the internet", and that "[t]he documentation must be published along with the source code." (art. 7*b* VEleS). All in all, "anyone is entitled to examine, modify, compile and execute the source code for ideational purposes, and to write and publish studies thereon" (Driza Maurer, 2019: 92).

According to Ardita Driza Maurer, "[t]he source code should be published only after the system has been certified. In the words of the federal [sic] Chancellery, a trustworthy control prior to publication guarantees that the advantages of the publication of the source code outweigh the potential risks associated with it" (2019: 92). As reported by to Jordi Puiggalí, "[t]he new sVote voting system passed the audit certification processes for complete verifiability compliance in January 2019 and therefore, the source code was published under the previous registration before starting the authorization process from any Canton" (2019: 312). Following the publication of the source code of Swiss Post's system on 7 February 2019, "[a] group of researchers discovered significant flaws in the course code" (Driza Maurer, 2019: 85). Two of these flaws concerned critical steps related to secret suffrage, including the mixing proof and the decryption proof[520].

(Public) Intrusion Tests and bug bounty programmes

Additionally, the election administration can organise a public intrusion test. During a public intrusion test, those who wish to do so are invited to try to hack into the systems (Swiss expert group, 2018: 20). For the time being, in Europe only Switzerland has conducted such a public intrusion test. "The federal Chancellery and cantons decided to organize a public intrusion test (PIT), open to anyone, to check the security of the Swiss Post system offering complete verifiability" (Driza Maurer, 2019: 93). More specifically, this PIT was framed as a bug bounty, "with the Swiss Post committing financial compensation to

[520] According to Jordi Puiggalí (2019: 321),

> "[t] The main critical findings where the three that affected the core cryptographic verifiability features of the voting system: universal and individual verifiability. The first finding affected the universal verifiability of the Mixing process implemented in the first control component (the one that anonymizes the votes before decryption). The second affected the universal verifiability of the partial decryption process implemented also in the first control component. Finally, the last one affected individual verifiability of the Return Codes generated in the voter device. While all these findings were reported with examples of theoretical attacks, none of these attacks were carried out in practice in the PIT platform. It can be excluded that past votes or elections have been manipulated because of these findings, since the attack always generates invalid votes and such votes have never been reported in previous elections."

participants who would be the first to reveal a relevant vulnerability" (Driza Maurer, 2019: 93).

According to Ardita Driza Maurer, it was the "most complete transparency exercise organized so far on a Swiss internet voting system and, to our knowledge, the most complete on an internet voting system for political elections"[521] (2019: 85). It is interesting to stress that one of the categories of the PIT included vulnerabilities related to vote privacy, such as "the privacy of a voter is broken (who voted) on the server" and "the privacy of a vote is broken (what did they vote) on the server"[522] (Puiggalí, 2019: 319). "As for the PIT, a total of 16 responses were classified as breachers of best practice. According to the federal [sic] Chancellery, they do not constitute major risks" (Driza Maurer, 2019: 85).

These experiences allow us to draw some conclusions. The first one is that the mere publication of the source code or the organisation of a public intrusion test may not be enough by themselves to ensure that the requirements are met. For example, the public review of the source code revealed "several flaws", whether the responses to the PIT were only classified as breached of best practice and "did not constitute major risks" (Driza Maurer, 2019: 85). In this regard, the Swiss Federal Chancellery has noted that "[a]n extensive publication of the source code doesn't guarantee that researchers and third-party developers continually participate in the improvement of the code" (Swiss Federal Chancellery, 2020b: 41). During the years, the Geneva internet voting system published more and more of its source code with an open source license[523] and adopted a more and more open development practice. However, there was very little contribution from 3rd party developers" (Swiss Federal Chancellery, 2020b: 41).

If we also think in the different objectives that a certification process aims at (i.e., certify the cryptographic protocol, the software security and functionality, the security of the infrastructure and its resilience against instructions, etc.) it also seems obvious that more than one certification mechanisms are needed (i.e., it is not possible to certify the security of the infrastructure and its resilience against instructions by reviewing the source code). When it comes to the Swiss case, and in the opinion of Jordi Puiggalí, the "two steps (source code publication and PIT) were important to detect and solve any issue that was not previously detected during the certification process" (2019: 312). Interestingly, Jordi Puiggalí identifies three layers for the certification of a voting system (2019: 316), which in fact could be applied to any experience [emphasis added]:

> "• **The regulatory layer**: sets-up the abstract model requirements. In the case of the Swiss regulation, we are talking about the VEleS regulation (and ordinance

[521] However, Jordi Puiggalí has reported that "[t]he closes experience conducted before is the public test on the 'D.C. Digital Vote-by-Mail Service' voting system piloted by the Washington, D.C. Board of Elections and Ethics (BOEE) in 2010. In this case, the voting system, consisted of an open-source web-based platform for downloading and uploading PDF files through the internet" (2019: 311).

[522] Compensation for finding these vulnerabilities was set at 5'000- Swiss francs, where compensation for other vulnerabilities spanned from 100.- Swiss francs in the case of best practices to 30'000.- and 50'000.- for undetectable vote manipulation (Puiggalí, 2019: 319).

[523] In this regard, the Swiss Federal Chancellery reports that « [l]e canton de Genève a publié en 2016 en open source plusieurs parties de code source de son système à vérifiabilité individuelle. Il a également publié en 2019 dans l'état de son développement le code source de son système à vérifiabilité complète » (2020c : 6).

passed by the Swiss Federal Chancellery)[524]. The nexus between this layer and the next one (abstract layer) is the VEleS technical annex.

- **The abstract layer**: in this layer, voting systems need to prove, in a mathematical sense, that they are compliant with the abstract model defined in the regulatory layer. The basis of this process is the VEleS' technical annex, and the way to certify compliance is by providing cryptographic and formal proofs compliant with the abstract model. In the case of complete verifiability, proofs must be provided to guarantee verifiability and vote secrecy.
- **The implementation layer**: this final layer contains the software development of a system based on the cryptographic protocol described in the abstract layer. The implementation of this layer is mainly based on two deliverables. The protocol specification (used for the development process) and the source code of the voting system and related documentation (deployment guides, audit documentation, etc.)."

To sum up, the publication of the source code still needs to be complemented with the certification and audit mentioned above, as well as with the complete verifiability mechanisms[525]. It seems reasonable that in order to certify a solution at each layer, including the properties that guarantee the standards of secret suffrage, different mechanisms will be necessary, including certification and audit, the publication of the source code, and (public) intrusion tests. Likewise, naked-eye observation of certain procedures will be needed to ascertain that procedural guarantees are also satisfied (i.e., in terms of the anonymisation procedures or the reconstruction of the election private key). In this regard, only the combination of the different measures will enhance the transparency and therefore possibly the trustworthiness of the system as well, whereas each of them individually may not be enough to satisfy these requirements.

[524] As we have seen above, in the Swiss case VEleS is not the only source at the regulatory layer, since the Constitution, the Federal Act on Political Rights, and the Federal Ordinance on Political Rights are on top of the Federal Chancellery's ordinance.

[525] According to the Swiss Federal Chancellery (2018c: 15)

> « [l]a vérifiabilité prévue à l'art. 8b P-LDP va également dans le sens du principe de transparence. Alors que la vérifiabilité permet de contrôler le vote et le dépouillement d'un scrutin effectif, la publication d'informations relatives au système et à son fonctionnement permet de s'en faire une idée indépendantment d'un vote réel. »

Conclusions

One of the key concerns about remote electronic voting is how to preserve secret suffrage. The list of authors who claim that Internet voting is incompatible with the secrecy of the vote is actually quite long. Even if later studies that analysed the actual implementation of remote electronic voting in public political elections had more nuanced findings, concerns about secret suffrage and remote electronic voting remain: in a recent survey among the member states of the Council of Europe, 5 out of 32 respondents (equivalent to 14%) mentioned the "inability to (permanently) guarantee secrecy of vote as one reason for not implementing e-voting solutions" (European Committee on Democracy and Governance, 2021b: 6).

Nowadays, addressing these concerns becomes an inescapable obligation. On the one hand, and because of the steady adoption of end-to-end verifiable remote electronic voting systems, debates about secret suffrage and remote electronic voting have resumed. On the other hand, on-going events and claims of espionage force us to look once again into this issue. In this context, the current research has offered insights and guidance at the intersection of ongoing debates about the national and transnational dimensions of electoral principles as well as the still unsolved engagement of legal and technological regulations. All in all, advancing existing research on secret suffrage and remote electronic voting is still necessary to fully understand, as put by Ardita Driza Maurer, "the challenge of regulating a domain at the cross-roads of law and technology" (2013:16).

To this end, the Introduction has provided an overarching framework for the study of secret suffrage and remote electronic voting: a non-originalist perspective towards secret suffrage in remote electronic voting. Because our research is related to the regulation of a transnational principle, in between law and digital technologies, we have resorted to the universalist search for just or good principles and the theories of postnational constitutionalism to approach it. Additionally, Lawrence Lessig's theories on the regulation of cyberspace and Luciano Floridi's "infosphere" has helped inform the digital dimension of secret suffrage in remote electronic voting. Together, both sets of theories have allowed us to cope with the relevance of new regulatory structures, the proliferation of regulatory agents, and the emerge of new social practices for secret suffrage in remote electronic voting.

In chapter 2 we have analysed the historical origins, evolution, and current configuration of secret suffrage in the European Electoral Heritage. Our goal in this chapter has been to identify the transborder common content of secret suffrage, its existence as a principle that transcend the culture bound opinions and conventions of a particular political community. Despite our focus being on Europe, non-European experiences have been also considered since understanding them is paramount to inform the evolution of secret suffrage. Once the historical roots of this principle have been set, we have focused on identifying the legal international and European frameworks on secret suffrage and democratic elections. This has allowed us to identify three main standards for secret suffrage: individuality, confidentiality, and anonymity. We have argued that understanding the principle of secret suffrage in terms of these standards is a better approach that an understanding based on specific technologies (i.e., voting booths, envelopes, etc.). The last section of this chapter has dealt with some limitations of the current configurations of secret suffrage, including how paper-based voting methods usually prevent some voters

from casting their votes in secret and how certain technologies are overcoming the existing protections for secret suffrage in polling stations.

In chapter 3 we have provided a first approach towards remote electronic voting in practice, looking both at national experiences and to the development and institutionalisation of transnational standards. Therefore, this chapter has aimed at providing an understanding of how remote electronic voting has shaped the regulation of elections in different countries, as well as at the international level. More specifically, we have studied the experiences in Switzerland, France, and Estonia. Analysing them has allowed us to take stock of almost twenty years of experiences regulating electoral principles in the face of digital technology. The study of the three national experiences has also helped us identify the existing legal framework, the actors involved in e-enabled elections, and the main issues in each of the different elections and votes. It has also allowed us to assess the relevance of secret suffrage, which have been important in all three countries: either as concerns, criticism, or being subject to judicial review. Following, we have also examined how international and European electoral standards have evolved to cope with these new developments, with specific focus on both legal and technological standards. As a result of the work carried out in this chapter, specific requirements have been elicited and questions about secret suffrage that are unique to remote electronic voting have been raised.

In chapter 4 we have deepened in how the introduction of remote electronic voting for public political elections has affected the observance of secret suffrage. The goal of this chapter has been twofold. First, we have assessed how secret suffrage is regulated in remote electronic voting, starting with international standards. Such an analysis has allowed us to provide a broader framework for scrutinising the intertwining of the principle of secret suffrage in remote electronic voting. To do so, we have assessed the standards on secret suffrage in the Council of Europe's Recommendation on e-voting as well as in other European standards. Secondly, we have addressed the national experienced in more detail. Together, both sections have allowed us to assess the degree of compliance of both international standards and the national experiences against the three minimum standards of secret suffrage: individuality, confidentiality, and anonymity.

Our broken-down analysis against the three minimum standards reveals which mechanisms have been put in place to observe them. First, individuality can be guaranteed by allowing voters to cast multiple votes, either online or both electronically and on paper. Second, confidentiality is ensured with the use of encryption, which should be applied to each vote (and not just to the voting channel) from the moment they are cast (and not server-side). At the same time, encryption may be reinforced with the use of key-sharing mechanisms that mitigate the risk of votes being decrypted ahead of the counting phase. Key-sharing mechanisms thus in turn call for the use of asymmetric or public key encryption. Third, anonymity is ensured with several techniques. Among them, mix-nets and homomorphic encryption have proven to be the most effective (while important flaws have been already identified for other alternatives). It has also been found that anonymity in remote electronic voting is conditional, in a similar way to other alternative voting channels (such as postal voting or advanced voting in polling stations). For this reason, and as it is the case with encryption, the use of a key-sharing mechanisms mitigates the risk of breaches of anonymity as well.

Lastly, chapter 5 has challenged the very formulation of such principle by identifying specific challenges to secret suffrage in remote electronic voting. In turn, we have

identified some mechanisms that can be put in place to address them but that also scape any approach towards secret suffrage in remote electronic voting by analogy to paper-based voting channels. All in all, this chapter has called for revisiting the very principle of secret suffrage in the context of remote electronic voting in general and, more precisely, for abandoning the resort to analogy (i.e., with postal voting) in the regulation of electoral principles for e-enabled elections. This has allowed us to provide some recommendations for the regulation of secret suffrage in remote electronic voting: coercion-resistance and multiple voting mechanisms for individuality; asymmetric, quantum-resistant vote encryption with key-sharing schemes for confidentiality; and anonymous tallying for confidentiality.

In chapter 5 we have also addressed another shortcoming: the fact that democratic elections must comply not only with secret suffrage, but also with the principles of universal, equal, free and direct suffrage. We have stressed that these principles impose additional requirements to the conduct of democratic elections, which span from voter eligibility and authentication, to integrity, transparency, and observation. Building on the theories presented in the Introduction, we have asked whether e-enabled elections raise any latent ambiguities. This question has proved salient when it comes to the verifiability of remote electronic voting, and especially individual verifiability mechanisms that allow voters to ascertain that their vote has been cast-as-intended and recorded-as-cast. This analysis has allowed us to conclude that, whereas a trade-off is usually drawn between secret suffrage vis-à-vis the integrity and the transparency of elections, it is not just possible but also necessary to envisage ways to observe secret suffrage in remote electronic voting.

These conclusions open to door to future research on secret suffrage and remote electronic voting. On the one hand, it is important to keep analysing the case studies. By the time of finalising it, Switzerland has adopted a new regulation that we have not manage to study in this PhD. At the end of the day, remote electronic voting regulations are constantly amended, and this requires an on-going assessment. The same thing happens when it comes to international standards. Having provided a throughout understanding of secret suffrage in remote electronic voting, future research could then address how technological developments may impact in our conclusions. On the other hand, we must also acknowledge the limitations of looking just into three European case studies. Our conclusions may be robust enough to inform the debates about secret suffrage and remote electronic voting in the context of the European Electoral Heritage. Notwithstanding, the external validity of these conclusions (and their applications to non-European scenarios in America, Oceania, Asia and Africa) may provide different results: at the end of the day, legal principles are contextual and cultural-dependent, and so is secret suffrage. Last, but not least, our conclusions could also be tested against other electoral principles. Are equal, universal, and free suffrage in remote electronic voting also regulated by analogy to paper-based voting channels? We cannot answer this question solely based on the research conducted so far, but our conclusions may point indeed towards the need of critical approaching these principles as well.

In sum, our research is quite novel. First and foremost, our starting point is not based on pre-existing legal definitions that are accepted as given. This is legal research, but our definition of secret suffrage has not been based on the provisions of national constitutions or electoral laws. Drawing from the universalist approach to comparative constitutional

law, we have understood that the principle of secret suffrage exists in such a way that it transcends the culture bound opinions and conventions of particular political communities. This core understanding has been translated into three standards: individuality, confidentiality, and anonymity. These standards should apply to any voting channel, and therefore they provide a better framework than the technologies that have been used to enforce secret suffrage in specific voting channels (i.e., voting booths, envelopes, or ballot boxes).

Second, we have taken a wider approach at the enforcement of this principle. We have showed that secret suffrage may be enforced through law, code, norms, and even the market. In the case of remote electronic voting, we have examined the role played by (and the limitations of) asymmetric encryption, anonymization based on mix-nets or homomorphic tallying, and of multiple voting to enforce secret suffrage. We have argued that remote electronic voting regulations should be more detailed when it comes to specifying how these architectures of cyberspace could contribute towards the enforcement of legal principles (e.g., by specifying procedures, decryption thresholds, algorithms, or even key sizes, be it directly or by referring to existing technological standards).

Therefore, this PhD has gone beyond specific case studies about Internet voting (be they focused on secret suffrage or not) and research on the broader interaction between international (electoral) principles and digital technologies. As a result, we have been able to provide an overarching framework to guide the examination of how digital technologies impact on electoral processes and the principles for democratic elections.

References

International and European standards

International standards (hard law and soft law)

International Covenant on Civil and Political Rights (ICCPR), 16 December

United Nations (1948) *Universal declaration of human rights*.

United Nations' Human Rights Committee (1996) *General Comment No. 25 (57) to the International Covenant on Civil and Political Rights*, 27 August

European standards (hard law and soft law)

European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights), as amended by Protocols Nos. 11 and 14, 4 November 1950.

Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights), as amended by Protocol No. 11, 18 May 1954.

Council of Europe (2004a) *Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting*.

Council of Europe (2004b) *Explanatory memorandum to the Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting*.

Council of Europe (2010a) *Guidelines on transparency of e-enabled elections*.

Council of Europe (2010b) *Certification of e-voting systems: Guidelines for developing processes that confirm compliance with prescribed requirements and standards*.

Council of Europe (2017a) *Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting*.

Council of Europe (2017b) *Explanatory Memorandum to Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting*.

Council of Europe (2017c) *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*.

European Commission for Democracy Through Law (Venice Commission) (2002a) *Code of Good Practice in Electoral Matters: Guidelines on Elections*. Adopted by the Venice Commission at its 51st and 52nd sessions (Venice, 5-6 July and 18-19 October 2002).

European Commission for Democracy Through Law (Venice Commission) (2002b) *Explanatory Report to the Code of Good Practice in Electoral Matters*. Adopted by the

Venice Commission at its 51st and 52nd sessions (Venice, 5-6 July and 18-19 October 2002).

European Commission for Democracy Through Law (Venice Commission) (2004) *Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe*. Adopted by the Venice Commission at its 58th Plenary Session (Venice, 12-13 March 2004)

European Commission for Democracy Through Law (Venice Commission) (2007) *Code of good practice on Referendums*. Adopted by the Council for Democratic Elections at its 19th meeting (Venice, 16 December 2006) and the Venice Commission at its 70th plenary session (Venice, 16-17 March 2007)

European Commission for Democracy Through Law (Venice Commission) (2016) *Interpretative Declaration of the code of good practice in electoral matters on the publication of lists of voters having participated in elections*. Adopted by the Council for Democratic Elections at its 56th meeting (Venice, 13 October 2016) and by the Venice Commission at its 108th Plenary Session (Venice, 14-15 October 2016).

Parliamentary Assembly of the Council of Europe (2007a) *Secret ballot – European code of conduct on secret balloting, including guidelines for politicians, observers and voters. Resolution 1590*.

Parliamentary Assembly of the Council of Europe (2007b) *Secret ballot – European code of conduct on secret balloting, including guidelines for politicians, observers and voters. Report*.

OSCE/ODIHR (1990) *Document of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE*, 29 June

Technological standards

BSI-CC-PP-0037 (2018) Common Criteria Protection Profile for Basic set of security requirements for Online Voting Products. Version 1.0.

National legal and administrative acts

Estonia

The Constitution of the Republic of Estonia (1992, last amended 13.04.2011)

Riigikogu Election Act (2002; last amended 11.12.2019)

Local Government Council Election Act (2002; last amended 11.12.2019)

State Electoral Office of Estonia (2017) *General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia*.

France

Constitution (1958; last amended 1.12.2009)

Code électoral (1964; last amended 1.05.2022)

CNIL (2003) *Délibération n° 2003-036 du 1er juillet 2003 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique*. JORF number 212 of 13 September 2003, text number 83.

CNIL (2006) *Délibération nº 2006-042 du 23 février 2006 portant avis sur le traitement de données à caractère personnel mettant en œuvre un dispositif de vote électronique pour les élections à l'Assemblée des Français de l'étranger du 18 juin 2006.* JORF number 92 of 19 April 2006, text number 88.

CNIL (2010) *Délibération n° 2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique*, JORF number 0272 of 24 November 2010, text number 29.

CNIL (2019a) *Délibération nº 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.* JORF number 0142, of 21 June 2019, text number 95.

CNIL (2019b) *Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via internet (rectificatif).* JORF number 0149, of 29 June 2019, text number 108.

CNIL (2019c) *Sécurité des systèmes de vote par internet : la CNIL actualise sa recommandation de 2010*. Online press release, 10 July 2019. Available at: <https://www.cnil.fr/fr/securite-des-systemes-de-vote-par-internet-la-cnil-actualise-sa-recommandation-de-2010> [retrieved 27 May 2022]

Switzerland

Loi fédérale sur les droits politiques (1976; last amended 1.11.2015)

Ordonnance sur les droits politiques (1976; last amended 1.07.2019)

Swiss Federal Chancellery (2013a) *Vote électronique: catalogue de critères pour les imprimeries*, of 6 February.

Swiss Federal Chancellery (2013c) *Ordonnance de la ChF sur le vote électronique (VEleS)*, of 13 December.

Swiss Federal Chancellery (2018d) *Annexe à l'ordonnance de la ChF du 13 décembre 2013 sur le vote électronique. Exigences techniques et administratives applicables au vote électronique*, of 1 July (version 2.0).

Case-law

European Court of Human Rights

European Court of Human Rights (1997) *Demir and Baykara v. Turkey*. Strasbourg: Council of Europe.

European Court of Human Rights (2018) *Magyar Kétfarkú Kutya Párt v. Hungary*. Judgement. Strasbourg: Council of Europe.

Estonia

Republic of Estonia, Supreme Court (2005) *Judgement of the Constitutional Review Chamber of the Supreme Court, Decision 3-4-1-13-05, 1 September.*

National reports

France

Anziani, Alain and Lefèvre, Antoine (2014) *Vote électronique : préserver la confiance des électeurs.* Sénat, fait au nom de la commission des lois.

Apple, Andrew W. (2006) *Ceci n'est pas une urne : On the Internet vote for the Assemblée des Français de l'Étranger*.

Buffet, François-Noël (2020) Le *vote à distance, à quelles conditions ?* Sénat, ait au nom de la commission des lois.

Deromedi, Jacky and Détraigne, Yves (2018) *Réconcilier le vote et les nouvelles technologies*. Sénat, ait au nom de la commission des lois.

Deromedi, Jacky; Frassa, Christophe-André and Leconte, Jean-Yves (2020) *16 propositions pour garantir les élections consulaires en 2021*. Sénat, ait au nom de la commission des lois.

Haritcalde, Marie-Christine (2020) *Bilan du Test Grandeur Nature*.

Lang, Bernard (2006) *Rapport sur l'usage du vote électronique par l'Internet pour les élections à l'Assemblée des Français de l'Étranger de juin 2006.*

Pellegrini, François (2006) *Rapport observation mandaté par l'association représentative Association Démocratique des Français à l'Étranger – Français du Monde afin d'auditer le. Déroulement du vote par correspondance électronique des électeurs inscrits sur les listes électorales consulaires des circonscriptions électorales d'Europe et d'Asie et Levant pour les élections de 2006 à l'Assemblée des Français de l'Étranger.*

Switzerland

Swiss Council of States (2000) *E-Switzerland. Modifications législatives, calendrier et moyens*, of 22 June.

Swiss Groupe d'experts Vote électronique (2018) *Rapport final*.

Swiss Federal Chancellery (2004) *Le vote électronique dans sa phase pilote - Rapport intermédiaire.*

Swiss Federal Chancellery (2011) *Feuille de route du vote électronique*.

Swiss Federal Chancellery (2013b) *Rapport concernant les résultats de la procédure d'audition relative à l'édiction d'un règlement technique sur le vote électronique*.

Swiss Federal Chancellery (2017a) *Consultation relative au nouvel instrument de planification. Rapport d'évaluation*.

Swiss Federal Chancellery (2017b) *Déclaration d'intention pour l'introduction du vote électronique*.

Swiss Federal Chancellery (2017c) *Mandat du Groupe d'experts Vote électronique : passage à la mise en exploitation et dématérialisation du vote*.

Swiss Federal Chancellery (2018a) *Vote électronique : publication du code source. Rapport explicatif sur la modification de l'ordonnance de la ChF sur le vote électronique (OVotE)*.

Swiss Federal Chancellery (2018b) *Loi fédérale sur les droits politiques. Passage de la phase d'essai à la mise en exploitation du vote électronique. Avant-projet du 19 décembre 2018.*

Swiss Federal Chancellery (2018c) *Modification de la loi fédérale sur les droits politiques (Passage de la phase d'essai à la mise en exploitation du vote électronique). Rapport explicatif pour la procédure de consultation.*

Swiss Federal Chancellery (2019a) *Public Intrusion Test. Fact sheet produced by the Federal Chancellery*.

Swiss Federal Chancellery (2019b) *Public Intrusion Test. Fact sheet produced by the Management Committee of the Confederation and the Cantons*.

Swiss Federal Chancellery (2019c) *Modification de la loi fédérale sur les droits politiques (Passage de la phase d'essai à la mise en exploitation du vote électronique). Rapport sur les résultats de la consultation*.

Swiss Federal Chancellery (2019d) *Vote électronique – Public Intrusion Test 2019. Final report of the steering committee*.

Swiss Federal Chancellery (2020a) *Dialog with Experts 2020. Management summary*.

Swiss Federal Chancellery (2020b) *Summary of the expert dialog. Redesign of Internet Voting Trials in Switzerland 2020*.

Swiss Federal Chancellery (2020c) *Restructuration et reprise des essais. Rapport final du Comité de pilotage Vote électronique (CoPil VE)*

Swiss Federal Council (2002) *Rapport sur le vote électronique du 9 janvier 2002: Chances, risques et faisabilité*.

Swiss Federal Council (2006) *Rapport sur les projets pilotes en matière de vote électronique*.

Swiss Federal Council (2013a) *Rapport du Conseil fédéral sur le vote électronique Évaluation de la mise en place du vote électronique (2006–2012) et bases de développement. Management Summary.*

Swiss Federal Council (2013b) *Rapport du Conseil fédéral sur le vote électronique Évaluation de la mise en place du vote électronique (2006–2012) et bases de développement.*

Swiss Federal Council (2013c) *Documentation complétant le troisième rapport du Conseil fédéral sur le vote électronique.*

Swiss National Council (2000) *Utilisation des technologies de l'information au profit de la démocratie directe*.

The United States

Congressional Research Service (2021) *EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield.*

Election observation methodologies and reports

Election observation methodologies

OSCE/ODIHR (2010) *Election Observation Handbook: Sixth Edition*. Warsaw, Poland: OSCE/ODIHR.

OSCE/ODIHR (2013) *Guidelines for Reviewing a Legal Framework for Elections*. Warsaw, Poland: OSCE/ODIHR.

OSCE/ODIHR (2014) *Handbook for the Observation of New Voting Technologies*. Warsaw, Poland: OSCE/ODIHR.

OSCE/ODIHR (2014) *Alternative voting methods and arrangements*. Available at: <https://www.osce.org/odihr/elections/466794> [retrieved: 27 May 2022]

OSCE/ODIHR observation reports

OSCE/ODIHR (2007a) *Republic of Estonia Parliamentary Elections 4 March 2007. OSCE/ODIHR Needs Assessment Mission Report*.

OSCE/ODIHR (2007b) *Republic of Estonia Parliamentary Elections 4 March 2007. OSCE/ODIHR Election Assessment Mission Report*.

OSCE/ODIHR (2007c) *Swiss Confederation Federal Elections 21 October 2007. OSCE/ODIHR Needs Assessment Mission Report*.

OSCE/ODIHR (2008) *Swiss Confederation Federal Elections 21 October 2007. OSCE/ODIHR Election Assessment Mission Report*.

OSCE/ODIHR (2011a) *Estonia Parliamentary Elections 6 March 2011. OSCE/ODIHR Needs Assessment Mission Report*.

OSCE/ODIHR (2011b) *Estonia Parliamentary Elections 6 March 2011. OSCE/ODIHR Election Assessment Mission Report*.

OSCE/ODIHR (2011c) *Swiss Confederation Federal Elections 23 October 2011. OSCE/ODIHR Needs Assessment Mission Report*.

OSCE/ODIHR (2012a) *Swiss Confederation Federal Elections 23 October 2011. OSCE/ODIHR Election Assessment Mission Report*.

OSCE/ODIHR (2012b) *France, Parliamentary Elections, 10 and 17 June 2012: Needs Assessment Report.*

OSCE/ODIHR (2012c) *France, Parliamentary Elections, 10 and 17 June 2012: Final Report.*

OSCE/ODIHR (2015a) *Estonia Parliamentary Elections 1 March 2015. OSCE/ODIHR Needs Assessment Mission Report*.

OSCE/ODIHR (2015b) *Estonia Parliamentary Elections 1 March 2015. OSCE/ODIHR Election Expert Team Mission Report*.

OSCE/ODIHR (2015c) *Swiss Confederation Federal Assembly Elections 18 October 2015. OSCE/ODIHR Needs Assessment Mission Report*.

OSCE/ODIHR (2016) *Swiss Confederation Federal Assembly Elections 18 October 2015. OSCE/ODIHR Election Expert Team Final Report*.

OSCE/ODIHR (2017) *France Presidential and Parliamentary Elections, 2017: Needs Assessment Mission Report*.

OSCE/ODIHR (2019a) *Estonia Parliamentary Elections 3 March 2019. ODIHR Needs Assessment Mission Report*.

OSCE/ODIHR (2019b) *Estonia Parliamentary Elections 3 March 2019. ODIHR Election Expert Team Final Report*.

OSCE/ODIHR (2019c) *Swiss Confederation Federal Assembly Elections 20 October 2019. ODIHR Needs Assessment Mission Report*.

Bibliography

Aidt, Toke S. and Jensen, Peter S. (2017) "From Open to Secret Ballot: Vote Buying and Modernisation". *Comparative Political Studies*, 50(5), pp. 555-593.

Arato, Andrew (2000) *Civil Society, Constitution, and Legitimacy*. Maryland, USA: Rowman and Littlefield Publishing, Inc.

Atienza Rodriguez, Manuel (1986) *Sobre la analogía en el derecho: ensayo de análisis de un razonamiento jurídico.* Madrid, España: Cuadernos Civitas.

Barlow, John Perry (1996) *Declaration of the Independence of Cyberspace*.

Barrat i Esteve, Jordi (2012) "El secreto del voto en el sufragio por internet". *Revista Mexicana de Análisis Político y Administración Pública*, 1:2, pp. 57-71.

Barrat, Jordi (2015) "The French *Conseil Constitutionnel* and Electonic Voting". Driza Maurer, Ardita and Barrat, Jordi (eds.) *E-Voting Case Law. A Comparative Analysis.* Surrey, England: Ashgate, p. 131-150.

Barrat, Jordi; Chevalier, Michel; Goldsmith, Ben; Jandura, David; Turner, John, and Sharma, Rakesh (2012) "Internet Voting and Individual Verifiability: the Norwegian Return Codes". Kripp, Manuel J.; Volkamer, Melanie, and Grimm, Rüdiger (eds.) *5th International Conference on Electronic Voting 2012 (EVOTE2012)*. Bonn: Gesellschaft für Informatik e.V., pp. 35-45.

Barrat i Esteve, Jordi and Goldsmith, Ben (2012) *Compliance with International Standards.* Norwegian E-Vote Project*.* Washington, United States: International Foundation for Electoral Systems.

Barrat i Esteve, Jordi; Goldsmith, Ben and Turrner, John (2012) *International Experience with E-Voting.* Norwegian E-Vote Project*.* Washington, United States: International Foundation for Electoral Systems.

Beard, Mary (2017) "Modern elections and the Romans". *The Times Literary Supplement*.

Bertrand, Romain; Briquet, Jean-Louis and Pels, Peter (2017) "Introdution". Bertrand, Romain; Briquet, Jean-Louis and Pels, Peter (eds) *The Hidden History of the Secret Ballot*. Bloomington and Indianapolis, USA: Indiana University Press, p. 1-15.

Beullens, Ward; D'Anvers, Jan-Pieter; Hüsling, Andreas; Lange, Tanja; Panny, Lorenz; de Saint Guilhem, Cyprien y Smart, Nigel P. (2021) Post-Quantum Cryptography: Current state and quantum mitigation, European Union Agency for Cybersecurity (ENISA).

Birch, Sarah and Watt, Bob (2004) "Remote Electronic Voting: Free, Fair and Secret?". *The Political Quarterly Publishing*, 75:1, pp. 60-72.

Braun, Nadja (2005) *Stimmgeheimnis : eine rechtsvergleichende und rechtshistorische Untersuchung unter Einbezug des geltenden Rechts*. Switzerland: Stämpfli Verlag AG, Bern.

Braun, Nadja (2004) "E-Voting: Switzerland's Project and their Legal Framework – in a European Context". Prosser, Alexander; Krimmer, Robert (eds): *Electronic Voting in Europe*: Technology, Law, Politics and Society. Bonn, pp. 43-52.

Brennan, Geoffrey and Pettit, Philip (1990) "Unveiling the Vote". *British Journal of Political Science*, 20(3), pp. 311-333.

Breuer, Fabian and Trechsel, Alexander H. (2006) *Report for the Council of Europe. E-voting in the 2005 local elections in Estonia. Report for the Council of Europe*. Florence: e-Democracy Centre, e-Governance Academy and the European University Institute.

Brundage, Miles et al. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*.

Buchstein, Hubertus (2015) "Public Voting and Political Modernization. Different Views from the Nineteenth Century and New Ideas to Modernize Voting Procedures". Elster, Jon (ed.) *Secrecy and Publicity in Votes and Debates*. New York, USA: Cambridge University Press, pp. 15-51

Buldas, Ahto; Heiberg, Sven; Krips, Kristjan and Willemson, Jan (2020). *Mobile voting feasibility study and risk analysis*. Cybernetica report T-184-5. Tallin: Cybernetica.

Carr, Nicholas (2011) *The Shallows: What the Internet Is Doing to Our Brains*. New York, USA and London, UK: W. W. Norton.

Castells, Manuel (2010) *The Rise of the Network Society.* West Sussex, United Kingdom: Blackwell Publishing Ltd, 2nd edition.

Cath, Corinne and Floridi, Luciano (2017) "The Design of the Internet's Architecture by the Internet Engineering Task Force (IETF) and Human Rights". *Sci Eng Ethics*, 23, pp. 449–468.

Chen, Lily; Jordan, Stephen; Liu, Yi-Kai; Moody, Dustin; Peralta, Rene; Perlner, Ray y Smith-Tone, Daniel (2016) R*eport on Post-Quantum Cryptography, NISTIR 8105*.

Chiudhry, Sujit (1999) "Globalizaion in Search of Justification: Toward a Theory of Comparative Constitutional Interpretation". *Indiana Law Journal,* Vol. 74, Issue 3, pp. 819-892.

Costa, Núria (2021) *Long-term privacy in electronic voting systems*. PhD Thesis. Available at: <https://upcommons.upc.edu/handle/2117/348913> [retrieved: 27 May 2022]

Costa, Núria; Martinez, Ramiro and Morillo, Paz (2017) "Proof of a Shuffle for Lattice-Based Cryptography".Lipmaa, H., Mitrokotsa, A., Matulevicius, R. (eds.) *Proceedings of NordSec 2017*. LNCS, vol. 10674, pp. 280–296. Springer (2017)

Costa, Núria; Martinez, Ramiro and Morillo, Paz (2019) "Lattice-Based Proof of a Shuffle". Bracciali, A., Clark, J., Pintore, F., Rønne, P.B., Sala, M. (eds.) *Proceedings of Financial Cryptography and Data Security - FC 2019*. LNCS, vol. 11599, pp. 330–346. Springer (2019)

Cucurull, Jordi; Rodríguez-Pérez, Adrià; Finogina, Tamara and Puiggalí, Jordi (2019) Blockchain-Based Internet Voting: Systems' Compliance with International Standards. Abramowicz W., Paschke A. (eds) Business Information Systems Workshops. BIS 2018. Lecture Notes in Business Information Processing, vol 339. Springer, Cham.

Dandoy, Régis and Kernalegenn, Tudi (2021) "Internet voting from abroad: exploring turnout in the 2014 French consular elections". *French Politics,* vol. 19, pp. 421–439

Davies, Tidd (2004): "Consequences of the Secret Ballot and Electronic Voting". *7th International Meeting of the Society for Social Choice and Welfare*, Osaka, July

Deibert, Ronald J. (2022) "Subversion Inc: The Age of Private Espionage". *Journal of Democracy*, Volume 33, Number 2, pp. 28-44.

del Pino, Rafaël, Lyubashevsky, Vadim, Neven, Gregory and Seiler, Gregor (2017). "Practical Quantum-Safe Voting from Lattices". *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (CCS '17). Association for Computing Machinery, New York, NY, USA, 1565–1581.

DeNardis, Laura (2013). The Emerging Field of Internet Governance. Dutton, William H. (ed.) *The Oxford Handbook of Internet Studies*. Oxford, United Kingdom: Oxford University Press.

De Vergottini, Giuseppe (2005) *Derecho Constitucional Comparado*. Buenos Aires, Argentina: Editorial Universidad.

Drechsler, Wolfgang (2003) "The Estonian E-Voting Laws Discourse: Paradigmatic Benchmarking for Central and Eastern Europe."

Drechsler, Wolfgang and Madise, Ülle (2002) "E-voting in Estonia". *TRAMES*, 6(56/61), 3, p. 234-244.

Drechsler, Wolfgang and Madise, Ülle (2004) "Electronic Voting in Estonia". Kersting, Norbert and Baldersheim, Harald (eds) *Electronic Voting and Democracy: A Comparative Analysis*. Basingstoke: Palgrave Macmillan, p. 97-108.

Driza Maurer, Ardita (2013) *Report on the possible update of Rec(2004)11 of the Council of Europe on legal, operational and technical standards for e-voting*, Council of Europe.

Driza Maurer, Ardita (2014) "Ten Years Council of Europe Rec(2004)11. Lessons learned and outlooj". Krimmer, Robert and Volkamer, Melanie (Eds.) *Proceedings of Electronic Voting 2014 (EVOTE2014)*, TUT Press, Tallinn, p. 111-117

Driza Maurer, Ardita (2015) *Report on the Scope and Format of the Update of Rec(2004)11*, Council of Europe.

Driza Maurer, Ardita (2016a) "Internet voting and federalism: the Swiss case". Barrat, Jordi (coord.) *El voto electrónico y sus dimensiones jurídicas: entre la ingenua complacencia y el rechazo precipitado*. Madrid, Spain: Iustel, pp. 259-301

Driza Maurer, Ardita (2016b) "Update of the Council of Europe Recommendation on Legal, Operational and Technical Standards for E-Voting – a Legal Perspective". *Tagungsband IRIS (Internationales Rechtsinformatik Symposion*), Universität Salzburg.

Driza Maurer, Ardita (2017) "Updated European Standards for E-voting". Krimmer, Robert; Volkamer, Melanie; Braun Binder, Nadja; Kersting, Norbert; Pereira, Olivier and Schürmann, Carsten (eds) *Electronic Voting. E-Vote-ID 2017*. Lecture Notes in Computer Science, vol 10615. Springer, Cham, pp. 146-162.

Driza Maurer, Ardita (2019) "The Swiss Post/Scytl Transparency Exercise and Its Possible Impact on Internet Voting Regulation". Krimmer, Robert; Volkamer, Melanie; Cortier, Veronique; Beckert, Bernhard; Küsters, Ralf; Serdült, Uwe and Duenas-Cid, David (eds.) *Fourth International Joint Conference on Electronic Voting E-Vote-ID 2019 : 1-4 October 2019.* Co-organized by the Tallinn University of Technology, Karlsruhe Institute of Technology, E-Voting.CC, Gesellschaft für Informatik and Kastel, TalTech Press, pp. 122-138.

Easterbrook, Frank H. (1996) "Cyberspace and the Law of the Horse". *University of Chicago Legal Forum*, 207, pp. 207-216.

Elklit, Jørgen (2018) "Is Voting in Sweden Secret? An Illustration of the Challenges in Reaching Electoral Integrity". *IPSA/ASIP 25th World Congress of Political Science*, Brisbane, Australia, July 21-25.

Elster, Jon (2015) "Introduction". Elster, Jon (ed.) *Secrecy and Publicity in Votes and Debates*. New York, USA: Cambridge University Press, pp. 1-14.

Engelen, Bart and Nys, Thomas R.V. (2013) "Against the secret ballot: Toward a new proposal for open voting". *Acta Politica*, 48(4), pp. 490-507.

Enguehard, Chantal (2010) "Introduction à l'analyse de chimères technologiques, le cas du vote électronique"- *Cahiers Droit, Sciences & Technologies*, 3, p. 261-280.

Essex, Aleksander and Goodman, Nicole (2020) "Protecting Electoral Integrity in the Digital Age: Developing E-Voting Regulations in Canada". *Election Law Journal*, Vol 19, Number 2, p. 162-179

European Committee on Democracy and Governance (2021a) *Replies to the questionnaire on member States' experience in relation to e-voting and recommendation CM/Rec (2017)5 of the Committee of Ministers on standards for e-voting*.

European Committee on Democracy and Governance (2021b) *Review meeting on the implementation of Recommendation CM/Rec(2017)5 on standards for e-voting*.

Farzaliyev, Valeh, Willmenson, Jan, Kaasik, Jaan Kristjan (2021) "Improved Lattice-Based Mix-Nets for Electronic Voting". *Cryptology ePrint Archive*.

Ferejohn, John (2015): "Secret Votes and Secret Talk". Elster, Jon (ed.) *Secrecy and Publicity in Votes and Debates*. New York, USA: Cambridge University Press, pp. 230-247

Floridi, Luciano (2007) "A Look into the Future Impact of ICT on Our Lives". *The Information Society*, vol. 23, Issue 1, pp. 59-64.

Galindo, David, Guasch, Sandra and Puiggalí, Jordi (2015) "Neuchâtel's Cast-as-Intended Verification Mechanism". Haenni, Rolf; Koenig, Reto E. and Wikström, Douglas (eds.) *Proceedings of the International Conference on E-Voting and Identity (VoteID)*. Springer-Verlag, Cham, Switzerland, pp. 3-18.

Garrigou, Alain (1988) "Le secret de l'isoloir". *Actes de la recherche en sciences sociales*, Vol. 71-72, pp. 22-45.

Gerber, Alan S.; Huber, Gregory A.; Doherty, David, and Dowling, Conor M. (2013) "Is There a Secret Ballot? Ballot Secrecy Perceptions and Their Implications for Voting Behaviour". *British Journal of Political Science*, 43(1), pp. 77-102

Germann, Micha and Serdült, Uwe (2017) "Internet voting and turnout: Evidence from Switzerland". *Electoral Studies*, 47, pp. 1-2.

Gharadaghy, Rojan and Volkamer Melanie (2010) "Verifiability in Electronic Voting - Explanations for Non- Security Experts". Krimmer, Robert and Grimm Rüdiger (eds.): *Proceedings of the 4th Conference on Electronic Voting*. LNI GI Series, Bregenz, Austria, July 21-24, pp 151-162.

Gibson, J. Paul; Krimmer, Robert; Teague, Vanessa, and Pomares, Julia (2016) "A review of E-voting: the past, present and future". *Ann. Telecommun*. 71, pp. 279–286.

Gingerich, Daniel (2013) "Can Institutions Cure Clientelism?: Assessing the Impact of the Australian Ballot in Brazil". *IDB Publications (Working Papers)*, 4602, Inter-American Development Bank.

Goldsmith, Jack L. (1998) "Against Cyberanarchy". *The University of Chicago Law Review*, vol. 65, no. 4, pp. 1199–250.

Goodman, Nicole J. (2014) "Internet Voting in a Local Election in Canada". Grofman, Bernard; Trechsel, Alexander H., and Franklin, Mark (eds.) *The Internet and Democracy in Global Perspective. Voters, Candidates, Parties, and Social Movements*. Studies in Public Choice, vol 31. Springer, Cham, pp. 7-24.

Heiberg, Sven, Krips, Kristjan, and Willemson, Jan (2020) "Planning the next steps for Estonian Internet voting". Krimmer, Robert; Volkamer, Melanie; Beckert, Bernhard; Driza Maurer, Ardita; Duenas-Cid, David; Glondu, Stéphane; Krivonosova, Iuliia; Kulyk, Oksana; Küsters, Ralf; Martin-Rozumilowicz, Beata; Roenne, Peter; Solvak, Mihkel; Spycher, Oliver (eds.) *Fifth International Joint Conference on Electronic Voting E-Vote-ID 2020 : 6-9 October 2020 : Proceedings*. Co-organized by the Tallinn University of Technology, University of Tartu, Karlsruhe Institute of Technology, E-Voting.CC, Gesellschaft für Informatik and Kastel, TalTech Press, pp 82-97.

Hill, Richard (2015) "Challenging an E-voting System in Court". In Haenni, Rolf; Koenig, Reto E. and Wikström, Douglas (eds) *E-Voting and Identity. Vote-ID 2015*. Lecture Notes in Computer Science, vol 9269. Springer, Cham. pp. 161-171.

Hill, Richard (2016) "E-voting and the Law. Issues, Solutions, and a Challenging Question". In Krimmer, Robert; Volkamer, Melanie; Barrat, Jordi; Benaloh, Josh; Goodman, Nicole; Ryan, Peter Y.A.; Spycher, Oliver; Teague, Vanessa and Wenda, Gregor (eds.) *The International Conference on Electronic Voting E-Vote-ID 2016:* 18–21 October. Co-organized by Tallinn University of Technology, Technische Universität Darmstadt, Karlstad University, Gesellschaft für Informatik and E-Voting.CC. pp. 123-138

Hoofnagle, Chris Jay and Garfinkel, Simon (2022). *Law and Policy for the Quantum Age*. Cambridge: Cambridge University Press.

Horwitz, Daniel (2015) "A Picture's Worth a Thousand Words: Why Ballot Selfies Are Protected by the First Amendment". *18 SMU Sci. & Tech. L. Rev. 247*.

International IDEA (2014) Int*ernational Obligations for Elections. Guidelines for Legal Frameworks*. Stockholm, Sweden: International Instititute for Democracy and Electoral Assistance.

Jackson, Vicki C. (2010) "Methodological Challenges in Comparative Constitutional Law". *Georgetown Public Law and Legal Theory*, Research Paper No. 11—11, pp. 319-326.

Jackson, Vicki C. (2012) "Comparative Constitutional Law: Methodologies". Rosenfeld, Michel and Sajó, András (eds.) *The Oxford Handbook of Comparative Constitutional Law*. Oxford, United Kingdom: Oxford University Press.

Jaffrelot, Cristophe (2006): "Voting in India: Electoral Symbols, the Party System and the Collective Citizen". Bertrand, Romain: Briquet, Jean-Louis and Pels, Peter (eds) *The Hidden History of the Secret Ballot*. Bloomington and Indianapolis, USA: Indiana University Press, p. 78-99

Johnson, James and Orr, Susan (1996) *Should Secret Voting Be Mandatory?* Cambridge, UK: Polity Press.

Johnson, David R. and Post, David (1996) "Law and Borders: The Rise of Law in Cyberspace". *Stanford Law Review*, vol. 48, no. 5, pp. 1367–402

Jones, Douglas W. (2004) "The European 2004 Draft E-voting Standard: Some critical Comments". Part of the Voting and Elections web pages.

Jones, Douglas W. and Simons, Barbara (2012) *Broken Ballots: Will Your Vote Count?* California, United States: CSLI Publications.

Kam, Cristopher (2017) "The Secret Ballot and the Market for Voters at the 19th-Century British Elections". *Comparative Political Studies*, 50(5), pp. 594-635

Kasara, Kimuli and Mares, Isabela (2017): "Unfinished Business: The Democratisation of Electoral Practices in Britain and Germany". *Comparative Political Studies*, 50(5), pp. 636-664

Koitmäe, Arne; Willemson, Jan and Vinkel, Priit (2021) "Vote Secrecy and Voter Feedback in Remote Voting – Can We Have Both?" Krimmer, Robert; Volkamer, Melanie; Duenas-Cid, David; Kulyk, Oksana; Rønne, Peter; Solvak, Mihkel and Germann, Micha (eds) *Electronic Voting. E-Vote-ID 2021*. Lecture Notes in Computer Science, vol 12900. Springer, Cham, pp. 140-154.

Krimmer, Robert (2012) *The Evolution of E-voting: Why Voting Technology is Used and How it Affects Democracy*.

Krimmer, Robert; Triessnig, Stefan, and Volkamer, Melanie (2007) "The Development of Remote E-Voting Around the World: A Review of Roads and Directions". In: Alkassar, Ammar, and Volkamer, Melanie (eds) *E-Voting and Identity. Vote-ID 2007*. Lecture Notes in Computer Science, vol 4896. Springer, Berlin, Heidelberg, pp. 1-7.

Krimmer, Robert, and Volkamer, Melanie. (2005) "Bits or Paper? Comparing Remote Electronic Voting to Postal Voting". *Electronic Government - Workshop and Poster Proceedings of the Fourth International EGOV Conference 2005*, August 22-26, Copenhagen, Denmark. pp., 225-232.

Krimmer, Robert; Volkamer, Melanie and Duenas-Cid, David (2019) "E-Voting – An Overview of the Development in the Past 15 Years and Current Discussions". Krimmer, Robert; Volkamer, Melanie; Cortier, Veronique; Beckert, Bernhard; Küsters, Ralf; Serdült, Uwe and Duenas-Cid, David (eds.) *Electronic Voting. E-Vote-ID 2019.* Lecture Notes in Computer Science, vol 11759, pp. 1-13.

Krips, Kristjan and Willemson, Jan (2019) "On Practical Aspects of Coercion-Resistant Remote Voting Systems". Krimmer, Robert; Volkamer, Melanie; Cortier, Veronique; Beckert, Bernhard; Küsters, Ralf; Serdült, Uwe and Duenas-Cid, David (eds.) *Electronic Voting. E-Vote-ID 2019.* Lecture Notes in Computer Science, vol 11759, pp. 216-232.

Krisch, Nico (2011) *Beyond Constitutionalism: The Pluralist Structure of Postnational Law*. Oxford, United Kingdom: Oxford University Press.

Kuo, Didi and Teorell, Jan (2017) "Illicit Tactics as Substitutes: Election Fraud, Ballot Reform, and Contested Elections in the United States, 1860-1930". *Comparative Political Studies*, 50(5), pp. 665-696

Kuoni, Beat (2015) "E-Voting Case Law: A Swiss Perspective". Driza Maurer, Ardita and Barrat, Jordi (eds.) *E-Voting Case Law. A Comparative Analysis.* Surrey, England: Ashgate, p. 197-214

Lécuyer, Yannick (2014) *Le droit à des élections libres*. Strasbourg: Council of Europe.

Leiser, Mark (2016) "The problem with 'dots': questioning the role of rationality in the online environment". *International Review of Law, Computers & Technology*, 30:3, pp 191-210.

Lendon, J. E. (2001) "Voting by Shouting in Sparta". Tylawsky, E. and Weiss, C. (eds) *Essays in Honor of Gordon Williams: Twenty-Five Years at Yale*, pp. 169-175.

Lessig, Lawrence (1999) "The Law of the Horse: What Cyberlaw Might Teach". *Harvard Law Review*, 113, pp. 501-546.

Lessig, Lawrence (2006) *Code. Version 2.0.* New York: Basic Books.

Levy, Steven (2001) *Crypto. How the code revels beat the government– saving privacy in the digital age.* New York: Penguin Books.

Licht, Nathan; Duenas-Cid, David; Krivonosova, Iuliia, and Krimmer, Robert (2021) "To i-vote or Not to i-vote: Drivers and Barriers to the Implementation of Internet Voting". Krimmer, Robert; Volkamer, Melanie; Duenas-Cid, David; Kulyk, Oksana; Rønne, Peter; Solvak, Mihkel and Germann, Micha (eds) *Electronic Voting. E-Vote-ID 2021*. Lecture Notes in Computer Science, vol 12900. Springer, Cham, pp. 91-105.

Loeber, Leontine (2014): "E-voting in the Netherlands; Past, Current, Future?". Krimmer, Robert and Volkamer, Melanie (eds.) *Proceedings of Electronic Voting 2014 (EVOTE2014)*. TUT Press, Tallinn, p. 43 – 46.

Loeber, Leontine (2017) "Legislating for E-Enabled Elections: Dilemmas and Concerns for the Legislator". Krimmer, Robert; Volkamer, Melanie; Barrat, Jordi; Benaloh, Josh; Goodman, Nicole; Ryan, Peter Y. A. and Teague, Vanessa (eds) *Electronic Voting. E-Vote-ID 2016*. Lecture Notes in Computer Science, vol 10141. Springer, Cham. pp., 203-217.

MacCormick, Neil (1993) "Beyond the Sovereign StateIn *Modern Law Review*, Volume 56, Issue 1, pp. 1-18.

Madise, Ülle (2007) *Elections, Political Parties, and Legislative Performance in Estonia: Institutional Choices from the Return to Independence to the Rise of E-Democracy*. Tallin University of Technology Doctoral Theses. Thesis on Humanities and Social Sciences, No. 16

Madise, Ülle and Martens, Tarvi (2006) "E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world". Krimmer, Robert (ed.) *Electronic Voting 2006. 2nd International Workshop co-organized by the Council of Europe, ESF TED, IFIP WG 8.5 and E-Voting.CC.* Bregenz, Austria: GIS, p. 15-26

Madise, Ülle and Vinkel, Priit (2011) "Constitutionality of Remote Internet Voting: The Estonian Perspective". *Juridica International. Iuridicum Foundation*, Vol. 18, p. 4-16

Madise, Ülle and Vinkel, Priit (2015) "A Juidicial Approach to Internet Voting in Estonia". Driza Maurer, Ardita and Barrat, Jordi (eds.) *E-Voting Case Law. A Comparative Analysis.* Surrey, England: Ashgate, p. 105-128

Madise, Ülle; Vinkel, Priit and Maaten, Epp (2006) *Internet Voting at the Elections of Local Government Councils on October 2005*: Report. Tallin: Estonian National Electoral Committee.

Maley, Michael (2018) "The Secret Ballot in Australia: What does it mean and how secret is it really?". *IPSA/ASIP 25th World Congress of Political Science*, Brisbane, Australia, July 21-25

Mandel, Gregory N. (2017) "Legal Evolution in Response to Technological Change". Brownsword, Roger; Scotford, Eloise and Yeung, Karen (eds.) *The Oxford Handbook of Law, Regulation and Technology*. Oxford, United Kingdom: Oxford University Press.

Manin, Bernard (2015) "Why Open Voting in General Elections is Undesirable". Elster, Jon (ed.) *Secrecy and Publicity in Votes and Debates*. New York, USA: Cambridge University Press, pp. 209-214

Mares, Isabela (2015) *From Open Secrets to Secret Voting: Democratic Electoral Reforms and Voter Autonomy* (Cambridge Studies in Comparative Politics). Cambridge: Cambridge University Press.

Martin, Keith (2020) *Cryptography*. *The Key to Digital Security, How it Works, and Why it Matters.* New York: W.W. Norton & Company.

McKenna, Mark (2001) "Building a 'closet of prayer' in the new world: The story of the 'Australian Ballot'". Sawer, Marian (ed.) *Elections: Full, Free & Fair*. Sydney, Australia: The Federation Press, pp. 45-62

Meagher, Sutton (2009) "When Personal Computers are Transformed into Ballot Boxes: How Internet Elections in Estonia Comply with the United Nations International Covenant on Civil and Political Rights". *American University International Law Review*, 23(2), p. 349-386

Mendez, Fernando and Serdült, Uwe (2014) "From Initial Idea to Piecemeal Implementation: Switzerland's First Decade of Internet Voting Reviewed". Zissis, Dimitrios and Lekkas, Dimitrios (eds): *Design, Development, and Use of Secure Electronic Voting Systems*.

Mendez, Fernando and Serdült, Uwe (2017) "What drives fidelity to internet voting? Evidence from the roll–out of internet voting in Switzerland". *Government Information Quarterly*, Volume 34, Issue 3, pp. 511-523.

Moreso, Josep Joan and Vilajosana Rubio, Josep M. (2004) *Introducción a la teoría del derecho*. Madrid, España: Marcial Pons, Ediciones Jurídicas y Sociales.

Murray, Andrew D. (2011a) "Nodes and Gravity in Virtual Space". *Legisprudence*, 5:2, pp. 195-221 .

Murray, Andrew D. (2011b) "Internet regulation". Levi-Faur, David (ed.) *Handbook on the Politics of Regulation.* Cheltenham, United Kingdom and Massachusetts, USA: Edward Elgard Publishing Ltd, pp. 267-279.

Peters, Anne (2007) "The Globalization of State Constitutions". Nijman, Janne E. and Nollkaemper, André (eds.) *New Perspectives on the Divide Between National and International Law.* Oxford, United Kingdom: Oxford University Press, p. 251-308.

Petitpas, Adrien; Jaquet, Julien M. and Sciarini, Pascal (2021) "Does E-Voting matter for turnout, and to whom?". *Electoral Studies*, Volume 71.

Preuss, Ulrich K. (1995) "Patterns of Constitutional Evolution and Change". Hesse, Joachim Jens and Johnson, Nevil (eds.) *Constitutional Policy and Changes in Europe*. Oxford, United Kingdom: Oxford University Press.

Przeworski, Adam (2015) "Suffrage and Voting Secrecy in General Elections". Elster, Jon (ed.) *Secrecy and Publicity in Votes and Debates*. New York, USA: Cambridge University Press, pp. 209-214.

Puiggalí, Jordi (2019) "Implementing a public security scrutiny of an online voting system: the Swiss experience". Krimmer, Robert; Volkamer, Melanie; Cortier, Veronique;

Beckert, Bernhard; Küsters, Ralf; Serdült, Uwe and Duenas-Cid, David (eds.) *Fourth International Joint Conference on Electronic Voting E-Vote-ID 2019 : 1-4 October 2019.* Co-organized by the Tallinn University of Technology, Karlsruhe Institute of Technology, E-Voting.CC, Gesellschaft für Informatik and Kastel, TalTech Press, pp. 311-326.

Puiggalí, Jordi and Cucurull, Jordi (2016) Distributed Immutabilization of Secure Logs. Barthe G., Markatos E., Samarati P. (eds) *Security and Trust Management. STM 2016*. Lecture Notes in Computer Science, vol 9871. Springer, Cham.

Puiggalí, Jordi; Cucurull, Jordi; Guasch, Sandra and Krimmer, Robert (2017) "Verifiability Experiences in Government Online Voting Systems". Krimmer, Robert; Volkamer, Melanie; Braun Binder, Nadja; Kersting, Norbert; Pereira, Oliver; Schürmann, Carsten (eds) *Electronic Voting. E-Vote-ID 2017*. Lecture Notes in Computer Science, vol 10615. Springer, Cham.

Puiggalí-Allepuz, Jordi and Guasch-Castelló, Sandra (2010) "Privacy and Anonymity Management in Electronic Voting". *UPGRADE. The European Journal for the Informatics Professional*. Vol XI, issue No. 1, pp. 49-65.

Puiggalí, Jordi and Rodríguez-Pérez, Adrià (2018) "Defining a national framework for online voting and meeting its requirements: the Swiss experience". Krimmer, Robert; Volkamer, Melanie; Cortier, Véronique; Duenas-Cid, David; Goré, Rajeev; Hapsara, Manik; Koenig, Reto; Martin, Steven; McDermott, Ronan; Roenne, Peter; Serdült, Uwe and Truderung, Tomasz (eds.) *Third International Joint Conference on Electronic Voting E-Vote-ID 2018:* 2–5 October. pp. 82-97.

Rambaud, Romain (2019) *Droit des élections et des référendums politiques*. Issy-les-Moulineaux, France: L.G.D.J

Reniu Vilamala, Josep Maria (2016) "Consideraciones sociopolíticas para los proyectos de voto electrónico". Barrat, Jordi (coord.) *El voto electrónico y sus dimensiones jurídicas: entre la ingenua complacencia y el rechazo precipitado*. Madrid, Spain: Iustel, pp. 57-82.

Rodríguez-Pérez, Adrià (2020) "My Vote, My (Personal) Data: Remote Electronic Voting and the General Data Protection Regulation". Krimmer, Robert; Volkamer, Melanie; Beckert, Bernhard; Driza Maurer, Ardita; Duenas-Cid, David; Glondu, Stéphane; Krivonosova, Iuliia; Kulyk, Oksana; Küsters, Ralf; Martin-Rozumilowicz, Beata; Roenne, Peter; Solvak, Mihkel; Spycher, Oliver (eds.) (eds) *Electronic Voting. E-Vote-ID 2020*. Lecture Notes in Computer Science, vol 12455. Springer, Cham. pp. 167-182.

Rodríguez-Pérez, Adrià (2021) "Entre la libertad de expresión y el secreto del voto: el caso Magyar Kétfarkú Kutya Párt vs. Hungría [2019] del Tribunal Edh". Ríos Vega, Luis Efrén and Spigno, Irene (dirs.) Esquivel Alonso, Yessica and Pérez Moneo, Miguel (eds.) *Estudios de casos líderes europeos. Vol. XXIII Las elecciones libres en la doctrina de Estrasburgo.* Ciudad de México, México: Tirant lo Blanch, pp. 95-129.

Rodríguez-Pérez, Adrià (forthcoming) "La dimensión tecnológica de las normas globales: el concurso del NIST estadounidense para la estandarización de algoritmos criptográficos post-cuánticos". García, Caterina; Pareja, Pablo; Rodrigo, Ángel J. (eds.) *La Creación de Normas Globales: entre el cosmopolitismo soft y el resurgir de Westfalia*.

Rodríguez-Pérez, Adrià; Cucurull, Jordi; and Puiggalí, Jordi (2022) "Voter authentication in remote electronic voting governmental experiences: requirements and practices". *EGOV2022 – IFIP EGOV-CeDEM-EPART 2022*.

Rodríguez-Pérez, Adrià and Puiggalí, Jordi (2019) "Internet voting for political parties: comparing scytl's experiences". Barrat i Esteve, Jordi and Pérez-Moneo, Miguel (ed. lit.) *La digitalización de los partidos políticos y el uso del voto electrónico*. Cizur Menor, España: Aranzadi Thomson Reuters, pp. 315-338.

Rodríguez-Pérez, Adrià and Puiggalí, Jordi (2020) "Con el voto (telemático) no es suficiente: herramientas digitales para el funcionamiento remoto de parlamentos y asambleas". Reniu Vilamala, Josep Maria and Meseguer Sánchez, Juan Victor (dir.) *¿Política confinada? Nuevas tecnologías y toma de decisiones en un contexto de pandemia*. Cizur Menor, España: Aranzadi Thomson Reuters, pp. 195-215.

Rodríguez-Pérez, Adrià; Valletbó-Montfort, Pol and Cucurull, Jordi (2019) "Bringing transparency and trust to elections: using blockchains for the transmission and tabulation of results". Soumaya, Ben- Dhaou; Carter, Lemuria and Gregory Mark (eds.) *ICEGOV2019: Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance*, pp. 46-55.

Rokkan, Stein (1961) "Mass Suffrage, Secret Voting and Political Participation". *European Journal of Sociology*, 2(1), pp. 132-152.

Rosenfeld, Michel (2001) "The Rule of Law and the Legitimacy of Constitutional Democracy". *Southern California Law Review*, Vol. 74, Issue 5 (July), pp. 1307-1352

Rosenfeld, Michel and Sajó, András (2012) "Introduction". Rosenfeld, Michel and Sajó, András (eds.) *The Oxford Handbook of Comparative Constitutional Law*. Oxford, United Kingdom: Oxford University Press.

Saglie, Jo and Bock Segaard, Signe (2016) "Internet voting and the secret ballot in Norway: principles and popular understandings". J*ournal of Elections, Public Opinion and Parties*, 26:2, pp. 155-169

Sadurski, Wojciech (2008) *Equality and Legitimacy*. Oxford, United Kingdom: Oxford University Press.

Schabas, William A. (2015) *The European Convention on Human Rights. A Commentary*. Oxford, United Kingdom: Oxford University Press.

Schwartzberg, Melissa (2010) "Shouts, Murmurs and Votes: Acclamation and Aggregation in Ancient Greece". *The Journal of Political Philosophy*, 18(4), pp. 448-468

Scott, Colin (2004). Regulation in the age of governance: the rise of the post-regulatory state. Jordana, Jacint and Levi-Faur, David (eds.). *The Politics of Regulation. Institutions and Regulatory Reforms for the Age of Governance*. Cheltenham, United Kingdom: Edward Elgar Publishing Limited, pp. 145-175

Serdült, Uwe; Germann, Micha; Mendez, Fernando; Portenier, Alicia and Wellig Christoph (2015) "Fifteen Years of Internet Voting in Switzerland: History, Governance and Use". Teran, Luis and Meier, Andreas (eds.) *ICEDEG 2015: Second International Conference on eDemocracy & eGovernment*.

Silverman, Jacob (2016) *Terms of Service: Social Media and the Price of Constant Connection*. New York, USA: Harper Perennial.

Singh, Simon (1999) *The Code Book. The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Nueva York: Anchor Books.

Solvak, Mihkel and Vassil, Kristjan (2016) *E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005-2015)*. Tartu, Estonia: Johan Skytte Institute of Political Studies, University of Tartu, in Cooperation with Estonian National Electoral Committee.

Sommer, Joseph H. (2000) "Against Cyberlaw". *Berkeley Technology Law Journal*, 15(3), pp. 1146-1232.

Springall, Drew; Finkenauer, Travis; Durumeric, Zakir; Kitcat, Jason; Hursti, Harri; MacAlpine, Margaret; Halderman, J. Alex (2014) "Security Analysis of the Estonian Internet Voting System". *Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS '14)*, November.

Staveley, Erbert Samuel (1977) *Greek and Roman Voting and Elections*. Ithaca, New York: Cornell University Press.

Stein, Robert and Wenda, Gregor (2014) "The Council of Europe and e-voting: History and impact of Rec(2004)11". Krimmer, Robert and Volkamer, Melanie (Eds.) *Proceedings of Electronic Voting 2014 (EVOTE2014)*, TUT Press, Tallinn, p. 105-110.

Tanchoux, Philippe (2004) *Les Procédures électorales en France de la fin de l'Ancien Régime à la Première Guerre mondiale*. Paris, France: Comité des travaux historiques et scientifiques (CTHS.- Histoire).

Teorell, Jan; Ziblatt, Daniel and Lehoucq, Fabrice (2016) "An Introduction to Special Issue: The Causes and Consequences of Secret Ballot Reform". *Comparative Political Studies*, 50(5), pp. 531-554.

Trechsel, Alexander H. (dir.), Schwerdt, Guido; Breuer, Fabian; Alvarez, Michael and Hall, Thad (2007) *Internet voting in the March 2007 Parliamentary Elections in Estonia. Report for the Council of Europe*.

Úbeda de Torres, Amaya (2017) "Between soft and hard law standards: the contribution of the Venice Commission in the electoral field". In Dickson, Brice and Hardman, Helen (eds) *Electoral Rights in Europe. Advances and Challenges*. London and New York: Routledge.

Van Reybrouck, David (2016) *Against Elections. The Case for Democracy*. London, United Kingdom: The Bodley Head.

Vassil, Kristjan; Solvak, Mihkel; Vinkel, Priit; Trechsel, Alexander H. and Alvarez, R. Michael (2016) "The diffusion of internet voting. Usage patterns of internet voting in Estonia between 2005 and 2015". *Government Information Quarterly*, Volume 33, Issue 3, pp. 453-459.

Vegas, Carlos and Barrat, Jordi (2016) "Overview of Current State of E-Voting Worldwide". Hao, Feng and Ryan, Peter Y. A. (eds.) *Real-World Electronic Voting. Design, Analysis and Deployment*. New York, USA: Auerbach Publications, pp. 51-75.

Véliz, Carrisa (2020) *Privacy is Power. Why and How You Should Take Back Control of Your Data*. London, United Kingdom: Bantam Press.

Vermeule, Adrian (2015): "Open-Secret Voting". Elster, Jon (ed.) *Secrecy and Publicity in Votes and Debates*. New York, USA: Cambridge University Press, pp. 215-229.

Vinkel, Priit (2015) *Remote Electronic Voting in Estonia: Legality, Impact and Confidence*. Tallin University of Technology Doctoral Theses. Series I: Social Sciences, No. 24.

Vinkel, Priit (2016) "Historical developments and legal aspects". Solvak, Mihkel and Vassil, Kristjan, *E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005-2015)*. Tartu, Estonia: Johan Skytte Institute of Political Studies, University of Tartu, in Cooperation with Estonian National Electoral Committee, p. 38-56.

Vinkel, Priit and Krimmer, Robert (2017) "The How and Why to Internet Voting an Attempt to Explain E-Stonia". Krimmer, Robert; Volkamer, Melanie; Barrat, Jordi; Benaloh, Josh; Goodman, Nicole; Ryan, Peter Y. A. and Teague, Vanessa (eds) *Electronic Voting. E-Vote-ID 2016*. Lecture Notes in Computer Science, vol 10141. Springer, Cham. pp., 178-191.

Vollan, Kåre (2006) "Voting in uncontrolled environment and the secrecy of the vote". Krimmer, Robert (Hrsg.), *Electronic Voting 2006 – 2nd International Workshop*, Co-organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting.CC. Bonn: Gesellschaft für Informatik e.V.. (S. 155-169).

Wagner, Rebecca (2020) *Responding to COVID-19 with 100 per cent Postal Voting: Local Elections in Bavaria, Germany*. Stockholm, Sweden: International Institute for Democracy and Electoral Assistance.

Waldron, Jeremy (2006) "The Core of the Case against Judicial Review". *The Yale Law Journal*, vol. 115, no. 6, pp. 1346–1406.

Watt, Bob (2003) "Human rights and remote voting by electronic means". *Representation*, 39:3, pp. 197-208.

Zuboff, Shoshana (2019) *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*. London, United Kingdom: Profile Books.

Zumbansen, Peer (2012) "Defining the Space of Transnational Law: Legal Theory, Global Governance and Legal Pluralism". Handl, Gunther; Zekoll, Joachim, and Zumbansen, Peer (eds.) *Beyond Territoriality*. Leiden, The Netherlands: Brill | Nijhoff, p. 53-86.

Press and media

Manancourt, Vincent (2022) "Hack of Spanish PM's phone deepens Europe's spyware crisis". *Politico*, online, May 2. Available at: <https://www.politico.eu/article/pegasus-hacking-spyware-spain-government-prime-minister-pedro-sanchez-margarita-robles-digital-espionage-crisis/> [retrieved: 6 May 2022]

Nichols, Shan (2021) "Pegasus spyware discovered on U.K. government networks". *Techtarget*, online, 18 April. Available at: <https://www.techtarget.com/searchsecurity/news/252516052/Pegasus-spyware-discovered-UK-government-networks> [retrieved: 6 May 2022]

Henley, Jon and Kirchgaessner, Stephanie (2021) "Spyware 'found on phones of five French cabinet members'". *The Guardian*, online, 23 September. Available at: <https://www.theguardian.com/news/2021/sep/23/spyware-found-on-phones-of-five-french-cabinet-members> [retrieved: 6 May 2022]

Rodríguez-Pérez, Adrià (2021) "Blockchain for online voting? The fundamentals". EDGE Elections, online, 3 December. Available at: <https://medium.com/edge-elections/blockchain-for-online-voting-ffd1e56eeb92> [retrieved: 6 May 2022]

Sánchez Sánchez, María (2015) "'No iba a votar en las elecciones y te cedo mi voto': la campaña que une a emigrados y abstencionistas". *El País*, online, 11 December. Available at: <https://verne.elpais.com/verne/2015/11/28/articulo/1448735959_359242.html> [retrieved: 6 May 2022]

Satter, Raphael and Bing, Cristopher (2022) "Exclusive: Senior EU officials were targeted with Israeli spyware". *Reuters*, online, April 11. Available at: <https://www.reuters.com/technology/exclusive-senior-eu-officials-were-targeted-with-israeli-spyware-sources-2022-04-11/> [retrieved: 6 May 2022]

Schneier, Bruce (1997) "Why Cryptography Is Harder Than It Looks". *Schenier on Security*.

Zilber, Neri (2018) "The Rise of the Cyber-Mercenaries". *Foreign Policy,* online, 31 August. Available at: <https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/> [retrieved: 6 May 2022]