FRAUD AGAINST INDIVIDUALS IN THE INTERNET ERA: TRENDS, VICTIMISATION, IMPACT AND REPORTING

Steven Kemp

Universitat de Girona

DOCTORAL THESIS

FRAUD AGAINST INDIVIDUALS IN THE INTERNET ERA: TRENDS, VICTIMISATION, IMPACT AND REPORTING

Steven Kemp

2020

-blank page-

Universitat de Girona

DOCTORAL THESIS

FRAUD AGAINST INDIVIDUALS IN THE INTERNET ERA: TRENDS, VICTIMISATION, IMPACT AND REPORTING

Steven Kemp

2020

DOCTORAL PROGRAMME IN LAW, ECONOMICS AND BUSINESS

Directors:

Dr Daniel Varona Gómez

Dr Fernando Miró-Llinares

Tutor: Dr Juan Gonzalo Escobar Marulanda

A doctoral thesis submitted for the degree of Doctor at the University of Girona

-blank page-

This doctoral thesis by compendium of publications is comprised of the following articles:

- Kemp, S., Miró-Llinares, F., & Moneva, A. (2020). The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research*. https://doi.org/10.1007/s10610-020-09439-2

The European Journal on Criminal Policy and Research is currently ranked in the first quartile of Scopus with an H index score of 30 and SJR indicator of 0.535. This article has three external citations (non-self-citations) at the time of thesis submission.

- Kemp, S., & Moneva, A. (2020). Fraude online vs. offline: Factores predictores de victimización y su impacto. *InDret*, 1.2020. pp. 424-444. Available at: https://indret.com/fraude-online-vs-offline-factores-predictores-de-victimizacion-y-su-impacto/

InDret currently has a Latindex score of 34/36.

- Kemp, S. (2020). Fraud reporting in Catalonia in the Internet era: Determinants and motives. *European Journal of Criminology*.

The European Journal of Criminology is currently ranked in the first quartile of Scopus with an H index score of 48 and SJR indicator of 1.208.

Universitat de Girona

El Dr. Daniel Varona Gómez, de la Universitat de Girona,

DECLARO:

Que la tesi doctoral titulada *Fraud against Individuals in the Internet Era: Trends, Victimisation, Impact and Reporting*, que presenta Steven Kemp en format de compendi de publicacions de primer autor o autor únic, ha estat realitzada sota la meva direcció, i que la considero idònia quant a forma i contingut per tal d'optar a l'obtenció del títol de doctor.

I, perquè així consti i tingui els efectes oportuns, signo aquest document.

Signatura

El Dr. Fernando Miró Llinares, de la Universidad Miguel Hernández,

DECLARO:

Que la tesi doctoral titulada *Fraud against Individuals in the Internet Era: Trends, Victimisation, Impact and Reporting*, que presenta Steven Kemp en format de compendi de publicacions de primer autor o autor únic, ha estat realitzada sota la meva direcció, i que la considero idònia quant a forma i contingut per tal d'optar a l'obtenció del títol de doctor.

I, perquè així consti i tingui els efectes oportuns, signo aquest document.

Signat:

DEDICATION

To my parents, for always being there on this roundabout academic journey that started in a very different place.

And above all to my three stars: Victoria, Aila and Marina. Motivation grows with the light it receives and I couldn’t receive more.

ACKNOWLEDGEMENTS

A PhD is hard at the best of times, but to complete it ahead of schedule, with two small children, while working full time and ending up in global pandemic is impossible without an extraordinary amount of support.

First, I do not think I could have had two better supervisors than Daniel Varona and Fernando Miró. Inspirational, supportive, dedicated and systematic, the list of positive adjectives is endless. Some co-authored research has been published, hopefully there is much more to come.

I am similarly indebted to Gonzalo Escobar, who is responsible for introducing me to criminology a decade ago and gave me the motivation and the opportunity to begin this academic journey.

Many others from the University of Girona have helped along the way as teachers or colleagues or both. Leanid Kazyrytski deserves special mention for the invaluable pragmatic advice. Maribel Narvaez, Ester Blay, Cristina Sobrino, Dolors Canals, Ignacio González, Cristina Vasilescu, Ignasi Bernat, to name but a few of those who provided assistance or encouraged me think.

I learnt much from my co-author of two of the papers in this thesis, Asier Moneva: R stats and plots, the research paper process, meticulousness, and much more. I sincerely hope to work together again soon.

And, finally, this whole process would have collapsed if it were not for the unwavering support of Victoria. The hours I dedicated were hours she dedicated. If anyone deserves a holiday, it is her (or us).

LIST OF ABBREVIATIONS

BoS	Bank of Spain
CRAN	Comprehensive R Archive Network
CSEW	Crime Survey for England and Wales
DV	Dependent Variable
ECB	European Central Bank
ESPC	Encuesta de Seguridad Pública
GH	General Hypothesis
IV	Independent Variable
IVI	Introduction, Interaction, Value
MIR	Ministerio del Interior
MO	Modus Operandi
OR	Odds Ratio
PMT	Protection Motivation Theory
RQ	Research Question
SE	Standard Error
UK	United Kingdom
US	United States
VD	Variable Dependiente
VI	Variable Independiente
VIVA	Value, Inertia, Visibility, and Accessibility

INDEX

LIST OF FIGURES

LIST OF TABLES

-blank page-

ABSTRACT

There is general consensus that a growing fraud problem exists in the digital era, but while some academic research has suggested it is the most prevalent property crime today, Spanish criminal justice statistics indicate fraud is still less frequent than theft and robbery. Research has examined how technological and societal changes could explain recent rises, and some qualitative studies have begun to explore the impact of fraud on individuals and other factors related to reporting that, in turn, may explain these inconsistencies in the estimates of its prevalence. As one of the volume crimes of the twenty-first century, many fraud research gaps still exist, especially in the Spanish context and in relation to quantitative studies. This thesis seeks to analyse the intertwined issues of trends, victimisation, impact and reporting with respect to fraud against individuals in the Internet era. Ultimately, the main objective is to produce academic knowledge that can help build an evidence base for prevention and response strategies. In addition, it is hoped that the data, methods and conclusions can provide a blueprint for future research on fraud.

The first chapters present an overview of existing fraud literature and introduce the data and methods used in this thesis. Subsequently, hypotheses regarding the interrelated issues of macro trends and individual victimisation, impact and reporting are then tested in three empirical papers that form the main body of this thesis by compendium of publications. The first of these explores macro trends and the extent of fraud underreporting to police, tying this into the extensive crime drop literature. The second study contrasts online and offline fraud in terms of victimisation correlates, impact and

the factors that may predict whether the person who suffers the fraud considers it a crime. The third study focusses on the reporting of online and offline fraud to identify and compare socio-demographic, context and crime event predictors, as well as the reasons for not reporting.

The general results show that fraud that exploits the criminogenic opportunities of digital technology is rising and that reporting is considerably lower in comparison to other property crimes in many European countries. This raises salient questions regarding policing and criminal policy. At a micro level, some contrasting predictors are found in relation to victimisation and the impact of online and offline fraud, which can extend beyond financial losses to psychological harm. Fraud reporting and the motives for not reporting are also associated with certain socio-demographic, context and crime event factors. These findings interconnect with the criminogenic characteristics of the Internet era and can help understand the previously identified macro trends as well as inform policy and practice.

RESUMEN

Existe un consenso general en cuanto a la existencia de un creciente problema de fraude en la era digital. Pero, aunque algunos estudios académicos han sugerido que es el delito contra la propiedad más frecuente hoy en día, las estadísticas del sistema penal español indican que el fraude sigue siendo menos frecuente que los hurtos y los robos. Las investigaciones académicas han examinado la forma en que los cambios tecnológicos y sociales pueden explicar los recientes aumentos, y algunos estudios cualitativos han comenzado a explorar el impacto del fraude en las personas y otros factores relacionados con la denuncia que, a su vez, pueden explicar estas incoherencias en las estimaciones de su prevalencia. Como uno de los delitos más extendidos del siglo XXI, todavía existen muchas lagunas en el estudio del fraude, especialmente en el contexto español y en relación con los estudios cuantitativos. La presente tesis trata de analizar algunas cuestiones interrelacionadas respecto a las tendencias, la victimización, el impacto y la denuncia del fraude contra las personas en la era de Internet. En última instancia, el objetivo principal es llevar a cabo investigación académica que puede ayudar a construir una base de conocimiento para las estrategias de prevención y reacción. Además, se espera que los datos, los métodos y las conclusiones puedan servir de guía para futuros estudios sobre el fraude.

En los primeros capítulos se presenta un resumen general de la bibliografía existente sobre el fraude y se introducen los datos y métodos utilizados en esta tesis. Posteriormente, en tres estudios empíricos que constituyen el cuerpo principal de esta tesis mediante

compendio de publicaciones se contrastan las hipótesis relativas a las cuestiones interrelacionadas sobre las macrotendencias del fraude y la victimización individual, el impacto y la denuncia. En el primero de estos estudios se examinan las macrotendencias y la extensión de la infradenuncia de fraude a la policía, vinculando la discusión a la amplia bibliografía sobre la disminución de la delincuencia en las últimas décadas. En el segundo estudio se contrasta el fraude en línea y offline en lo que respecta a los predictores de la victimización, el impacto y los factores que podrían predecir si la persona que sufre el fraude lo considera un delito. El tercer estudio se centra en la denuncia del fraude en línea y offline para identificar y comparar los factores predictores sociodemográficos, del contexto y del hecho delictivo, así como las razones para no denunciar.

Los resultados generales muestran que el fraude que aprovecha las oportunidades criminógenas de la tecnología digital va en aumento y que la denuncia es considerablemente menor en comparación con otros delitos contra la propiedad en distintos países europeos. Esto plantea cuestiones destacadas en relación con la policía y la política criminal. A nivel micro, se encuentran algunos predictores contrastantes en relación con la victimización y el impacto del fraude en línea y fuera de línea, que puede ir más allá de las pérdidas económicas hasta el daño psicológico. La denuncia del fraude y los motivos para no denunciarlo también se asocian a ciertos factores sociodemográficos, del contexto y del hecho delictivo. Estos resultados se interconectan con las características criminógenas de la era de Internet y pueden ayudar a comprender las macrotendencias identificadas previamente, así como a informar las políticas y la práctica.

RESUM

Hi ha un consens general pel que fa a l'existència d'un creixent problema de frau en l'era digital. Però, encara que alguns estudis acadèmics han suggerit que és el delicte contra la propietat més freqüent avui dia, les estadístiques del sistema penal espanyol indiquen que el frau segueix sent menys freqüent que els furts o els robatoris. La recerca ha examinat la forma en què els canvis tecnològics i socials poden explicar els recents augments, i alguns estudis qualitatius han començat a explorar l'impacte del frau en les persones i altres factors relacionats amb la denúncia que, subseqüentment, poden explicar aquestes incoherències en les estimacions de la seva prevalença. Com un dels delictes més estesos del segle XXI, encara hi ha moltes llacunes en l'estudi del frau, especialment en el context espanyol i en relació amb els estudis quantitatius. La present tesi tracta d'analitzar algunes qüestions interrelacionades pel que fa a les tendències, la victimització, l'impacte i la denúncia del frau contra les persones en l'era d'Internet. En última instància, l'objectiu principal és dur a terme recerca acadèmica que pot ajudar a construir una base de coneixement per a les estratègies de prevenció i resposta. A més, s'espera que les dades, mètodes i conclusions puguin proporcionar un pla per a futures investigacions sobre fraus.

En els primers capítols es presenta un resum general de la bibliografia existent sobre el frau i s'introdueixen les dades i mètodes utilitzats en aquesta tesi. Posteriorment, en tres estudis empírics que constitueixen el cos principal d'aquesta tesi mitjançant compendi de

publicacions es contrasten les hipòtesis relatives a les qüestions interrelacionades sobre les macrotendències i la victimització individual, l'impacte i la denúncia. En el primer d'aquests estudis s'examinen les macrotendències i l'extensió de la infradenuncia del frau a la policia, vinculant això a l'àmplia bibliografia sobre la disminució de la delinqüència en les últimes dècades. En el segon estudi es contrasta el frau en línia i *offline* pel que fa als predictors de la victimització, l'impacte i els factors que podrien predir si la persona que pateix el frau el considera un delicte. El tercer estudi se centra en la denúncia del frau en línia i fora de línia per identificar i comparar els factors predictors sociodemogràfics, del context i del fet delictiu, així com les raons per no denunciar.

Els resultats generals mostren que el frau que aprofita les oportunitats criminògenes de la tecnologia digital va en augment i que la denúncia és considerablement menor en comparació amb altres delictes contra la propietat en distints països europeus. Això planteja qüestions destacades en relació amb la policia i la política criminal. A nivell micro, es troben alguns predictors contrastants en relació amb la victimització i l'impacte del frau en línia i fora de línia, que pot anar més enllà de les pèrdues econòmiques fins al dany psicològic. La denúncia del frau i els motius per no denunciar també s'associen a certs factors sociodemogràfics, del context i del fet delictiu. Aquests resultats es relacionen amb les característiques criminogèniques de l'era d'Internet i poden ajudar a comprendre les tendències macro identificades prèviament, així com a informar polítiques i pràctiques.

-blank page-

CHAPTER 1 GENERAL INTRODUCTION

In Spain and abroad it is commonplace to find reports from the press, the private cybersecurity sector, the police or the judicial system that detail the rising threat presented by the various forms of fraud committed in the Internet era. Multinational cybersecurity solutions providers publish numerous threat reports in this regard (For example, PricewaterhouseCoopers, 2020) and Europol (2020), the Spanish Ministry for Home Affairs (Ministerio del Interior, 2020) and the Spanish Public Prosecutor's Office (Fiscalía General del Estado, 2019) have documented a steep rise in police-recorded fraud or related judicial proceedings in recent years. Yet, despite the growth in fraud documented in all these sources and the widespread prevalence highlighted in the press and by private sector organisations, official statistics still seem to indicate it plays a more residual role in comparison to other property crimes. This inconsistency is not necessarily surprising because, as is well known, the aforementioned sources cannot provide the whole picture that is necessary to understand a criminal phenomenon: the press and private security firms may tend to overexaggerate problems related to crime in order to advance their profit-making objectives, while the dark figure of crime not found in police and criminal justice figures has been well documented (Skogan, 1977), especially with regard to cybercrime (Miró-Llinares, 2012). Academic sources such as Tcherni et al. (2016) or Levi (2017) appear to confirm that victimisation of fraud is indeed very prevalent in the USA and the UK in the Internet era, and indicate that the prevalence may be far greater than is reflected in official statistics. Fraud could be the volume crime of the twenty-first century. On the other hand, Button et al. (2014) and Cross (2018) use qualitative interview methods to describe the economic, emotional, psychological and even physical consequences of fraud victimisation on individuals in England and Wales and Australia. They affirm that the effects of fraud are often misunderstood, and they find that the impacts can be extensive and potentially long-lasting. As a result, there appear to be two lucid gaps in the research on fraud. Firstly, there seems to be a notable discrepancy between fraud victimisation recorded by criminal justice institutions and the potential prevalence highlighted in academic literature. This raises questions about how prevalent fraud genuinely is, and if fraud is extremely widespread, why is this the case in the Internet era and what is causing the divergence between official sources and the true extent of the issue? Secondly, and relatedly, there is insufficient research, especially quantitative research, on the impacts of fraud on individuals in the Internet era and how these might relate to the potential dark figure of fraud. Thus, it seems that research from both a macro and a micro perspective is warranted and that criminologists should endeavour to do so with academic rigour. It is necessary to understand fraud developments from a macro perspective in terms of its general prevalence and role in crime statistics, and from a micro perspective in order to understand individual experiences as well as the mechanisms that may influence the macro context.

And this is the grounds for this thesis: to elucidate and provide criminological insight on a criminal issue – fraud against individuals - that may be extremely prevalent, that appears to be growing but we do not know to what extent, in what form, what the effects are, and, importantly, it is unclear why so little is known. In this sense, the present thesis studies fraud trends at a societal level as well as victimisation correlates, impact and reporting at the individual level. Ultimately, in-depth analysis of fraud in the Internet era that improves understanding of the issue can help build a knowledge base for the design and implementation of interventions that prevent and respond to fraud more effectively. To begin this process, it has been considered most appropriate to focus on fraud against individuals based on research priorities as well as practicalities. Priorities because individuals generally cannot afford the antifraud prevention measures or insurance policies that organisations can, and they are therefore less protected. And, practicalities in the sense that it is easier to obtain data on individuals from victimisation surveys. In addition, organisations are made up of individuals so any findings may applicable in organizational contexts.

This introductory chapter begins by outlining the underlying themes that link the articles of this doctoral thesis by compendium of publication into a coherent whole. Next, the chapter details how the present thesis ties into and contributes to wider criminological debates. Finally, the structure of the thesis is briefly set out.

1.1 The past and present of fraud research

1.1.1 Definitional debates

To begin the analysis conducted herein, it is necessary to introduce fraud in greater detail; however, over a century ago, Weber (1904) highlighted the complexity of precisely delineating concepts in the social sciences. Crime is often difficult to define (Fattah, 1997; Larrauri, 2019) and fraud is no different, as a variety of definitions are frequently employed (Levi & Burrows, 2008). The most common of these involve some form of reference to deception with the objective of obtaining an illicit economic gain, but there are many nuances to this; for example, when does the marketing of products of dubious efficacy become deception? Or, can avoiding a loss via deception be considered an illicit gain? The first article (CHAPTER IV) of this thesis begins by setting out a general fraud definition, which will have limitations as do all crime definitions, but which provides the foundations for the empirical research in the rest of that article and the remaining two:

> “fraud is an act of wilful deception that produces an economic benefit (or evasion of a loss) for the deceiver and a loss for the victim”

In order to identify these common elements, a variety of sources were employed. This began with the legal definitions provided in the Spanish Criminal Code (article 248) or the UK Fraud Act 2006, continued through academic criminological literature such as Button and Cross (2017b) or Levi (2012), and also included more institutional statistical projects such as the US report entitled Modernizing Crime Statistics that was produced by the National Academies of Sciences, Engineering and Medicine (2016) at the request of the Bureau of Justice Statistics and the Federal Bureau of Investigation.

It is also noted that encompassed within this broad definition there are many types of fraud and fraud victim (Levi et al., 2017). For instance, fraud committed against individuals, which is the subject of this thesis, can differ in many ways from fraud committed against organisations. Given the distinct characteristics of the targets, there will often be variations in the modus operandi, the impact and the reaction. Moreover, within fraud against individuals one can distinguish between fraud that has a direct victim, such as when an individual purchases inexistent goods or services, or more indirect victims, such as when multinational corporations commit systematic tax fraud and, in reality, all citizens are the victim (Croall, 2016). In general, this thesis deals with the former more direct victimisation, though articles two (CHAPTER V) and three (CHAPTER VI) do also examine the question of subjective criminal fraud victimisation. In this sense, even the individual who has suffered a direct fraud may not necessarily define themselves as a victim of a crime. As with fraud prior to the advent of digital technologies, central to fraud reporting in the Internet era, and therefore the potential response from the relevant institutions, is whether the person who has suffered a fraud acknowledges the condition of victim and considers it a criminal act (Wall, 2007/10). This subjective victimisation is discussed at greater length in section 1.1.6. on fraud victims and in relation to victimisation surveys in the conclusion and limitations of CHAPTER VI.

Fraud encompasses such a great deal of actions that it may be that it suffers from a ‘Name Fallacy’ similar to cybercrime. It can appear that the term cybercrime refers to one specific thing, but, in reality, cybercrime is very diverse (Miró-Llinares, 2015). Fraud is comparable in this regard as there are many different actions that can constitute fraud, many of which occur in very distinct circumstances. The first article shows that in order to help comprehend the broad category of fraud, there have been many attempts to provide a typology or taxonomy of fraud (for example: Beals et al., 2015; Button & Cross, 2017b; Levi, 2012; National Academies of Sciences, 2016). These categorizations allow researchers and practitioners to reflect upon the particularities of each fraud type and, therefore, the individualized prevention measures and responses that each may necessitate. Most classifications are quite similar in content, differentiating between individual and organizational victims as well as numerous fraud categories such as investment fraud, consumer fraud and charity fraud. As article one highlights and justifies, the categorization endorsed in this thesis is Button and Cross's (2017b) adaptation of Beals et al's taxanomy (2015).

A final distinction that is of marked relevance for the articles comprising this thesis is the role of the Internet in the commission of the act. This shall be discussed in the following section.

1.1.2 Old fraud in new bottles

Back in 2001, Grabosky argued that ‘virtual crime’ is ‘old wine in new bottles’ in the sense that the fundamentals of the crime are the same but the manner in which it is committed has changed. In the subsequent years, counter claims were presented, for example, Yar (2005, p. 407) argued that “‘cybercrime’ does indeed represent the emergence of a new and distinctive form of crime”. Eventually, categorizations of cybercrime appeared that differentiated between offences in accordance with the role played by IT in their commission. Possibly the most influential of these was developed by McGuire and Dowling (2013a, 2013b), who made the distinction between cyber-dependent crimes and cyber-enabled crime. The first of these refers to “offences that can only be committed using a computer, computer networks or other form of IT” (McGuire & Dowling, 2013a, p. 4), while the latter is defined as “traditional crimes, which can be increased in their scale or reach by use of computers, computer networks or other forms of IT” (McGuire & Dowling, 2013b, p. 4). These authors specifically refer to fraud as a potentially cyber-enabled crime and this is undoubtedly accurate - think famous fraudsters such as Charles Ponzi who were causing suffering long before the advent of the Internet (Will, 2013).

In Spanish criminology, the most well-known categorisation of cybercrimes is that of Miró-Llinares (2012), which distinguishes between pure attacks, replica attacks and content attacks. Content attacks refer to criminal acts where the illegality emanates from the content that is communicated, for example, child pornography. Pure attacks are defined in similar terms to the cyber-dependent crimes that McGuire and Dowling classified in English a year later (2013). Analogously, and of particular pertinence for this thesis, replica attacks are established along similar lines to cyber-enabled crimes: they are traditional crimes that are now also being committed in cyberspace. In this sense, the potential harm from fraud has been increased by information technologies, but that is not to say that more traditional methods have disappeared. While it is known that a shift in criminal opportunities has occurred, the specific dynamics of that shift and the consequences are still unclear (Miró-Llinares & Moneva, 2019). Studying one particular crime that can be committed in a traditional format or in manner which is fostered by the Internet may help understand the criminal developments we have been witnessing in recent years. Research comparing traditional crime and cybercrime has analysed many issues, such as victimization and offending (Kranenbarg et al., 2019; Leukfeldt & Roks, 2020) or reporting (van de Weijer et al., 2018), but with regard to economic crime this research has rarely been conducted within one offence. In order to more closely examine the specific similarities or divergences between traditional and modern cyber-enabled crime variants it seems opportune to do so within one crime type such as fraud, which encompasses the majority of economic cybercrime. This is a theme that runs through this thesis, since all three of the comprising articles seek to explore the difference between online and offline fraud in relation to trends, victimisation, impact or reporting.

However, it should be noted at this early stage, and as is discussed in articles two and three, making this delineation is not without limitations because online/offline boundaries are often blurred (Caneppele & Aebi, 2017; Cross, 2019; Floridi, 2015; McGuire, 2019). If somebody uses the Internet to learn how to commit fraud in door-to-door sales, is this online or offline? McGuire (2019) suggests that examples such as this could be encompassed in a third category of cyber-assisted crime, yet this is neither free from grey areas. Cyber-assisted crimes refer to those where the role of computer technology is incidental, but as later discussed in CHAPTER VI, this role may ultimately be decided by survey respondents in accordance with their own personal criteria. Placing the decision in the hands of survey participants has drawbacks, but also advantages, such as providing additional information on the very relevant subjective experiences of victimisation.

1.1.3 Cyberspace and fraud opportunities

The previous section of this chapter touched upon the shift in fraud opportunities brought about by the emergence of the Internet. Nowadays, it seems rather obvious to discuss how the Internet has changed the fraud landscape; yet, the fraud externalities stemming from this technological evolution are inherently linked to the *raison d'être* of this thesis, and, what is more, at the time of writing, the world is currently undergoing enforced changes in social relations and work conditions that has likely enhanced fraud opportunities even further (Buil-Gil et al., 2020); thus, let us provide a brief overview of the relationship.

Prior to the advent of telecommunications and above all the Internet, motivated fraudsters would likely have to encounter potential victims in the same physical space and time, thereby greatly limiting the number of suitable targets. The growth of cyberspace has brought about a simultaneous shrinking of both the distance and time necessary for two subjects to communicate (Miró-Llinares, 2011). One consequence of these developments in human interaction is that fraud has become globalised and industrialised (Button & Cross, 2017a). Firstly, globalised insofar as it is now theoretically possible for fraudsters around the world to defraud anyone who connects to the Internet, which in 2020 is over four and a half billion users[1]. In the Internet era, fraud does not respect physical borders; for instance, organised groups that commit high-tech fraud in the Netherlands have been found to consist of members from a variety of countries (Leukfeldt & Jansen, 2016). These authors found that the money mules who participate in the Dutch groups’ criminal

[1] Figure retrieved from Internet Live Stats on 23/06/2020: https://www.internetlivestats.com/

activity can come from all parts of Europe. Various studies have identified West Africa, especially Nigeria, as a hotspot for organized gangs who act to defraud individuals in Europe and Northern America (Akanle & Richard Shadare, 2020; Whitty, 2018). Similarly, 'boiler room' telephone frauds targeting UK investors were found to often base their operations in countries such as Spain where police interest was lower (Levi, 2008).

On the other hand, fraud has become industrialised since one fraudster or group of fraudsters can now attempt to deceive many people at the same time. In Spain, between 2010 and 2019 the number of households with Internet access rose from 57.8% to 91.4% while the percentage of people who have ever bought something online increased from 17% to 46.9% (Ministerio del Interior, 2020). The pool of potential targets has grown dramatically in the last decade and when the data for 2020 become available, it is highly likely the enforced changes in work and leisure brought about by the COVID-19 pandemic will lead to an even greater expansion of the online activities that generate opportunities for fraud. In this sense, as Yar and Steinmetz (2019) highlight, using the Internet in fraud schemes is very cost effective and traditional modi operandi have been adapted to take advantage of this. So much so, that fraud is the ultimate objective of many of the illicit acts that take place in cyberspace (Miró-Llinares, 2013); for example, the end goal of phishing attacks or data breaches is often to use the data obtained to commit fraud.

There are salient advantages to motivated offenders from the globalised and industrialised potential for fraud in the Internet era. One of the most important is the ability to avoid police investigations (Newman & Clarke, 2003; Yar & Steinmetz, 2019). By carrying out their illicit acts across borders, the jurisdictional nature of policing limits the ability of any one police force to act (Cross, 2020b) and, therefore, cooperation is required. This in turn generates two further issues: on the one hand, it is often necessary for formal cooperation agreements and frameworks to exist; and, on the other hand, the country being asked to investigate may not be motivated to initiate police proceedings against their own citizens when the victim is not a citizen of their country, and/or the country may not have the infrastructure and sufficient resources. Police investigations are time-consuming and costly, and each law enforcement agency has its own priorities. This ties into the industrialization of fraud, whereby organized groups are able to steal small amounts from many individuals (Button & Cross, 2017b). Police forces are less likely to investigate cases involving only small or moderate losses, meaning the perpetrators are often able to avoid a criminal justice response: *de minimis non curat lex* or 'the law does not deal with trifles' (Wall, 2007/10).

Two further characteristics of the Internet foster opportunities to perpetrate fraud and avoid detection. Firstly, cyberspace allows greater anonymity and fraudsters are able to operate under false identities. For example, romance frauds often involve the creation of a fake profile with which to lure potential victims (Whitty, 2015). Phishing also involves posing as a fictitious person or organisation or mimicking the identity of a real person or organisation with the aim of deceiving the potential victim (Williams et al., 2018). Even if the fraud is detected and reported, uncovering the real identity of the offender can be a complex task due to the many opportunities and tools modern technology offers to hide one's identity and prevent tracing illicit financial flows back to offenders (Miró-Llinares, 2012). Secondly, technology and society are in constant evolution. The tools available to offenders to, for example, hide their identity and illicit earnings are in perpetual development and it is difficult for public law enforcement agencies to keep pace (Bossler et al., 2020; Hadlington et al., 2018). Offenders in the Internet era are highly adaptable to opportunities as has become evident in analysis of fraud in the period since the COVID-19 pandemic began. Various sources (Buil-Gil et al., 2020; Hawdon et al., 2020; Payne,

2020) have highlighted the manner in which fraudsters have adapted existing fraud strategies to take advantage of the pandemic.

Researching crime from an opportunity approach has been taking place for nearly half a century (Cohen & Felson, 1979). This section has examined fraud opportunities from the perspective of the offender and of the criminal justice system as a guardian, but the victim can also play an essential role in the criminal event. This will be discussed in relation to fraud in the next section.

1.1.4 Routine activities theory and fraud victimisation

The rise in fraud as a consequence of societal and technological changes is a central theme and justification for the present thesis. The growth in Internet use in Spanish households and online shopping was highlighted in the previous section and these represent two of the most important changes in daily activities with regard to fraud today. This section examines how fraud research links to criminological theory on routine activities and how this can help understand rising victimisation.

According to Cohen and Felson's (1979) routine activity theory, crime occurs when the following three elements converge in time and space: 1) a motivated offender; 2) a suitable target; and, 3) the absence of a capable guardian. The opportunities offered by the Internet that could increase a fraud offenders' motivation were outlined in the previous section, as were some of the challenges that traditional criminal justice guardians face. Routine activity theory has been applied to fraud victimisation in the Internet era by many authors and of particular interest is how the daily behavioural routines of potential targets increase their attractiveness to the motivated offenders (Holt et al., 2017). In accordance with the original theory, a target's suitability depends on the elements that comprise the acronym VIVA (Value, Inertia, Visibility, and Accessibility). Value is the perceived value of the target by the offender. Inertia refers to the physical properties of the person or object that could affect whether it is considered suitable. Visibility means whether motivated offenders can detect the target. Finally, Accessibility refers to whether the target is accessible to offenders. However, Miró-Llinares (2012) theorised that other than Value these were not applicable in cyberspace. Instead the acronym IVI was proposed, which consists of: Introduction, whether the target has been introduced into cyberspace; if the target is perceived to be of sufficient Value to make it attractive; and, the victim's Interaction in cyberspace, in other words, online behaviour such as the time spent online and the places and people with whom a subject interacts. These new elements captured the essential capacity of the individual to influence the level of risk to which they are exposed in the Internet era.

Empirical literature examining the role of behaviour in individual fraud victimisation is extensive (Alshalan, 2008; Bossler & Holt, 2010; Copes et al., 2010; Holt & Bossler, 2008; Holt & Turner, 2012; Holtfreter et al., 2005, 2008; Hutchings & Hayes, 2009; Kerstens & Jansen, 2016; Leukfeldt, 2014; Leukfeldt & Yar, 2016; Ngo & Paternoster, 2011; Payne, 2020; Policastro & Payne, 2015; Pratt et al., 2010; Reisig & Holtfreter, 2013; Reyns, 2013; Reyns & Henson, 2015; Schoepfer & Piquero, 2009; Titus et al., 1995; van Wilsem, 2013; Van Wyk & Benson, 1997; Whitty, 2019; Williams, 2016), and many of these studies have also sought to identify individual demographic correlates.

Towards the end of last century, Titus et al. (1995) and Van Wyk and Benson (1997) examined fraud experiences in the United States. Regarding demographics, the first authors found few correlations with fraud victimisation; only being younger and having a mid-level education correlated with experiencing fraud. They suggested that a routine activities approach to fraud research may have greater potential than solely focussing on individual characteristics. Van Wyk and Benson (1997) analysed how demographic factors and attitudes toward financial risk correlate with fraud victimisation. Similarly to the study by Titus et al. (1995), they observed that the likelihood of victimisation decreases with age. In addition, they show that increased risk-taking attitudes (and therefore probably behaviour) are related to increased risk of victimisation.

After the turn of the century, a great deal more empirical research appeared, much of which was now also interested in fraud that took place via the Internet, and some common trends began to appear. The most lucid of these, as predicted by Titus et al. (1995), is the difficulty to identify any form of general demographic fraud victim profile (Holtfreter et al., 2008), which may be due to the disparity of criminal behaviours that fall under the fraud umbrella term. There appears to be some consensus that age and sex are generally correlated with fraud victimisation. Schoepfer & Piquero (2009) for a global measure of fraud, Reyns (2013) for identity theft, and Holtfreter et al. (2005), van Wilsem (2013) and Leukfeldt & Yar (2016) for consumer fraud, respectively, all found younger people to be associated with greater likelihood of fraud victimisation. However, Whitty (2019) concluded the opposite for online fraud and other studies did not encounter any correlation with various forms of fraud targeting or victimisation (Holt & Turner, 2012; Ngo & Paternoster, 2011). Recently, Payne (2020) identified that while young people may suffer at a greater rate, the over 50's have suffered far greater losses during the COVID-19 pandemic, both in comparison to young people and to the previous year. There is indeed a myriad of demographic factors that have been tested in relation to fraud. Some studies discovered that males were correlated with greater risk of suffering fraud (Holt & Turner, 2012; Holtfreter et al., 2008; Policastro & Payne, 2015; Reyns, 2013), but this again was contradicted by others who found no relationship (Schoepfer & Piquero, 2009; Titus et al., 1995) or a correlation with females (Copes et al., 2010). The disparities in results for individual demographic variables are similar with regard to education, income or ethnicity, amongst others.

Interestingly, some research has shown that after controlling for routine activities (Alshalan, 2008; Pratt et al., 2010); or delinquent peer associations (Bossler & Holt, 2010), demographic relationships often disappear. It seems that rather than demographics, it is behaviour that is key, although certain behaviours may be associated with certain demographics. In this sense, simply using the Internet more frequently (Alshalan, 2008; Hutchings & Hayes, 2009; Kerstens & Jansen, 2016; Eric Rutger Leukfeldt & Yar, 2016; Pratt et al., 2010) or sending emails (Reyns, 2013) or participating in forums (Johan van Wilsem, 2013) have been correlated with increased fraud risks. Furthermore, a number of studies found that online shopping is correlated with fraud victimisation (Holtfreter et al., 2008; Leukfeldt & Yar, 2016; Pratt et al., 2010; Reyns, 2013; Reyns & Henson, 2015; van Wilsem, 2013), as are other forms of buying or selling, such as telemarketing or mail-order purchases (Reisig & Holtfreter, 2013) or auction selling (Williams, 2016). Using online banking is another type of financial operation that appears to be related to increased likelihood of experiencing fraud (Reyns, 2013; Reyns & Henson, 2015).

Given the current permeation of technological developments into society and recent restrictions on traditional methods of leisure and work, it is hard to consider that necessary activities, such as Internet or email use, online shopping or banking, are unsuitable or preventable. Nevertheless, empirical research has identified some other behaviours that may be undesirable and avoidable. This approach appears more aligned with Hindelang et al's lifestyle theory (1978), which places greater emphasis on risky behaviours rather than the demographics or more general routine activities correlated with crime victimisation (Pratt & Turanovic, 2016). With regard to fraud, firstly, excessive disclosure of personal or financial information has been identified as a correlate of online fraud victimisation (Alshalan, 2008; Kerstens & Jansen, 2016; Reyns & Henson, 2015). Secondly, and closely related to Van Wyk and Benson's (1997) finding about attitudes to financial risk, a combination of risky behaviours, including sharing banking information or participating in free prize draws, may increase the likelihood of general fraud victimisation (Schoepfer & Piquero, 2009). Using public Wi-fi is a further potential risk factor that was identified by Williams (2016). Bossler & Holt (2010) also examined the relationship between risky behaviours, such as digital piracy, pornography use and access or modifying others’ computers or files, and 5 types of cyber victimisation, including credit card fraud. However, they found that these did not correlate with suffering online credit card fraud and instead associating with deviant peers was a determining factor in their sample.

In addition to demographic factors and activities that may be associated with increased fraud risk, it has also been highlighted that individuals play a key role in preventing victimisation by acting as self-guardians (Miró-Llinares, 2012). Using data from a special Eurobarometer, Williams (2016) showed that passive guardianship (for example, using antivirus software or secure browsers) was negatively associated with online identity theft, that is to say, it may help prevent against identity theft. Situational crime prevention measures like these were also found to be useful in preventing online economic crime by Newman and Clarke (2003). William’s (2016) results were the opposite for active guardianship (e.g. changing security settings and passwords), which showed a positive association. The author posits that this may be due to individuals taking action posteriorly to victimisation, a finding supported by Whitty (2019) and Martens et al. (2019).

This section has shown that there appears to be no clear demographic profile of fraud victim and while there is more consensus with regard to some routine activities, there are discrepancies with others. Internet and email use and online shopping and banking do seem correlated with online fraud victimisation but avoiding these is likely impractical and undesirable in today’s society. On the other hand, avoiding risky or deviant behaviours and employing personal guardianship techniques may be effective and may be more realistic. In other words, we cannot avoid some activities related to fraud victimisation, but some prevention interventions can work to reduce individual risk and potentially slow any documented growth in fraud. This will be examined in relation to the theoretical frameworks of the General Theory of Crime (Gottfredson & Hirschi, 1990) and Protection Motivation Theory (Rogers, 1975) in the next section.

1.1.5 The psychology of fraud victimisation in a hyperconnected world

Human behaviour does not occur in an emotionless vacuum; Psychological mechanisms influence how we act. As previously identified, risky behaviours and fraud victimisation may be related, and risky behaviours may be related to self-control (Holtfreter et al., 2010). In order to test this relationship, a number of authors have used the theoretical framework of the General Theory of Crime (Gottfredson & Hirschi, 1990). The theory was originally conceived to explain offending and low self-control, which is characterised by being impulsive, short-sighted, insensitive, impatient, and risk-taking, but more recently it has been applied to victimisation (Schreck, 1999). A meta-analysis on self-control by Pratt et al. (2014, p87) states that it is “a modest yet consistent predictor of victimization”, especially with regard to noncontact forms of victimisation, for example, fraud. In this sense, individuals who are less prone to long-term financial planning and are more likely to take short-term financial risks are, therefore, a more suitable target for fraudsters (Van Wyk & Benson, 1997; Van Wyk & Mason, 2001).

Self-control theory was tested by Holtfreter et al. (2008) with regard to consumer fraud targeting and consumer fraud victimisation. They found that low self-control was not related to fraud targeting, but it was statistically significantly related to victimisation. They postulate that perpetrators of fraud target potential victims based on individual routine activities and then self-control can determine the eventual victimisation. Low self-control has also shown a correlation with consumer fraud in various other studies (Reisig et al., 2009; Reisig & Holtfreter, 2013; van Wilsem, 2013). With respect to the relationship between financial risk taking, self-control and prevention, it might be that lower self-control is related to a lesser propensity to adopt guardianship strategies to prevent being defrauded (Graham & Triplett, 2017). In fact, Internet use has been linked to lower self-control via what Suler (2004) termed ‘the online disinhibition effect’. This refers to Internet users disclosing more information or carrying out more deviant acts online than offline. It should be remembered that these are two factors that have been correlated with fraud victimisation (Alshalan, 2008; Kerstens & Jansen, 2016; Reyns & Henson, 2015), and online disinhibition has been linked to cybercrime victimisation in general (Agustina, 2015). It could be that the shifts in opportunities that explain the rise in online fraud documented in article one of this thesis may include changes in self-guardianship behaviours. The increased use of the Internet as a means of communication may have brought about an increase in disinhibition, which could be related to the increase in fraud.

Disinhibition is closely related to the motivation to protect oneself, which has been conceptualised as Protection Motivation Theory (Maddux & Rogers, 1983; Rogers, 1975) and has been extensively applied in a plethora of areas of potential risks such as nutrition, disease, healthcare or road safety (Floyd et al., 2000). More recently, it has also been employed as a theoretical framework for studies on behaviour change regarding economic cybercrime and safe Internet usage (see, for example: Briggs et al., 2017; Chen et al., 2017; Jansen & van Schaik, 2019; Martens et al., 2019; Sommestad et al., 2015; van Bavel et al., 2019).

In accordance with this framework, an individual's motivation to protect themselves depends on their assessment of the threat – threat appraisal – and their view of dealing with the threat – coping appraisal (Floyd et al., 2000). The threat appraisal is comprised of two elements: on the one hand, the perceived severity of the threat; and, on the other hand, the perceived vulnerability of the individual to that threat. The coping appraisal involves three factors. Firstly, the ability of the individual to respond to the threat. Secondly, the perceived efficacy of this response with regard to the threat. Finally, the individual will consider the costs of the response. There appears to be notable degree of overlap with the constructs that form PMT and self-control theory: an individual with low self-control does not accurately appraise potential risks and overestimates their ability to respond. In other words, their motivation to protect themselves is not sufficient for the threats faced.

With regard to fraud, research has shown that interventions that aim to generate fear in individuals to raise awareness of potential phishing threats are not sufficient to change behaviour and reduce information sharing behaviour (Jansen & van Schaik, 2019). Similarly, Martens et al. (2019) found that increasing awareness of scams makes people feel less vulnerable and, therefore, less likely to employ guardianship strategies. The authors postulate that individuals becoming more aware of obvious scams may foster excessive optimism in their ability to detect fraudulent schemes. Chen et al., (2017) found low self-control and risky routine activities such as information disclosure and opening emails from unknown sources to be correlated with increased scam victimisation, which, in turn, is related to the adoption of protection measures. In short, it appears self-control and disinhibition are related to a lack of motivation to implement personal guardianship strategies, but it still remains unclear what works to motivate individuals to adopt fraud prevention measures in the Internet era. Exploring approaches based on behavioural economics may provide some interesting results in this regard (Acquisti et al., 2017; Briggs et al., 2017; van Bavel et al., 2019). While the present thesis does not deal directly with PMT or self-control theory, the three articles do discuss interventions that seek to improve prevention and reaction to fraud, thus, it is useful to bear in mind these related theoretical developments.

Further victim-centred research on fraud susceptibility has examined how the big five personality traits may influence victimisation (van de Weijer & Leukfeldt, 2017). In their study of over 3,500 Dutch individuals, van de Weijer & Leukfeldt (2017) found that from the traits of extraversion, agreeableness, conscientiousness, emotional stability and openness to experience, only emotional stability was negatively correlated with online consumer fraud victimisation. Analysis of their sample found there to be no relationship between the other four traits and fraud.

As well as the personality traits of those who suffer fraud, victimisation has also been explained from the perspective of the many psychological techniques that offenders may employ to defraud their victims (Button & Cross, 2017b; Fischer et al., 2013; Lea et al., 2009; Norris et al., 2019; Stajano & Wilson, 2011; Whitty, 2013; Williams et al., 2018), some of which shall be outlined next. Firstly, fraudsters may only request or steal small amounts of money. When asked for an insignificant sum of money, the victim is more likely to acquiesce, which may start a sequence of further requests (Fischer et al., 2013; Whitty, 2013) that are more prone to acceptation due to a continuation of behavioural commitment (Lea et al., 2009). Faced with smaller losses, individuals are also less likely to notice or report the fraud (Button & Cross, 2017b). A second group of factors are related to authority and legitimacy and social compliance. According to Button & Cross (2017b), legitimacy can be a key technique employed by fraudsters in the sense that they can attempt to appear legitimate by mirroring genuine websites or organisations or by directly using real websites such as auction sites or dating sites. Fraud perpetrators frequently pretend to be legitimate persons or organisations with a certain degree of authority so as to gain trust and induce compliance with their demands (Button & Cross, 2017b; Fischer et al., 2013; Lea et al., 2009; Stajano & Wilson, 2011; Williams et al., 2018). Reciprocity is a further persuasion technique that can be employed, especially in romance scams (Whitty, 2013). By offering gifts to potential targets, the offender is preparing the ground for a reciprocal positive response to their subsequent request for economic help. Fourthly, and imitating typical sales tactics, urgency and pressure are often used to elicit the desired response from a potential fraud victim (Button & Cross, 2017b; Fischer et al., 2013; Lea et al., 2009; Norris et al., 2019; Stajano & Wilson, 2011; Williams et al., 2018). Urgency may take the form of time pressure or scarcity, for example, a 'once in a lifetime investment opportunity'. Other forms of pressure that aim to induce compliance with a fraudulent scheme may be related to possible negative outcomes, such as, being locked out of one's bank account or losing a potential client. In fifth place, many scams also use social proof as a means to entrap potential targets (Lea et al., 2009; Stajano & Wilson, 2011; Williams et al., 2018). People tend to look to others for guidance on how to act and scammers often seek to trick potential victims into believing that others have participated and benefited from their scheme. Finally, visceral appeals are of great importance (Button & Cross, 2017b; Fischer et al., 2013; Lea et al., 2009; Stajano & Wilson, 2011; Whitty, 2013) and are related to many of the previous categories. Humans are motivated to act by emotions such as love, fear or greed. Fraudsters will aim to take advantage of this, and their persuasion techniques will include appeals to basic human needs and desires. For instance, investment or employment frauds may exploit financial instability and economic fears, while romance frauds seek to benefit from desires for companionship. In sum, fraud perpetrators employ many tactics to achieve their goals and they are very adept at implementing their strategies so as to take advantage of particular opportunities. This underscores the responsibility of the offender in the fraud event, which is key to the issues discussed subsequently.

1.1.6 The ideal victim and fraud impact and reporting

The articles that make up this thesis approach fraud from a victim-centred perspective in the sense that they attempt to understand and document how fraud is experienced. This is not a new approach; Levi & Pithouse (1992) conducted one of the earliest efforts to examine fraud victimisation and the media and criminal justice response almost 3 decades ago. However, there are still relatively few studies that have analysed this topic using quantitative methods, thereby further justifying the second and third articles of this thesis. In the Levi & Pithouse (1992) study, of particular interest for the present thesis is the introduction of the idea of a dissonance between the 'ideal victim', as described by Christie (1986), and fraud victims. According to this author, the condition of victim is not bestowed homogenously upon all crime sufferers but, rather, different characteristics provoke different responses. For example, if the person who suffers the offence is weak, is conducting legitimate activities at the time of the attack, and the offender is big and bad, there is a greater chance they will be conferred the label of 'victim'. Why is this relevant for fraud? Because fraud victims do not commonly hold the attributes of the 'ideal victim' and are often blamed for suffering an attack (Cross, 2015), which Van Wyk and Benson (1997) specifically described as erroneous. Through a number a interviews with fraud victims, Cross (2015) details the typical discourse that labels fraud victims as greedy, gullible or foolish, which is relevant for the analysis of the demographic correlates of fraud, such as education, found in article two.

Blaming fraud victims for their suffering adds to the negative consequences of fraud that have been identified in the literature. Button et al. (2014) employed face-to-face and telephone interviews in the UK to identify that fraud can lead to financial hardship, damaged reputations, broken relationships, psychological effects, mental and physical health problems and negative behaviour changes. Golladay & Holtfreter (2017) found comparable consequences from identity theft in their study in the US, which highlighted the negative emotional and physical impact of fraud as well as the financial losses. Similarly, Brenner et al., (2020) described how consumer fraud victimization can lead to a loss of confidence in decision-making abilities, especially with regard to financial matters. In Australia, Cross' (2018) findings add support to those from the UK and the US. This author showed that fraud can have far-reaching consequences such as relationship breakdowns, unemployment, homelessness, and even suicidal ideation. Perhaps some of the worst effects have been detailed for romance fraud, for which Sorell & Whitty (2019) established that there can be serious psychological damage. In fact, the psychological abuse suffered by romance fraud has even been likened to that of domestic violence victimisation (Cross et al., 2018). Article two of the present thesis seeks to expand the study of the negative impacts of fraud victimisation beyond the English-speaking world. It has been stated that comprehending the extent of the consequences of fraud allows for the design of improved victim support services (Cross, 2018a; Green et al., 2020; Leukfeldt et al., 2020).

The negative consequences of fraud are closely related to reporting, which is one of the central themes of this compendium of publications and this relationship is what inextricably unites CHAPTERS IV, V and VI: the impact of fraud may influence the reporting decision and the reporting experience may influence the impact of fraud. It has been claimed that fraud reporting rates in the Internet era are especially low (Button & Cross, 2017b; Caneppele & Aebi, 2017; Copes et al., 2010; Maras, 2017; Schoepfer & Piquero, 2009; van de Weijer et al., 2020), which could be explained by, for example, the relatively small amounts lost, the noncontact nature of the offence, the reporting process and expected results, and psychological factors such as shame and embarrassment. Van de Weijer et al., (2020) recently highlighted that fraud reporting may vary between fraud types, and this finding could be related to the factors mentioned above. More in-depth discussion of crime reporting and fraud underreporting can be found in the reviews of the literature in articles one and three. With the aim of adding to this body of literature and the wider debate regarding crime reporting, article one compares fraud reporting rates in various victimisation surveys from around Europe to the reporting rates for other property crimes.

Fraud reporting also ties into the extensive criminological inquiry regarding the congruence between cybercrime and traditional crime. It has been suggested that cybercrime reporting is low in comparison to traditional offences but that quantitative examinations of economic cybercrime reporting are scarce (van de Weijer et al., 2018). Article three seeks to advance knowledge on this topic by comparing reporting of online and offline offences within one crime type. Crime reporting is invaluable to the design of prevention and reaction measures (Reep-van den Bergh & Junger, 2018), therefore, to foster reporting it is necessary to understand the dynamics of the decision and how these can alter depending on the characteristics of the person or the event. For this reason, the third article examines the factors that correlate with reporters and their motives.

1.1.7 The dark figure of fraud

The discussion on fraud reporting in the previous section brings us to the salient issue of the potentially large dark figure of fraud, in other words, fraud that is not recorded in official statistics. It has been highlighted that there may be a substantial dark figure of property crime, such as fraud, in the Internet era and that further research is urgent (Tcherni et al., 2016). If fraud is not reported, obtaining a precise picture of the threat posed is complicated, which, as with all crime, can lead to the inadequate distribution of resources (Skogan, 1977). If a threat is underestimated, it is likely that responses will be insufficient; however, overestimating threats can also have negative ramifications. For example, it has been argued that the construction of cyberspace has brought about "moral panics" with regards to ever increasing crime in the Internet era (McGuire, 2019). Wall (2008) also suggested that society may hold a distorted image of cybercrime which can confuse our ability to appraise threats and blur our expectations of policing. Thus, based on the above, the first article of this thesis aims to shine a little light on the dark figure of fraud so as to help avoid misplaced concern or inadequate policy responses. As we enter a period when information and communication technologies will undoubtedly permeate even further into our lives, with all the fraud opportunities this may give rise to, it appears necessary to have the clearest possible image of what risks we are dealing with. And it is here that we find the greatest nexus between the macro and micro perspectives in CHAPTERS IV, V and VI. The first of these identifies a divergence between the official statistics on fraud and the prevalence captured in victimisation surveys, a predominance that catapults fraud to top of the property crime pile. The latter two present evidence of the individual-level factors associated with victimisation and impact, as well as reporting, which can help understand a criminal phenomenon that is simultaneously pervasive but obscure.

1.2 Fraud in the Internet era and wider issues of criminological inquiry

The introduction to existing fraud research provided in section 1.1 has shown that the present doctoral thesis by compendium of publications is humble with regard to its contribution to wide-ranging debates of a more theoretical nature. However, at the same time it is ambitious in its attempt to provide knowledge on a particular criminal phenomenon, for which data is scarce and research is lacking, in a manner that can have practical implications for crime prevention and reaction in Spain and abroad. Clarke (2010) highlighted that being crime specific is fundamental to academic research that aims to bridge the gap to applied crime prevention strategies. By focussing on fraud against individuals in the Internet era, this thesis aims to advance knowledge on a specific issue that appears to be particularly pressing and intends to do so from a victim-centred perspective, as advocated by Button and Cross (2017b). As will now be discussed, researching fraud in this manner should also make a contribution to three wider bodies of criminological knowledge: twenty-first century crime trends, cybercrime, and crime reporting.

Firstly, if fraud is indeed as extensive as it appears and we can obtain a clearer picture of the prevalence, this could help understand the effects that changes in criminal opportunities have had on crime trends this century. The importance of researching individual crime types has been highlighted by Baumer, Veléz and Rosenfeld (2018) in relation to crime trends. These authors argue that the study of crime trends and their causes should be central to criminological inquiry. The so-called crime drop has been discussed at great length in the US (Blumstein & Wallman, 2005; Zimring, 2007), Western Europe (Aebi & Linde, 2010) and even from an international perspective (van Dijk & Tseloni, 2012). It has been discussed in relation to violent crime such as homicide (Aebi & Linde, 2014), property crime such as domestic burglary (Tseloni et al., 2017) and youth crime (Fernández-Molina & Gutiérrez, 2018). Many hypothesis have been put forward to explain the reduction, such as: improved security (Farrell et al., 2011), higher abortions rates (Donohue & Levitt, 2001), lower levels of gun ownership (Duggan, 2001), a reduction in childhood lead exposure (Wolpaw Reyes, 2007) or lifestyle changes brought about by technological advances and the Internet (Aebi & Linde, 2010, 2014), amongst others. The growth of the Internet has undoubtedly changed the potential modi operandi for the commission of deviant acts (Holt & Bossler, 2015) and this may well have affected the overall panorama of crime (Miró-Llinares & Moneva, 2019). The impact cybercrime might have had, or not, on overall criminal reductions has been debated extensively (Farrell & Birks, 2018). By researching trends regarding one specific crime type that has not been considered in most previous work on the crime drop and is fundamental to any discussion on the relationship between the Internet and crime, it is believed the first article (CHAPTER IV) can make a contribution to this wider area of academic inquiry.

Secondly, and closely related to the previous consideration and section 1.1.2, the difference or similarity between cybercrimes and traditional crimes has caused considerable criminological debate (Weulen Kranenbarg et al., 2019) and is one of the main questions criminologists interested in cybercrime have attempted to answer (Yar & Steinmetz, 2019). However, many cybercrimes differ greatly from traditional crimes and many comparisons would seem bordering on redundant. In the same way a murderer is generally incomparable with a shoplifter, they are also likely to be incomparable with a website defacer. One possibility for contrast would be those crimes that are closely related, such as, online and offline bullying or online and offline fraud. The juxtaposition of fraud committed via the Internet with fraud committed offline may provide insights for issues of more far-reaching criminological relevance; for instance, how crime is experienced according to the different modus operandi. To this end, CHAPTER IV introduces the differing trends that can be found in online and offline fraud with regards to prevalence. This is expanded upon in CHAPTER V, which analyses correlates of online and offline fraud victimisation and impact. To further analyse online and offline fraud a/symmetries, CHAPTER VI examines the factors and motives that may influence the decision to report victimisation.

Finally, a victim-centred approach to crime research necessitates focussing on victim impacts and reactions. Crime affects people in different ways. From burglary (Mawby & Walklate, 1997) to intimate partner violence (Medina-Ariza & Barberet, 2003), the objective and subjective consequences of victimisation can differ in accordance with the characteristics or circumstances of the victim or the criminal act. It seems likely that fraud also provokes different outcomes in different people and responses to fraud may therefore benefit from being tailored or adapted to the needs of individual victims. Likewise, crime reporting, or not, may correlate with certain factors and it represents one of the central elements of the reaction to victimisation. Variations in reporting between different crime types has been a topic of extensive criminological interest (For example: Baumer & Lauritsen, 2010; Gutierrez & Kirk, 2017; Skogan, 1976) and it seems necessary that a potentially high-volume crime such as fraud be present in this discussion. In the second article, the thesis seeks to document different factors that correlate with financial and non-financial impacts of fraud. Furthermore, the first article touches upon the motives for fraud reporting, while the third article analyses the potentially influencing factors and motivations for reporting in greater detail. In this way, the impact of a specific crime type is linked to reporting at a micro level which is, in turn, linked to macro level trends in fraud. These findings are also of wider relevance for research on victimology and crime reporting in general.

As has been shown, although this research focusses specifically on fraud with the aim of informing interventions related to fraud, that does not mean it is only relevant for scholars and practitioners interested in this crime type. The findings of this thesis can also contribute to global criminological debates, such as the crime drop, cybercrime or crime reporting, which have been the subject of considerable academic attention.

1.3 Chapter conclusion and thesis outline

The aim of this chapter was to identify the underlying themes of the articles that form this doctoral thesis and to establish how the articles contribute to broader criminological inquiries. Several fundamental themes have been highlighted, specifically: the definitions and categorisations of fraud; fraud from an opportunities or lifestyles perspective; the importance of understanding the impacts of victimisation; and, underreporting and the dark figure of fraud. Furthermore, it has been demonstrated that the articles in this thesis are relevant for prominent global debates on crime trends in the twentieth century, cybercrime, and crime reporting in general. The next chapter will briefly restate and clarify the objectives of the thesis and, subsequently, detail the methodology employed as well as the potential sources of information and strategies that can be used by those researching fraud in general. Following on from this are the three articles as CHAPTERS IV, V and VI. Finally, the thesis concludes with the general results, discussion and conclusions, which can be found in CHAPTER VII.

-blank page-

CHAPTER II OBJECTIVES, RESEARCH QUESTIONS AND HYPOTHESES

The previous chapter identified the wider criminological debates to which this thesis contributes as well as the key themes and issues that run through the three articles. The aim of this brief chapter is to restate the previous discussion in the form of clear general research objectives and questions as well as their derived hypotheses. By doing so, the thesis as a logically-ordered coherent whole is further emphasised.

In short, this doctoral thesis seeks to provide comprehensive analysis of fraud against individuals in the Internet era, above all, but not exclusively, in relation to the Spanish and Catalan context. To achieve this main general objective, the issue is broken down into four more specific areas: trends, victimisation correlates, victimisation impact and reporting. These four areas have been selected, on the one hand, based on the existing literature as well as the literature gaps that have been identified and, on the other hand, bearing in mind that the thesis pursues the production of knowledge that can have practical applications for prevention and reaction from a victim-centred perspective. Understanding trends is essential to establish criminal policy priorities and adequate responses. Identifying factors associated with victimisation is key to designing effective prevention strategies. Comprehending the subjective experience of victimisation is necessary to provide support services that can reduce the impact. And, without sufficient reporting rates, all of the above are considerably more complex. Furthermore, as Felson and Eckert (2020) explain in the 6th edition of their seminal book *Crime and Everyday Life*, research that aims to inform prevention and reaction should focus on the modus operandi of crime. In the case of fraud in the Internet era, the fraud opportunities discussion in CHAPTER I suggests that an initial approximation to focussing on modus operandi should explore the method of contact between victim and offender. Thus, the thesis aims to answer the following general research questions:

> RQ_1 How has fraud against individuals evolved during the Internet era?
>
> RQ_2 What factors influence fraud victimisation in the Internet era?
>
> RQ_3 How does fraud in the Internet era impact victims?
>
> RQ_4 What factors are associated with fraud reporting in the Internet era?

From these general research questions, the general hypotheses are derived that the three articles seek to test. With regard to RQ_1, article one (CHAPTER IV) sets out to test whether:

GH_1 Fraud is rising in the Internet era, especially due to the prevalence of online fraud.

This is carried out by analysing the dark figure of fraud in the context of the supposed property crime drop.

With respect to RQ_2, it is hypothesized that:

GH_2 The sociodemographic characteristics correlated with online fraud victimisation differ from those correlated with offline fraud victimisation.

This hypothesis is tested in the second article (CHAPTER V), which examines the correlates of fraud victimisation by comparing online, telephone and in-person fraud.

Article two also responds to RQ_3, this time considering the hypothesis:

GH_3 Certain sociodemographic characteristics and crime event factors are correlated with increased impact of fraud victimisation.

To test this hypothesis, it was considered essential to look beyond solely the financial impact and also examine the annoyance caused and the psychological impact. Article two performs this examination and once again differentiates between different fraud modi operandi.

Finally, regarding RQ_4, the following hypothesis was formulated:

GH_4 Certain sociodemographic characteristics and crime event factors are correlated with the decision to report fraud.

This hypothesis is tested in article three (CHAPTER VI), which explores the correlates of fraud reporting in the Internet era as well as the motives for not reporting.

The articles follow a conscious order, whereby a problematic, growing and underdetected crime issue is highlighted from a macro perspective in the first article, then the individual factors associated with victimisation are examined, followed by the impact resulting from suffering fraud, and, lastly, this feeds into the analysis of the factors that may influence the decision to report and, thus, the obscure nature of the problem. The next chapter describes the data and methodology used to answer the aforementioned questions, test the hypotheses and, ultimately, achieve the main research objective.

-blank page-

CHAPTER III METHODOLOGY: RESEARCHING FRAUD IN THE INTERNET ERA

In the editorial introduction to the *Sage Handbook of Criminological Research Methods*, Gadd, Karstedt and Messner (2012) describe collecting data for criminological research as particularly challenging, even in comparison to other social sciences. Crime is illicit by nature, crime is diverse and criminological data is often messy and hard to come by. Overcoming these hurdles are paramount to criminological expertise that can compete with political and media ‘common sense’ claims in the design and development of public policy. In his chapter of the same handbook, Levi (2012) highlights that in relation to fraud, most research has not been conducted with academic rigour. In part because of the aforementioned methodological challenges regarding data collection, availability and analysis, but also more simply because of a lack of research interest in fraud and its consequences. Nevertheless, it need not be all doom and gloom. According to Levi (2012, p. 479), “a ‘true picture of fraud’ is a chimera, but a better and truer picture of fraud is possible”. And greater awareness of fraud is necessary if we want to reduce the social and economic costs of what appears to be an ever-growing issue and the volume crime of the digital era. This chapter begins by outlining the main data sources used in this thesis as well as the related motives and limitations. Subsequently, the methods and tools employed to prepare and analyse the data and visualise the results are set out.

3.1 Data sources

This thesis draws on secondary data, which although limited are often a valid and invaluable resource for criminologists (Bachman & Paternoster, 2020; Davies & Francis, 2018). In order to deal with the patchiness of the data available on fraud, a variety of sources have been employed to analyse the issue that is the focus of the present thesis. Utilizing a wide range of sources has been recommended when testing criminological hypotheses, for example, regarding the crime drop (Tilley, et al., 2018). As with much criminological research, the first port of call is official statistics and CHAPTER IV provides an introductory descriptive overview of police-recorded property crimes, including fraud, in Spain and Catalonia. However, the limitations of official statistics are well documented (Maguire & McVie, 2017) and they have received strident criticism in Spain (Aebi & Linde, 2010). One of the greatest limitations has already been discussed and identified as a key theme for this thesis: official statistics require crimes to be reported and fraud reporting in the Internet era is believed to be low due to victims being unaware of the offence or unwilling to report it. This shall be discussed further in the chapters containing the articles. Official statistics also require fraud to be recorded by police once it has been reported. It has been suggested that in the case of cybercrimes, the typical motives for not recording crime may be aggravated (Yar & Steinmetz, 2019). These motives include political and policing prioritisations of certain crimes over others, especially those that are likely to remain unresolved and potentially harm the police forces' reputation. CHAPTER I described the difficulties faced by law enforcement agencies with regard to fraud in the Internet era, thereby highlighting a potential disincentive to record offences. It has even been suggested that governments may be concealing recent rises in fraud so they are able to claim they have been successful in reducing crime (Levi, 2017). In addition, changes in criminal law also impede coherent recording of crime over time, which therefore hampers the ability to chart crime trends.

One of the main aims of CHAPTER IV is to identify trends with regard to fraud; thus, it is necessary to compliment and compare Spanish and Catalan police statistics with other sources. This is initially performed by examining data produced by other official sources; in this case, fraud data provided by the Bank of Spain, UK Finance and by the European Central Bank. Data provided by financial institutions can be a valuable resource for academic fraud research provided they supply information on the definitions and counting methodology followed. These institutions will also have an agenda with regard to publicising data on victimisation, but this may diverge from that of law enforcement and political parties; thus, fraud trends can be compared, and similitudes and discrepancies identified. Nevertheless, these remain official sources and, therefore, victimisation surveys were also employed in order to counteract some of the aforementioned shortcomings. Victimisation surveys have long been cited as a means to partially overcome the limitations of analysis based on official statistics (Maguire & McVie, 2017; Tilley, et al., 2018; Yar & Steinmetz, 2019). Reep-van den Bergh and Junger (2018) give a brief overview of the benefits of victimisation surveys and why they have had a considerable impact on knowledge about crime. In this sense, firstly, they offer information on crime levels and trends without requiring a police report. Secondly, they have helped develop classifications for crime other than the legal classification used by police. Moreover, they have been important for theoretical advancements such as the routine activities approach. In fourth place, they can provide information on how victimisation is experienced and the consequences it produces. Finally, they have been described as the most suitable method for comparing crime levels between countries.

While victimisation surveys offer benefits in comparison to official statistics, they also suffer from limitations of their own, especially with regard to sampling, methodological choices and the variations in respondents' interpretations of the questions (Reep-van den Bergh & Junger, 2018). One of the design choices that is relevant for fraud research is the decision regarding which crime types to include in any survey: Fraud was not present in many initial victimisation surveys. This has begun to change in recent years, and many countries now include questions related to fraud in their national victimisation surveys. This means there are rich sources of data to be explored by criminologists interested in fraud. In CHAPTER IV of this thesis, surveys from Catalonia[2], England and Wales[3], Netherlands[4], Sweden[5], Finland[6], France[7], Denmark[8] and Luxembourg[9] are all employed in pursuit of a clearer picture of fraud in the Internet era. CHAPTERS V and VI, which seek to delve deeper into issues related to fraud, conduct quantitative analysis on the Catalan survey. Details of the methodology followed by the Catalan survey can be found in Spanish in CHAPTER V and in English in CHAPTER VI.

The data from the Catalan Public Security Survey were obtained via a freedom of information request to the Catalan regional government, meaning that on receipt the data

[2] Information on the Catalan Public Security Survey (*Enquesta de Seguretat Pública*) is available on the regional government website: https://interior.gencat.cat/es/el_departament/publicacions/seguretat/estudis-i-enquestes/enquesta_de_seguretat_publica_de_catalunya/index.html

[3] Data from the Crime Survey for England and Wales is available on the website for the Office of National Statistics: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice

[4] The website for the Dutch Security Monitor (*Veiligheidsmonitor*) is available at: http://www.veiligheidsmonitor.nl/

[5] The Swedish National Crime Survey (*Nationella trygghetsundersökningen*) is available with an English summary here: https://www.bra.se/publikationer/arkiv/publikationer/2019-10-08-nationella-trygghets-undersokningen-2019.html

[6] The Finland National Crime Victim Survey (*Kansallisen Rikosuhritutkimuksen*) is conducted by the Institute of Criminology and Legal Policy at Helsinki University: https://researchportal.helsinki.fi/fi/projects/kansallinen-rikosuhritutkimus-kansallinen-turvallisuuskysely

[7] The Living Environment and Security Survey (*L'enquête Cadre de vie et sécurité*) available on the website of the French Home Office: https://www.interieur.gouv.fr/Interstats/L-enquete-Cadre-de-vie-et-securite-CVS

[8] The 2017 Internet Crime Survey (*Internet-kriminalitet*) was conducted jointly by the Crime Prevention Council and Copenhagen University: https://dkr.dk/materialer/it-kriminalitet/internetkriminalitet-2017/

[9] The 2013 Luxemburg Security Survey (*Enquête sur la Sécurité*) is available in English here: https://statistiques.public.lu/catalogue-publications/economie-statistiques/2015/85-2015.pdf

had to be cleaned and prepared for analysis. Cleaning, or tidying, data requires a tremendous amount of time and effort because data is often messy (Wickham, 2014). Even though the data are collected by the Catalan Home Office following recommended survey methodology best practices, the Catalan Public Security Survey is not designed with inferential statistical analysis on fraud victimisation in mind. This means that the acquired data must be prepared for analysis. Fortunately, the tidyverse packages available in R offer tools that are “human centred” and can make this process as easy as possible (Wickham et al., 2019), including for non-expert criminology users. R is the statistical software environment chosen for the analysis conducted in this thesis for two main reasons that are highlighted on the R Project website[10]: on the one hand, it “provides a wide variety of statistical techniques” and easily produces “publication quality plots”; on the other hand, it is available as free open source software (R Core Team, 2019) and therefore contributes to a culture of open science. Pridemore et al., (2018) have called for an open science culture in criminology and the possibility of replicating the scripts of code produced in R can help encourage this. In other words, the potential transparency offered by R can contribute to fostering research integrity in criminology, which, like many social sciences has been called into question in recent years (Savolainen & VanEseltine, 2018; Sweeten, 2020).

Having briefly outlined the data sources used in this compendium of publications and introduced the most suitable tools to prepare the data, the next section details the statistical methods employed to analyse the data.

[10] https://www.r-project.org/about.html

3.2 Statistical methods

Criminological research methods systematically “develop, refine, apply, and report” knowledge on issues related to crime and criminal justice (Bachman & Paternoster, 2020). This means data are collected and analysed in a systematic manner in order to offer conclusions regarding the object of study (Jupp et al., 2000). CHAPTER II set out the general research questions that this thesis aims to answer as well as the hypotheses that will be tested through the systematic research methods. This will be achieved through an eminently quantitative approach: On the one hand, CHAPTER IV seeks to test the first general hypothesis on fraud trends via descriptive statistics, while, on the other hand, CHAPTERS V and VI turn to more advanced methods to conduct inferential statistics on predictors of victimisation, the impact of fraud and fraud reporting. These methods have been chosen based on the questions they intend to answer. One of the central goals of CHAPTER IV is to describe trends, therefore, a descriptive approach is more apt. CHAPTERS V and VI seek to identify and examine the factors that may correlate with or predict different phases of the fraud victimisation experience, thus, statistical modelling is chosen. Almost all scientific disciplines employ modelling to some degree, and criminology is no different; models can allow us to better understand social phenomena and potentially help predict a certain outcome. In pursuit of shedding light on various facets of fraud and producing knowledge that can be relevant for policy design, three types of regression model have been employed. These statistical models, which have their origins in the late nineteenth century (Angrist & Pischke, 2009) and are widespread in the social sciences today (Britt & Weisburd, 2010), will now be summarised. The aim of this brief overview is to provide a general roadmap for potential future hypothesis testing in fraud studies using R.

CHAPTERS V and VI both use binary logistic models. These are employed when the dependent variable or outcome is dichotomous, for example: crime or no crime (CHAPTER V), or report or no report (CHAPTER VI). In other words, the dependent variable is categorical, and it only has two levels, which are assigned the values of 0 for the reference category and 1 for the category of interest. This technique calculates the odds or the probability that the outcome variable belongs to one of the categories depending on the relevant independent or input variables, for example: male or female; Spanish or foreign; primary education, high school education or university; financial losses. As can be observed in the latter two examples, it is not necessary that the independent variables only have two levels but, rather, they can be categorical with multiple levels or continuous. Britt & Weisburd, (2010) provide an overview of the use of logistic regression models for criminological research in their chapter entitled *Logistic Regression Models for Categorical Outcome Variables* in the *Handbook of Quantitative Criminology*. Regarding the present thesis, in CHAPTER V, the outcome variable is whether the person who has suffered a fraud considers it a crime or not. In CHAPTER VI, many binary models are conducted to analyse the factors correlated with fraud reporting and the motives for not reporting.

While further details of each individual analytic strategy are available in the respective articles, it has been considered pertinent to offer a general overview here. As with the data preparation, the modelling performed in the articles is carried out in R. There are many high-quality free resources that can assist criminologists who want to learn the basics of data science in R (Grolemund & Wickham (2016) is possibly the most well-known in this regard[11])[12] or, more specifically, modelling for criminology[13][14]. Once the data are suitably prepared, running a binary logistic model is fairly straightforward in R. To highlight this, below is an example of the script used in CHAPTER V and one example from CHAPTER VI. This shows that the R function used is `glm()` and the dependant outcome variable `delito` or `report` is specified along with the independent input variables that come after the `~` symbol. The dataframe being used is identified - `DFFraud` or `ReportFraud` - and, finally, it is specified that a binomial model is being used with `family="binomial"`.

- Example of R script for logistic regression CHAPTER V

```
Delito_model <- glm(delito ~ tipo_fraude + sexo + edad + nacionalidad +
educacion + situacion_profesional + situacion_economica + discapacidad +
perdidas + impacto + molestias + percepcion_seguridad_local, data = DFFraud,
family = "binomial")
```

- Example of R script for logistic regression CHAPTER VI

```
Reporting_model <- glm(report ~ Type + sex + age + nationality +
Education + profesional_sit + financial_sit + disability + financial_impact
+ psych_impact + annoyance + opi_securitylocal + opi_mossos +
opi_local_police + crime, data = ReportFraud, family = "binomial")
```

CHAPTER V also employs multinomial and linear models. The former refers to models in which the categorical dependent variable has more than two levels. In this case, when

[11] The book is, and always will be, available for free as an open source resource: https://r4ds.had.co.nz/
[12] Code and documentation for individual R packages can be found in the CRAN archives, available at: https://cran.r-project.org/index.html
[13] The didactic resource produced by Medina & Solymosi is highly recommendable for criminologists interested in modelling: https://jjmedinaariza.github.io/modelling_book/
[14] Another useful free book on R for criminology was written by Kaplan: http://crimebythenumbers.com/

comparing the factors that may predict victimisation between the different fraud modi operandi, the dependent variable or outcome categories are online fraud, telephone fraud, in-person fraud or others. The process for this in R is very similar to that for the binomial model. The script below shows that there are two main differences. On the one hand, the `multinom()` function is now used, and, on the other hand, it is no longer necessary to specify `family = "binomial".`

- Example of R script for multinomial regression CHAPTER V

```
victim_model <- multinom(tipo_fraude ~ sexo + edad + nacionalidad + educacion
+ situacion_profesional + situacion_economica + discapacidad, data=DFFraud)
```

Finally, the linear regression model measures the association between a continuous dependent variable (or a discrete ordinal variable with a sufficiently large number of values (Torra et al., 2006)) and the independent variables. This requires a similar script to the multinomial regression but this time using the `lm()` function instead of `multinom()`.

CHAPTERS V and VI utilize two different methods to interpret the results of regression models. In the chapter on victimisation predictors and impact, this is achieved through the regression coefficients. Coefficient estimates are produced automatically with the `summary()`function. where the `estimate` column indicates the size and direction (positive or negative) of the association between the outcome and input variable. For example, in the logistic regression for whether the fraud is considered a crime in CHAPTER V, the coefficient estimate is -1.35 for the category “telephone” fraud from the variable “Type of fraud”. This means that in comparison to the reference category “online” fraud, “telephone” fraud predicts lower probability of being considered a crime in the sample used. However, -1.35 refers to the estimated decrease in the coefficient estimate, which is not that easy to communicate to general readers in terms of the size of the effect. On the other hand, in the chapter that analyses fraud reporting, odds ratios are used. Odds ratios also describe the strength and direction of the relationship between the dependant and independent variables, plus their interpretation can be somewhat easier. For example, in CHAPTER VI it is found that the odds of reporting a fraud are six times higher (odds ratio = 6.278) if the person who has suffered the fraud considers it a crime. One further step is required to obtain odds ratios in R, which can be calculated by running `exp(coef(model_name))` and the confidence intervals for the odds ratios by using `exp(confint(model_name))`. A more detailed interpretation of the results can be found in CHAPTERS V and VI, and statistical tables can be found in appendices A and B.

To communicate the results in CHAPTERS V and VI to readers it was considered useful to plot these in R. A variety of plots have been used from the highly versatile ggplot2 R package[15]. The subsequent lines will provide an example of the script employed in the third article to plot the odds ratios using the `ggplot()` function. Before plotting, a dataframe was created with the names of the statistically significant variables (or those that approached significance) and the values for the odds ratios and their respective confidence intervals. An example of the code for this step is as follows:

- Example of R script for dataframe of odds ratios to be plotted

```
# Create labels #
boxLabels = c("Telephone ***\n (ref=Internet)", "In person ***\n
(ref=Internet)", "Other **", "Considered\n a crime ***", "Financial impact
*", "Annoyance ·")


# Create dataframe #
```

[15] For further information on how to use ggplot2, see (Wickham, 2016) or the CRAN project page: https://cran.r-project.org/web/packages/ggplot2/index.html

```
Reportf <- data.frame(

  yAxis = length(boxLabels):1,

  boxOdds = c(0.092, 0.385, 0.365, 6.278, 1.03, 1.094),

  boxCILow = c(0.042, 0.23, 0.188, 3.348, 1.01, 0.997),

  boxCIHigh = c(0.18, 0.628, 0.669, 13.115, 1.065, 1.206)

)
```

Next, the odds ratios and confidence intervals can be plotted with `ggplot()`. The script below shows the versatility of this function. For example, the position, size and type of a vertical intercept line can be set with `ggeom_vline()`. The size, height and colour, amongst others, of the error bar to display the confidence interval are adjusted with `geom_errorbar()`. The size and colour of the odds ratio point is modified using `geom_point()`. The background and general appearance of the figure is set with different variants of `theme()`. Finally, `ylab("")`, `gxlab("")` and `ggtitle("")` are used to write the axis labels and the titles.

- Example of R script for plotting odds ratios

```
victim_model p <- ggplot(Reportf, aes(x = boxOdds, y = yAxis))

p1 <- p + geom_vline(aes(xintercept = 1), size = .25, linetype = "dashed")

+ geom_errorbarh(aes(xmax = boxCIHigh, xmin = boxCILow), size = .5, height

= .2, color = "gray50") +

geom_point(size = 3.5, color = "orange") +

theme_bw() +

theme(panel.grid.minor = element_blank()) +

scale_y_continuous(breaks = 6:1, labels = boxLabels) +

scale_x_continuous(breaks = seq(0,7,1) ) +

coord_trans(x = "log10") +

ylab("") +
xlab("Odds ratio (log scale). (Ref=1)") +

ggtitle("Model 1. All fraud")
```

This chapter has sought to provide a general overview of the data and methods employed in this doctoral thesis. By doing so, it is hoped that it can act as a brief introductory guide for others who wish to conduct quantitative research on fraud. The chapter aimed to highlight key resources for obtaining data on fraud as well as their subsequent analysis. Clearly, the examples of the R code used in this chapter will not be sufficient by themselves for others who wish to conduct basic models and plots for fraud research. Nevertheless, they can provide a valuable starting point along with the other, more comprehensive sources cited in this chapter and will hopefully also serve to encourage further research. Having described the general objectives, data and methods, it is now time to proceed to the articles that constitute the main content of the present thesis.

-blank page-

CHAPTER IV THE DARK FIGURE AND THE CYBER FRAUD RISE IN EUROPE: EVIDENCE FROM SPAIN

4.1 Defining before measuring: an introduction to cyber fraud

Fraud is by no means a new phenomenon, as evidenced by the Sicilian corn trader who deceived a potential customer for illicit gain in ancient Greece (Johnstone, 1998). Yet, fast forward to the present and fraud in the Internet era persists and has developed and expanded within the social and technological changes related to information and communication technology (Clough, 2015; Smith, 2010). While the Internet brings innumerable benefits, it also presents criminogenic features (Leukfeldt et al., 2017; Miró-Llinares, 2012; Savona & Mignone, 2004) which have changed the way much crime is committed. Indeed, many authors talk of ‘cyber’, ‘online’ or ‘Internet’ fraud (Button & Cross, 2017b; Levi et al., 2017; Miró-Llinares, 2013; Williams, 2016) to differentiate a modern globalised variant from the traditional face-to-face methods and to highlight the role that the Internet plays in twenty-first century manifestations of this property crime. Various types of cyber fraud have been highlighted as particularly widespread; for example, card–not-present fraud is a significant threat (Europol, 2018), bank and credit account fraud victimization is extensive (Levi, 2017) and romance fraud constitutes a global problem (Whitty, 2013). In fact, Williams (2016) has stated that online fraud is Europe’s most widespread property crime.

Meanwhile, in studies using police statistics various authors have identified a property crime drop in Western societies (Fernández-Molina & Gutiérrez, 2018; Tonry, 2014) or in Europe (Aebi & Linde, 2010; Gruszczyńska & Heiskanen, 2018), but fraud or cyber fraud have not been considered in the analysis. As Baumer et al. (2018, p. 40) state, there has been "insufficient attention to differences in crime trends by offense type". A broad definition of property crime includes fraud (Tcherni et al., 2016; Wright & Jaques, 2017), thus, it seems useful to consider fraud in the property crime drop analysis.

The present article begins by defining fraud and cyber fraud. The subsequent section employs both police statistics and data provided by central banks to analyse the nature and evolution of the issue in recent years. The aim of this second section is to examine whether fraud trends follow a similar pattern to other property crimes and if their inclusion in the property crime drop analysis affects the overall picture. Next, the article examines the results of victimization surveys from a number of European countries with the objective of estimating fraud prevalence and determining whether there exists a property crime drop or, on the contrary, a cyber fraud 'police recording flop' (Caneppele & Aebi, 2017). To answer this question, the paper revises fraud reporting rates and motivations in several European countries. Finally, the implications of the findings are discussed with regards to the challenges for policing and prevention policy and whether this exemplifies the new multi-agency cybercrime policing network (Holt & Bossler, 2015) in which public police forces no longer play the title role (Wall, 2007/10).

A key step in all crime measurement is the delimitation of the delinquents acts which are to be measured (Gadd et al., 2012; Maguire, 2012), yet fraud is difficult to define (Anderson et al., 2013; Leukfeldt et al., 2013; Levi & Burrows, 2008). Deceit and illicit gain (or evasion of a liability) are the essential elements that have been identified by a variety of sources (Beals et al., 2015; Levi, 2012; Miró-Llinares, 2013; National

Academies of Sciences, 2016; *Spanish Criminal Code*, n.d.; United Nations Office on Drugs and Crime, 2015), in other words, fraud is an act of wilful deception that produces an economic benefit (or evasion of a loss) for the deceiver and a loss for the victim. This highlights the broad nature of fraud and with the aim of providing a clearer vision of the actions that typically constitute fraud in a criminal sense, Button and Cross, (2017b) adapt Beals et al's (2015) Framework for a Taxonomy of Fraud perpetrated against individuals. Their adaptation includes the initial seven categories of fraud and an additional eighth category of identity fraud. All eight fraud types are also present in the Fraud section of Modernizing Crime Statistics by the American National Academies of Sciences, Engineering, and Medicine (2016) as shown in table 1[16].

Table 1. **Eight categories of fraud against individuals.**

1. Consumer investment fraud	The use of false information to wilfully deceive a potential investor, commonly involving the promise of high returns.
2. Consumer products and services fraud	The sale of worthless and non-existent products or worthless, unnecessary and non-existent services as well as unauthorized billing for products and services. Includes very common fraudulent activity such as online marketplace fraud, tech support scams or spoofing websites.
3. Employment fraud	Consists in an initial payment in return for inexistent future employment or training.
4. Prize and grant fraud	Advance payments made in expectation of future winnings which do not exist.
5. Phantom debt collection fraud	An individual is led to believe they must pay an inexistent debt.

[16] 'Identity fraud' is called 'identity theft' but the definition is the same.

6. Charity fraud	Fraudulently presenting oneself as a genuine charity in order to collect money.
7. Relationship and trust fraud	The exploitation of a personal relationship with a victim in order to obtain financial gains.
8. Identity fraud	The use of another party's personal information, such as bank card details, for financial benefit. Personal information is often obtained using deception and when the information is used, deception often occurs in the process, for example, card-not-present fraud involves the deception of a financial institution or payment service.

Source: adapted from Button and Cross (2017b) and American National Academies of Sciences, Engineering, and Medicine (2016).

As can be appreciated from the above eight categories, fraud is an extremely wide-ranging issue. On the one hand, it therefore seems surprising that it is often not considered in crime trend analysis; however, on the other hand, this may in fact explain its absence, since definitional difficulties can obstruct recording.

It should be remembered that the above classification refers only to those frauds perpetrated against individuals and not those involving an organisational victim. As highlighted in Table 2, the National Academies of Sciences, Engineering, and Medicine (2016) and Beals et al. (2015) differentiate frauds committed against organizations. While this article focusses primarily on fraud offences involving individual victims, the existence of organisational victims should be recognised, especially as police and bank data on fraud should include any reports made by these.

Table 2. **Fraud against organizations.**

1. Fraud against government agencies, programs, regulations, and society	Includes offences such as welfare fraud or tax fraud.
2. Fraud against an organization or business (public, private, or non-profit)	Subdivided into occupational fraud (carried out by internal actors) and frauds carried out by external perpetrators.

Source: adapted from Beals et al. (2017) and American National Academies of Sciences, Engineering, and Medicine (2016).

As regards the cyber element, cyber fraud is, in short, one of the aforementioned fraud types which is perpetrated via the Internet. This may be as a hybrid crime that combines offline and online activities or a fully online crime (Caneppele & Aebi, 2017). Within cybercrime, the role of the Internet can vary significantly but most cyber frauds fall into McGuire & Dowling's (2013b) category of cyber-enabled. This means that they are traditional types of fraud that have been enhanced by using the Internet in some capacity. For example, consumer fraud can now be perpetrated through online commercial retailers and marketplaces from almost anywhere in the world in a fraction of the time and with reduced risk of police intervention.

4.2 Official statistics, crime drop and fraud in Spain

As Rosenfeld (2018) stated in his address to the American Society of Criminology, if an evidence-based criminologist wants to know which measures to employ in order to reduce crime, they first need an accurate measure of crime rates. It is necessary to understand the nature and extent of crime so as to inform and evaluate crime control policies and agencies

(Fafinski et al., 2010) and, in this sense, various authors have highlighted the importance of fraud measurement (Levi et al., 2017; Tunley, 2014).

The so-called crime drop and its causes have generated great debate in Criminology in the last 25 years. A reduction in property crime has been a central feature of the discussion with numerous authors highlighting a drop in the USA (Blumstein & Wallman, 2005; Levitt & Dubner, 2005; Zimring, 2007), internationally (Van Dijk et al., 2012; Tonry, 2014; Tseloni et al., 2010) and Western Europe (Aebi & Linde, 2010; Gruszczyńska & Heiskanen, 2018). However, the analysis has typically not examined fraud offences and it has been suggested that the rise in property crime perpetrated via Internet may be greater than the offline drop (Tcherni et al., 2016), meaning an overall increase in property crime.

It has also been postulated that displacement has taken place from traditional forms of crime to online and hybrid crime (Button & Cross, 2017b; Caneppele & Aebi, 2017; Levi, 2017b; Tcherni et al., 2016). However, there are significant counter arguments against the displacement effect (Farrell & Birks, 2018), specifically, a lack of robust evidence, inconsistencies regarding the timing, and problems with causal mechanisms. While Farrell and Birks suggest that the timings are inconsistent in the USA, UK and Australia, they do state that fraud may constitute one form of criminal activity which could plausibly have been subject to online adaptation. In contrast, Miró-Llinares & Moneva (2019) argue that there is enough empirical evidence to support the idea that "increases in criminal opportunities in cyberspace […] go hand in hand with decreases in criminal opportunities in physical space, particularly with respect to dual crimes" (p. 4), which would help to understand the underlying mechanism of the shift.

The aim of this section is to examine how fraud trends in Spain can add to this property crime drop literature by including, in addition to police statistics fraud data provided by banks. Combining data sources may shed new light on fraud prevalence and trends. If, as some authors suggest, displacement has indeed taken place between offline crime and cybercrime, it should follow that any rise in cyber fraud would be accompanied by a similar decrease in traditional fraud.

The analysis begins with crime drop statistics provided by the Spanish Ministry of the Interior (MIR). It should be highlighted that crime statistics in Spain have historically been notable for their unreliability (Aebi & Linde, 2010). However, transparency has improved in recent years and they serve as a starting point for the present analysis. Furthermore, official crime statistics are often used to inform criminal policy and as such it is important to evaluate their reliability with regards to fraud.

In Figure 1[17], the Spanish Ministry of the Interior highlights a general crime drop (violent and property crime) between 2008 and 2016. The timing for the Spanish crime drop is considerably later than the trend identified in America, however, it has been shown that certain crime types increased in the European context until at least 2007 (Aebi & Linde 2012), crime trends in Europe vary from those in the United States (Killias & Aebi 2000) and occasional lags in crime trends between particular countries have been identified (Tonry 2014).

[17] All data transformation and visualization have been executed using the tidyverse R package version 1.3.0 (Wickham et al. 2019) in RStudio version 1.2.5033 for the R free software version 3.6.2.

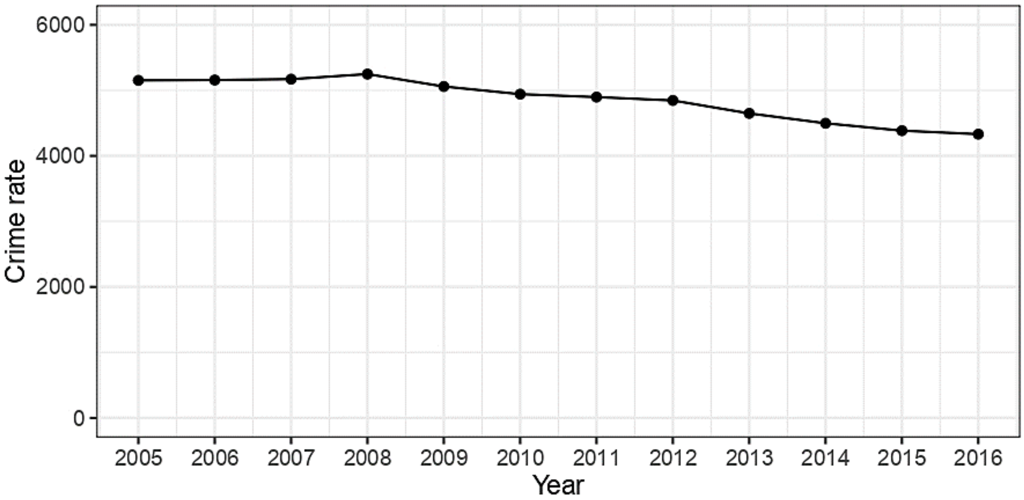

Figure 1. Crime in Spain per 100,000 population, 2005-2016. Source: Spanish Ministry of Interior. http://www.interior.gob.es/documents/10180/6865255/Presentacion+ministro_Balance+de+Criminalidad+2016.pdf

According to the Spanish National Police (2016)[18], the steep crime reduction detailed between 2012-2016 is due to increased police efficiency as a result of the introduction of a Strategic Plan focused on the fight against terrorism, organized crime, irregular immigration, human trafficking and cybersecurity, amongst others. As evidence of its improved efficiency related to cybercrime the police force stated that in this period there was a significant rise in the number of detentions for cybercrimes, including identity fraud and online fraud.

Figure 2 shows the official data for the property crime types which are included in the MIR crime rate calculation (theft, robbery with forced entry, violent robbery, vehicle theft, fraud). With the exception of fraud, these show a decrease from 2010 (from when data for individual crimes is available), and above all from 2012 onwards.

[18] Retrieved from http://www. interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6 ztgsg/content/id/6222655

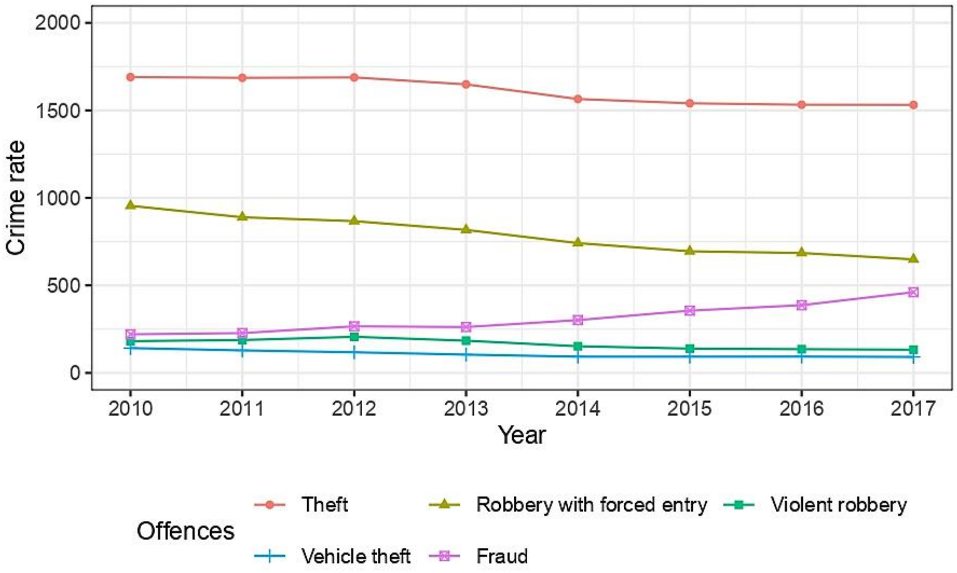

Figure 2. Property crime in Spain per 100,000 population, 2010-2017. Source: Spanish Ministry of Interior statistics database: https://estadisticasdecriminalidad.ses.mir.es/

As detailed in Figure 3, data from the Ministry of the Interior show that reported frauds rose over 100% in the same period, increasing from approximately 200 per 100000 inhabitants to over 450. This increase is particularly pronounced from 2013-2017.

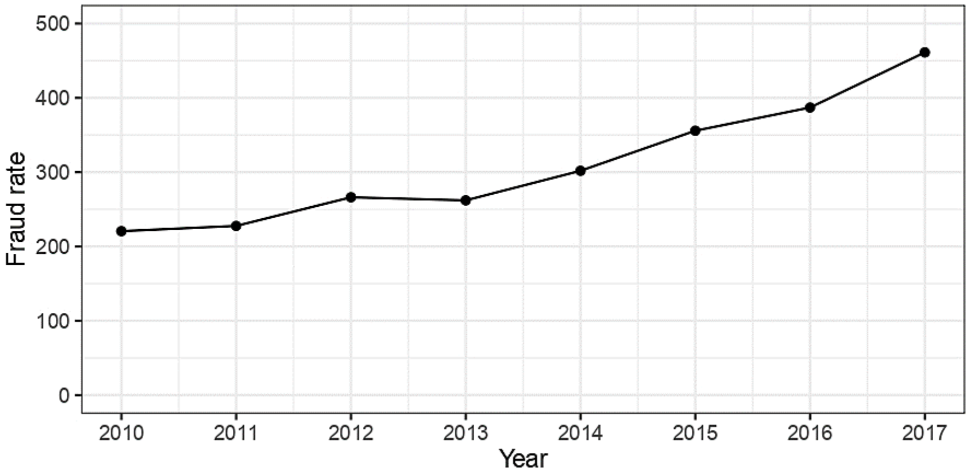

Figure 3. Fraud recorded by police per 100,000 population, 2010-2017. Source: Spanish Ministry of Interior statistics database. https://estadisticasdecriminalidad.ses.mir.es/

However, the unreliability of police data for crime trend analysis has been highlighted (Baumer et al., 2018; Van Dijk, 2015) and it is highly unlikely that these official statistics provide an accurate picture of fraud prevalence as underreporting of fraud to police is common (Button & Cross, 2017b; Caneppele & Aebi, 2017; Maras, 2017; Wall, 2007/10). There are a number of possible reasons explaining the low level of fraud reporting to police:

- The victim is often unaware of their victimisation due to not checking their bank accounts or to a lack of understanding about financial cybercrime.
- The victim may be unsure of where to report cybercrime.
- In accordance with expected utility theory, if the amount lost is relatively insignificant the victim may decide not to report as the time and resources required outweigh the losses that may be recovered.
- The victim may only need to report to their financial institution in order to obtain a reimbursement, thus, the police are not informed unless it is a requirement to recover losses.
- The victim may be embarrassed by the events or view themselves as partially responsible. In this sense, not reporting can be a defence technique to avoid secondary victimisation.
- The victim may not believe the police are experts in cybercrime and therefore lack confidence in their ability to respond. They may believe the police do not have the resources or expertise to investigate and identify the perpetrators.
- The victim might not want to share their Internet activity with police in order to aid their investigations.

While many of the reasons enumerated above are applicable to both individuals and organisations, underreporting by the latter is strikingly common and as a result, academic research on the nature and prevalence of fraud against organisations is scarce (Jansen et al., 2017; Tunley, 2014). It has been noted that organisational victims prefer to carry out their own investigations and responses to fraud (Wall, 2007/10). Furthermore, organisations involved in financial transactions are actively encouraged to act as a 'front-line of defence' to aid police services that do not have the resources necessary to be the main actor in fraud prevention (Levi & Burrows, 2008).

4.3Bank statistics and the rise of cyber fraud

As a consequence of significant underreporting to law enforcement agencies, it is necessary to identify statistics from alternative sources in order to obtain a clearer picture of crime trends (Caneppele & Aebi, 2017). In Spain, one such industry source is the Bank of Spain (BoS). In its report titled *Annual report on the supervision of financial market infrastructures*[19], BoS provides statistics on fraudulent transactions recorded by the payments systems networks used in this territory. This means that it registers fraudulent transactions carried out in Spain using Spanish bank cards and overseas bank cards, as well as transactions conducted outside Spanish territory using bank cards emitted in Spain. BoS understands a fraudulent transaction to be a transaction involving a bank card, bank card information or bank account without the owner's authorisation. The Spanish Criminal Code article 248.2 (a) and (c) uses the same definition. In accordance with the terminology used in section 1, this means BoS provides data on identity frauds. It should be noted that when reported to the Spanish police, these are recorded as bank frauds and are also included within the general fraud statistics.

Information on fraud has only been included in the BoS reports since 2012. In the period for which information is available at the time of writing (2012-2016), and as shown in

[19] Available from: https://www.bde.es/bde/es/secciones/informes/Publicaciones_an/Memoria_anual_so/index2016.html

Figure 4, there was a rapid increase in the volume of identity fraud. In this five-year period, the rate of fraudulent transactions rose by over 50%.

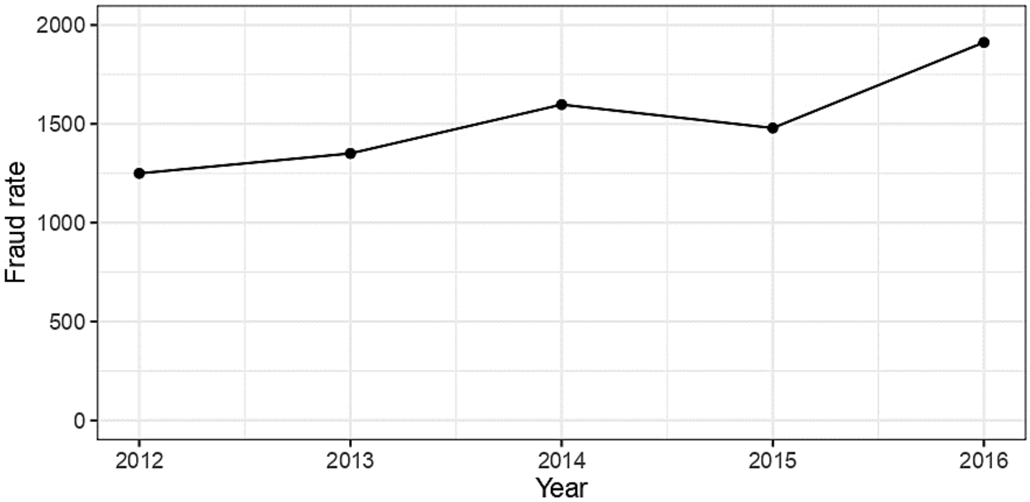

Figure 4. Fraudulent bank transactions per 100,000 population, 2012-2016. Source: BoS

Interestingly, the BoS data reveals that this rise is due to increases in remote fraudulent transactions, in other words, fraud with a substantial cyber component (Figure 5). This is particularly relevant for the displacement debate as while non-remote bank card fraud has decreased slightly, the reduction is significantly less pronounced than the increase in cyber fraud. There are two possible explanations for this. On the one hand, there may be only slight displacement between the two types of fraud and, thus, the rise is due to the appearance of new fraud and fraudsters. On the other hand, it could result from the increased criminal opportunities provided by cyberspace, whereby a tactical crime displacement has occurred, and the new modus operandi has permitted an escalation in offending.

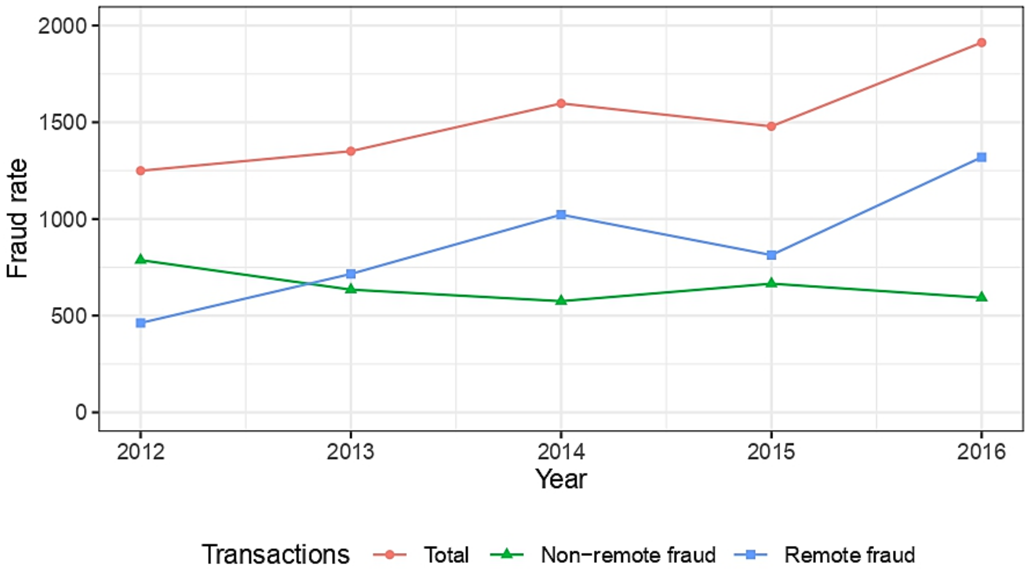

Figure 5. Figure 5. Remote and non-remote fraudulent transactions per 100,000 population, 2012-2016. Source: BoS

The Spanish fraudulent transaction data is analogous to data provided by UK Finance (2018), the industry body for the UK banking and financial sector. Their most recent report shows that card fraud almost doubled, mainly due to nearly 700,000 thousand more instances of remote card fraud (cyber fraud) per year. The other forms of card fraud detailed in their report show much less significant changes in absolute numbers.

At a European level, the *European Central Bank* (ECB, 2018) in their Fifth Report on Card Fraud, state that the value of card fraud using cards issued in the Single European Payment Area rose approximately 500 million euros between 2012 and 2016. This increase was mainly due to growth in remote fraud, as the other fraudulent transactions included in the study, point of sale fraud and ATM fraud, changed by comparatively small margins.

The data available from Spanish, UK and European banking authorities thus suggest that the rise in identity fraud is above all the result of increases in remote bank card fraud rather than a displacement effect from face-to-face card or cheque fraud.

Further evidence for this trend is provided by data from the Mossos d'Esquadra, the Catalan police force. The Mossos d'Esquadra are the main police force in the autonomous region of Catalonia, which accounts for approximately 16% of the total Spanish population. They process their crime statistics separately from the centralised Spanish Ministry of Interior and freedom of information requests can be made to them directly. Unfortunately, the Spanish Ministry of Interior refused the authors access to the corresponding data for the other police forces active in Spanish territory, stating that they consider freedom of information requests for academic purposes to be 'abusive'[20]. Figure 6 shows the frauds that were flagged as Internet frauds by the Mossos d'Esquadra in comparison to those that did not receive this tag. Non-Internet frauds have remained relatively stable during this period, while cyber fraud has increased significantly. In short, the Bank of Spain, UK Finance and European Central Bank data and the Catalan police statistics suggest that fraud offline-online displacement has been insignificant and it is the rise of cyber fraud that is driving the current fraud boom. As Farrell and Birks (2018) state, it seems logical to imagine that if there were indeed some degree of causal relationship between increased cybercrime and a drop in traditional offences, this would be evident above all within a crime type such as fraud.

[20] The police in Spain is not made up of one homogenous body but rather several different forces: the National Police, Civil Guard, Local Police as well as the police forces that correspond to the autonomous communities of Catalonia, Basque Country and Navarra.

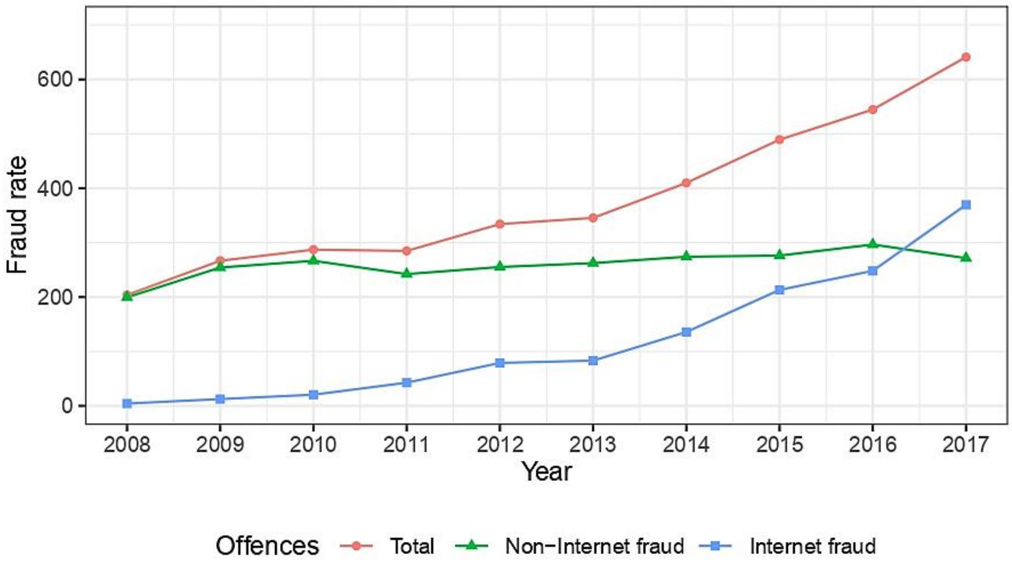

Figure 6. Police recorded fraud in Catalonia per 100,000 population, 2008-2017. Source: Catalan Ministry of the Interior

Returning to the Bank of Spain statistics, it is also relevant that in this period fraudulent transactions as a percentage of total transactions have risen only slightly (Figure 7). This trend is similar in the UK Finance and European Central Bank data and leads to the conclusions that: a) in part, fraudulent transactions have risen in absolute terms as a consequence of the increase in the total number of transactions; b) prevention has not improved in this five-year period; and thus, c) we can expect that as Internet-based transactions rise in the future, cyber fraud will continue to rise unless prevention is improved.

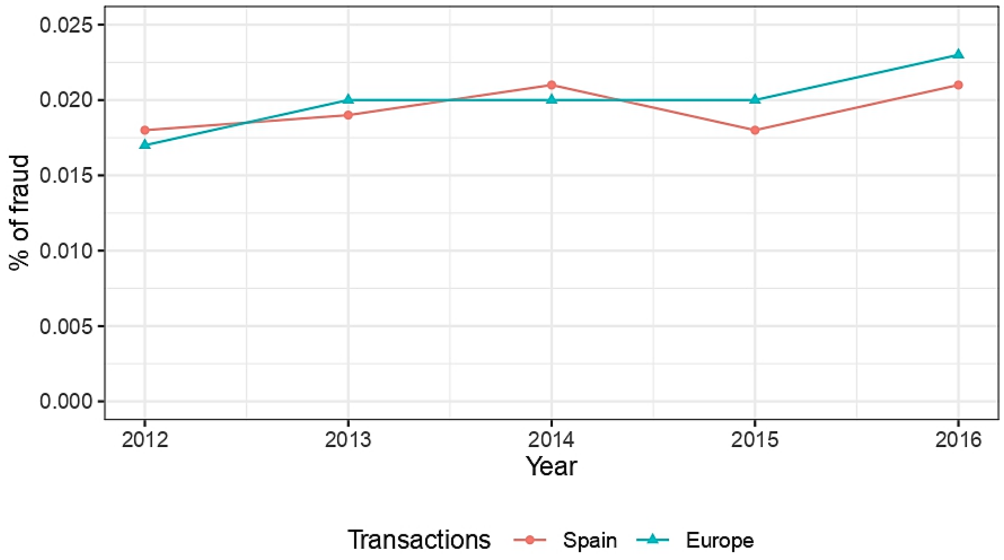

Figure 7. Percentage of fraudulent transactions relevant to total transactions, 2012-2016. Source: BoS

4.4 Property crime drop?

Figure 8 shows the property crime rate when bank recorded fraud is used to calculate the property crime rate rather than police recorded bank fraud. The graph indicates it is difficult to affirm that there has been a property crime drop in Spain if we consider fraud statistics from both the MIR and the Bank of Spain. In fact, there may well be a rise, especially considering Spanish banks only provide data on identity fraud. In most types of fraud, such as advance fee fraud or romance fraud, the customer typically authorises the transaction themselves so therefore the bank may not recognise it as fraudulent and, in addition, the offence may also not be reported to the police for the reasons enumerated previously. In such cases, these transactions will not be included in either the MIR statistics or the data published by the Bank of Spain.

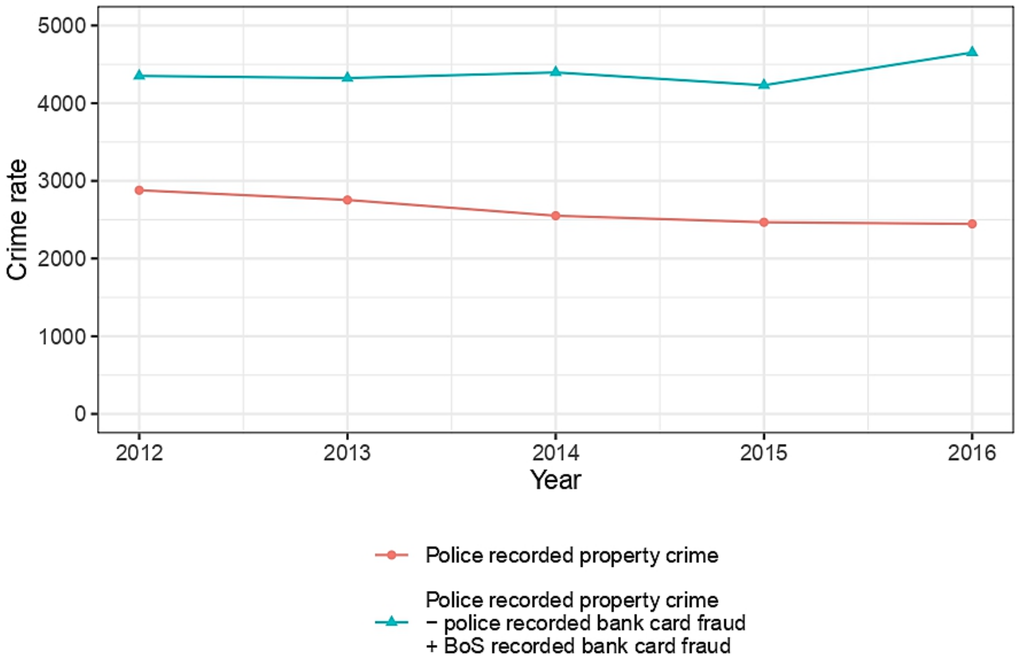

Figure 8. Property crime drop? Official property crime per 100,000 population vs. Official property crime – police recorded fraud + Bank of Spain recorded fraud per 100,000 population.

It should be noted that counting is likely to be different for banks and police. For example, three fraudulent transactions involving one individual could constitute one reported fraud in police statistics. As such, adding the bank statistics to the police statistics is a very crude calculation. Nevertheless, in the Internet age it seems unwise for the Spanish Ministry of Interior to draw conclusions on police efficiency and crime tendencies only from police statistics. This will lead to inefficient use of criminal justice resources and ineffective criminal justice policies. The limitations of the data analysed in this section mean it cannot be categorically stated that there has not been a property crime drop; however, the trends identified in the BoS data certainly call into question official sources that take this drop for granted. The Bank of Spain statistics show an increase of over 300,000 bank frauds in the period 2012-2016, which is due to an increase in remote bank card fraud. The bank card frauds registered by the police in 2016 were 35,824. This represents just 4% of the 888,000 bank card frauds detected by banks in Spain and thus suggests extreme underreporting of bank card fraud to the police. Even if it were assumed that each bank card fraud recorded by the police corresponds to five fraudulent transactions, the reporting rate would only be 20.1%. It should also be highlighted that bank data include those fraudulent transactions detected by the bank as well as the customer.

In sum, fraud appears to be rising fast and if we include police fraud statistics and bank card fraud data from the Bank of Spain in the crime rate analysis, it is hard to maintain that there has been a property crime drop; in fact, it appears there may have been a property crime rise in recent years in Spain. It also suggests that there has not been an increase in police efficiency as claimed by the Spanish National Police, but rather the public police's ability to record and respond to modern versions of property crime is diminished. Furthermore, it appears that the displacement effect from offline fraud to online fraud has limited explanatory power, as the increase in fraud with a strong cyber component is much greater than the decrease in traditional frauds. One possible explanation is that the characteristics of cyberspace allow many cybercrimes to be executed with little effort (Miró-Llinares, 2011), unbalancing the proportion of crimes committed online and offline.

4.5 Victimization surveys

As with other crimes, victimization surveys can help shine further light on the dark figure of fraud (Mayhew & Dijk, 2012) as well as the impact of fraud on the overall panorama of delinquency. The high levels of fraud underreporting combined with the fact that financial institutions may not identify many transactions that constitute criminal fraudulent activity mean these surveys can be especially useful for fraud analysis.

Victimisation surveys are scarce in Spain, especially those that use rigorous survey methodology. To the authors' best knowledge, the only victimisation survey which produces statistically representative results and includes data on fraud is the Catalan Public Security Survey. This is conducted biennially in the Spanish autonomous province of Catalonia which, as previously mentioned, accounts for approximately 16% (7.5 million) of the total Spanish population. In its 2017 version, the survey asked over 7,000 respondents whether, in the previous 12 months, they had been victim of a scam, fraud or deception that they considered to be criminal[21]. In response, 7.7% of respondents affirmed that they had suffered fraud victimization, of which 20% reported it to the police. Therefore, 1.2 % of respondents stated they have been victim of a fraud and that they had reported it to the police.

Large-scale victimisation surveys are carried out annually in a number of countries in the European Union, namely France, Netherlands, England and Wales, Denmark, Sweden and Finland. Direct comparisons between countries are hazardous (Van Dijk, 2015) but these surveys can help determine whether the Catalan results are in line with other European countries. Furthermore, by analysing the results of victimisation studies from various Western European countries, fraud prevalence and trends can be roughly estimated for Spain.

The methodology employed to choose the surveys was based on five factors. This methodology was chosen as it aligns with previous property crime victimisation research (Levi, 2017; Reep-van den Bergh & Junger, 2018):

[21] Further information on the survey methodology and results can be found here: https://interior.gencat.cat/es/el_departament/publicacions/seguretat/estudis-i-enquestes/enquesta_de_seguretat_publica_de_catalunya/enquesta_de_seguretat_publica_de_catalunya_2017/

1. The survey includes a question on fraud, either in general or one particular type that refers to the previous 12-month period.
2. The survey publishes their methodology or made their methodology available to the authors on request.
3. The survey uses a random sample that is statistically representative of the population.
4. The survey is carried out annually or biannually and the questions have remained significantly unchanged since 2010.
5. The survey has been carried out in a country belonging to the European Union.

Unfortunately, to the authors' knowledge there are no surveys on organisations that meet the criteria, therefore, the results are only relevant for individual victims. The surveys that were finally selected for inclusion in the analysis were: (1) England and Wales: Crime Survey for England and Wales (Office for National Statistics, 2018)[22]; (2) Sweden: "National Security Survey" (Brottsförebyggande, 2018)[23]; (3) France: "Living environment and safety" survey report (Ministère de l'Intérieur, 2018)[24]; (4) Netherlands: "Security Monitor" (Centraal Bureau voor de Statistiek, 2018) [25]; (5) Denmark: "Internet Criminality" (Kruize, 2018)[26]; and (6) Finland: "National Crime Research" (Danielsson & Näsi Matti, 2018)[27].

Figures 9 and 10 show the evolution of fraud results included in these surveys from 2010-2017. With the exception of the survey from England and Wales, for which only two

[22] Data for Crime Survey England and Wales is available here: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables

[23] The English summary of the Swedish Crime Survey 2017 is available here: https://www.bra.se/bra-in-english/home/publications/archive/publications/2018-03-08-swedish-crime-survey-2017.html

[24] Information on the French survey is available here: https://www.interieur.gouv.fr/Interstats/Actualites/Rapport-d-enquete-Cadre-de-vie-et-securite-2017

[25] The Dutch Security Monitor can be accessed here: https://www.cbs.nl/nl-nl/publicatie/2018/09/veiligheidsmonitor-2017

[26] The Danish Internet Criminality survey can be accessed here: https://dkr.dk/materialer/it-kriminalitet/internetkriminalitet-2017/

[27] Information on the Finnish National Crime Victims Survey can found here: https://www.helsinki.fi/fi/kriminologian-ja-oikeuspolitiikan-instituutti/kansallinen-rikosuhritutkimus

years are available, all surveys indicate an upward trend in fraud victimisation. It is worth noting that in the first 9 months of 2018 fraud victimisation rose in England and Wales to slightly above the 2016 mark.

It should be highlighted that significant differences exist in the questions used, and also therefore disparities in the results. For the most recent year data is available, the percentage of the population who have been victims of fraud is: 7.7% in Catalonia; 5.9% in England and Wales; 8.9% in Finland; 7.5% in France and 9.9% in Sweden. In 2016, Sweden commenced an extended version of their original survey. The total fraud results for this study were considerably higher than the original, which the authors suggest is due to the inclusion of questions on specific fraud types. The current survey found consumer fraud to be 4.8% and bank account or card fraud to be 5.1%, giving a total fraud victimisation rate of 9.9%. As of 2017, the extended version is the only survey format employed.

On the other hand, the surveys conducted in Netherlands, France and Germany enquired about victimisation for particular fraud types, namely consumer fraud and bank account or card fraud. In 2017, 3.9% of the Dutch population and 4.7% of the German population stated that they had been victims of online consumer fraud. In France, results indicate that the victimisation rate for bank account or card fraud was 4.2% for 2017. However, in 2017 a new question was introduced to the French survey regarding scam victimisation, which they define as all frauds and scams that are not fraudulent debits from a bank account or card. The response rate for scams was 3.3%, which means that overall 7.5% of the French population were fraud victims that year.

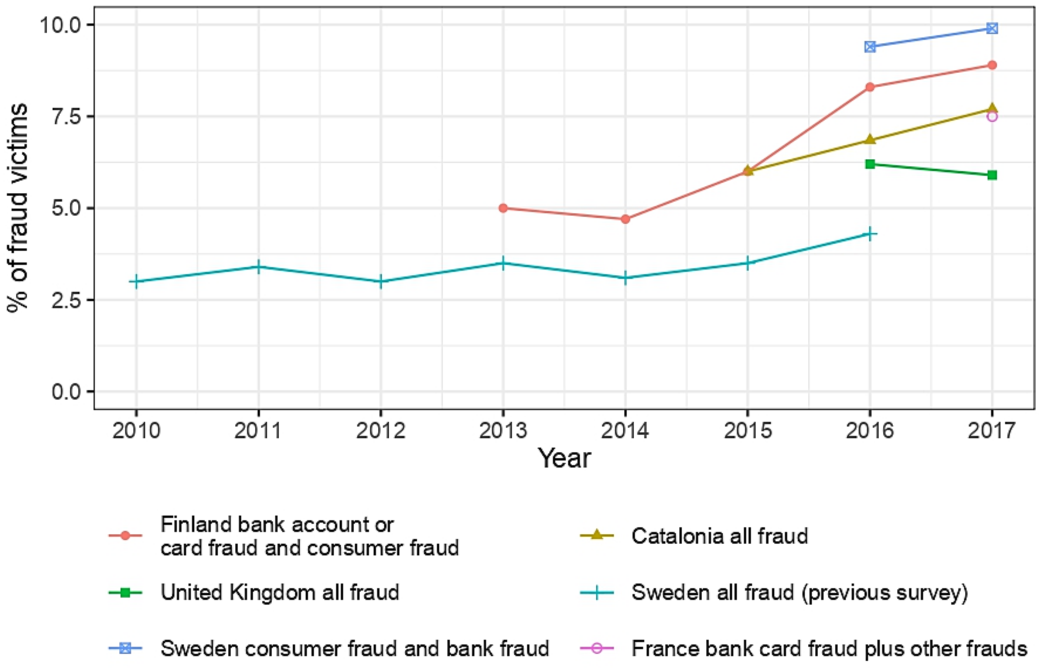

Figure 9. General fraud victimisation rates in European victimisation surveys.

Source: Catalan Public Security Survey; Crime Survey for England and Wales; Sweden, "National Security Survey"; France, "Living environment and safety" survey; Finland, "National Crime Research"

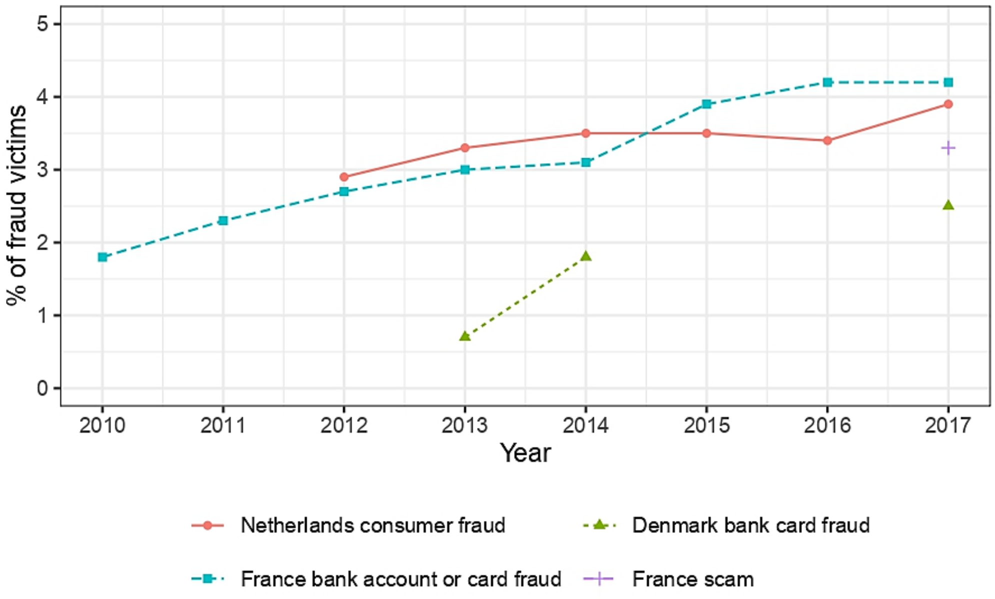

Figure 10. Specific fraud victimisation rates in European victimisation surveys. Source: the Netherlands, "Security Monitor"; Denmark, "Internet Criminality"; France, "Living environment and safety" survey

As a result of the Europe-wide comparison, including one large Spanish region, a conservative, and rather crude, estimate of current individual fraud victimisation rates in Spain would be between 3 and 5% of the adult population. The use of a conservative estimate is justified by the Eurobarometer[28] on Internet security and the European Central Bank data on fraudulent transactions, which indicate that fraud prevalence in Spain may be slightly below the European average. Moreover, this allows a margin for self-selection bias and inaccurate responses as a result of incorrect timings or overestimation of the criminality of the acts.

Although it is difficult to affirm this range of 3 to 5% with great confidence, the estimation can give us an indication of the dark figure of fraud. If, for example, we take the conservative 3% victimisation rate for the adult population (lower than all other European countries analysed even for only one specific fraud type), this would give almost 1.2 million instances of fraud victimisation in Spain[29] for a twelve-month period, compared with 214,000 registered by the Police in 2017. At the top end of the estimated range, a 5% victimisation rate converts to almost 2,000,000 million fraud victims, roughly equal to the total of all offences that are included in the Spanish national crime rate calculation.

At this point, it is worth reiterating that the victimisation surveys do not include reports from organisations, whereas the police statistics should. In other words, the estimate of between 1.1 million and 2 million does not include frauds against organisations, which would undoubtedly increase the figures further.

[28] Special Eurobarometer 480
[29] Based on the Spanish adult population of 39 million on 1 January 2017

In short, it appears fraud in Europe is rising and in Spain its prevalence is rather higher than that recorded by the official statistics and, as a consequence, it is vital that criminal justice and policing policy decision makers are fully aware of this issue when designing and implementing crime prevention strategies.

The Swedish surveys also provide some insight into the nature of fraud growth. Firstly, in Sweden while the volume of reported fraud carried out via the Internet increased 100% between 2010 and 2015 (the 2016 surveys do not include this question), fraud that was not identified with this characteristic dropped only 10%. This indicates that rather than a clear displacement from offline to online, there is merely growth in cyber fraud.

4.6 Reporting rates

Some victimisation surveys also include questions on fraud reporting rates which may assist in further illuminating the dark figure of fraud. As can be seen in Table 3, although the rate varies between countries, it can be concluded that in general fraud reporting rates are very low, with approximately only 20 to 25% of frauds against individuals being reported to the Police. In the most recent Catalan survey, fraud is the least reported economic offence with only 21% making a formal report in comparison to 38.4% for the other property crimes included in the survey. This provides further salient evidence that the official crime statistics are insufficient with regards to estimating the threat that fraud presents to society in the Internet era.

Table 3. **Fraud reporting rates by region.**

Region	Source	Crime	Year	Fraud reporting rate (%)	Average reporting rate for other property crimes (%)
Catalonia	Catalan Public Security Survey	Fraud	2017	21.0	38.4[a]
England & Wales	Crime Survey for England & Wales	Fraud	2017	19.0	58.0[b]
France	French National Victimisation Survey	Bank fraud	2017	26.0	49.6[c]
Netherlands	Weijer, Leukfeldt and Bernasco (2018)	Online consumer fraud	2018	24.0	55.5[d]
Luxembourg	Luxembourg National Security Survey	Consumer fraud	2009-2013	22.4	54.9[e]

[a] Vehicle related theft, burglary, robbery and other thefts.

[b] Theft from the person, other theft of personal property, burglary, other household theft, vehicle-related theft, bicycle theft.

[c] Burglary, thefts related to vehicles, bicycle theft, robbery.

[d] Burglary, theft from car, bicycle theft, robbery and pickpocketing

[e] Burglary, theft from a car, robbery, theft of personal property, bicycle theft.

Fraud reporting rates are considerably lower than other types of property crime in all the surveys providing this information. Table 3 also details crime reporting rates for other property crimes. Depending on the survey, these are a combination of vehicle theft, theft from a car, theft of a bicycle, burglary, attempted burglary, robbery and theft of personal property. For instance, in the case of England and Wales, the other property crimes were reported at a rate three times higher than fraud, 59% to 19%. Or, in the Netherlands, 55.5% reported traditional property crimes in comparison to 24% for consumer fraud.

Some surveys provide information on victims' motivations for reporting or not reporting to the police. Table 4 shows that the main reasons for reporting are related to the moral duty to report, punishing offenders, preventing reoffending and recovering losses. On the other hand, Table 5 shows that victims decide not report primarily due to the insignificance of the event, the complexity of the reporting process and a lack of confidence in police ability to respond adequately. In this sense, we can see both that both private costs and intrinsic and extrinsic benefits (Bowles, Garcia Reyes, and Garoupa 2009) are taken into account when individuals decide whether to report.

Table 4. **Reasons for reporting fraud to police**[30]

Region	Source	Crime	Year	Most common reason for reporting	2nd most common	3rd most common
France	French National Victimisation Survey	All fraud except bank fraud	2017	Identify and punish offenders	Obtain reimbursement from offenders	Stop offenders reoffending
Germany	German Victimisation Survey (2019)	Online consumer fraud	2017	Crime should be reported	So offenders are punished	So it does not happen again

Table 5. **Reasons for not reporting fraud to police**[31]

Region	Source	Crime	Year	Most common reason	2nd most common reason	3rd most common reason
Catalonia	Catalan Public Security Survey	Fraud	2017	Too complicated, could not be bothered, too much bureaucracy and time	Not significant	The police cannot do anything
Germany	German Victimisation Survey	Online consumer fraud	2013-2017	The incident was not serious enough	Police could not or would not have done anything	Victim or family solved the matter
Luxembourg	Luxembourg National Security Survey	Consumer fraud	2009-2013	Did not see the need, felt it would have been useless	Not serious Enough	Not enough evidence to involve the police

[30] It should be noted that not all surveys employ the same list of items when asking for reasons for reporting

[31] It should be noted that not all surveys employ the same list of items when asking for reasons for not reporting

4.7 Discussion

The evidence presented in this paper points to fraud being one of, if not, the most prevalent property crimes in the cybercrime era. Combining secondary data sources, which has been identified as an effective strategy for analysing crime patterns (Tilley, et al., 2018), allowed fraud trends to be identified thereby making an important contribution to crime trend research. A more accurate depiction of this crime reality is necessary for many reasons (Smith, 2010). Firstly, criminologists and other academics require evidence to inform debate, research and policy. A necessary first step in much crime research is understanding the extent of the problem. Secondly, governments make claims about their ability to protect citizens from crime, yet the evidence provided suggests citizens are currently underprotected with regards to fraud. Crime data enables governments and other criminal justice institutions to be held accountable for crime control policy since evaluations of crime trends permit evaluations of prevention strategies. Similarly, identifying the prevalence of criminal activity enables criminal justice institutions and other public institutions involved in crime control to better allocate resources both in the short term and with regards to long-term strategies and policy. Finally, highlighting increases in cyber fraud can encourage the organisations involved in ICT design and supply to produce and use products that do not expose users to unnecessary risks by creating crime opportunities. To foster safety by design, evidence must be provided that shows products and systems are failing the user. If, as this paper suggests, somewhere between 3 and 5 percent of the Spanish adult population are currently falling victim to fraud every 12 months, the failure is lucid. Even more so when taking into account that fraud can have significant negative consequences on victims, both financially and in terms of physical and mental well-being (Cross, 2018a).

The low levels of fraud reporting to the police combined with even lower rates of investigation and prosecution (Fiscalía General del Estado, 2019) reiterate the changing role of the police and the criminal justice system regarding crime control in the Internet era. The police have generally taken it for granted that they are the main actor in prevention, but this is not necessarily the case in the modern era (Wall, 2007/10). In fact, the role of police is reduced with regards to detecting, preventing and investigating cyber fraud. Various studies have highlighted the insufficient training of police officers to deal with cybercrimes (Leukfeldt et al., 2013; Webster & Drew, 2017), meaning investigations are often not even considered. The limitations regarding resources and a traditional organisational culture that is not conducive to change are combined with jurisdictional issues to put much technology-related crime out of the grasp of the public police. In this sense, and as many authors have previously noted (For example: Dupont, 2017; Levi & Williams, 2013; Wall, 2007/10), policing crimes that involve the Internet requires a multi-agency response that goes beyond traditional reactive investigations. Security networks which involve cooperation and partnerships between the police, other government institutions, the private sector as well as end-users should be created or enhanced. Responsibilizing the private sector may be particularly effective as increased criminal opportunities can be a negative externality of private sector activity (Tilley, 2018). This is not to say that traditional law enforcement bodies have no role in cybercrime prevention but, rather, to emphasize that they must form part of multistakeholder and transnational approaches that bring together different capabilities and resources.

4.8 Conclusions

The evidence presented in this paper indicates fraud is rising both in Spain and Europe. Property crime trends are undergoing significant changes, as traditional offences are decreasing while fraud, which can be enhanced and assisted by information and communication technology, displays an upward trend. As shown by comparing official fraud statistics, financial sector statistics and victimisation surveys from Spain and throughout the European Union, fraud appears to be one of the most prevalent offences in the Internet era. As a result, it requires a suitable response from the institutions charged with crime control policy.

Contrary to expectations, there is evidence to suggest that fraud displacement from traditional to cyber is not sufficient to explain the increase in Internet-based fraud. Traditional fraud has only decreased slightly while fraud involving a cyber element has demonstrated a strong upward trend. This trend is likely to continue as more transactions and banking are carried out online. It may be the result of new criminal actors or that the crime opportunities provided by cyber space have prompted changes in the modus operandi of existing fraud perpetrators.

By comparing official Spanish police statistics with Bank of Spain fraud statistics and self-reported victimisation it appears there is considerable underreporting with regards to fraud. This represents a basic yet extremely salient challenge to those involved in prevention and policing: the unknown cannot be prevented or policed.

The underreporting of fraud found in this investigation indicates that the overall crime rate in Spain may be considerably higher than the current MIR figure. If, as the evidence suggests, there are well over 1 million fraud victims in Spain every year, property crime could potentially be 100% higher than the official figure. On the other hand, the inclusion of fraud in the overall crime total may increase this by over 50%, since the MIR calculation gives a total of approximately 2 million criminal acts in Spain. Furthermore, contrary to the official Spanish government position and much academic literature, a property crime rise may even have taken place in Spain in recent years.

The data employed in this study has its limitations, such as possible definitional differences, reporting biases and limited data points. In response to these limitations, firstly, to minimize definitional differences a broad fraud definition has been employed. Secondly, the increasing fraud trend may be partially explained by increasing awareness of the problem and therefore increased reporting, but the data suggests that it is only cyber fraud that is rising, and fraud reporting remains particularly low according to the victimisation surveys. Finally, with regards to trends, the measurement of fraud by central banking institutions and victimisation surveys is recent and therefore the time period is short. However, this means the data provides new perspectives on property crime and, moreover, this is one of the first attempts to include Spain, the fifth largest country in the EU, in European crime trend analysis. This initial insight into fraud trends may provide a blueprint for future research.

The aim of the study was not to categorically deny the existence of a property crime drop in Spain, but rather to suggest that it is unclear in the digital age, to highlight differences in crime types and to show fraud can add to the analysis. This is especially salient for public police forces that should be aware of their limitations in the Internet-era and avoid simplistic conclusions when evaluating their performance and deciding where to focus resources.

-blank page-

CHAPTER V FRAUDE ONLINE VS. OFFLINE: FACTORES PREDICTORES DE VICTIMIZACIÓN Y SU IMPACTO

5.1 Introducción

El fraude a personas, y en especial sus modalidades online, ha sido descrito recientemente como un fenómeno creciente y extremadamente prevalente (Levi, 2017; Tcherni et al., 2016). Tanto es así, que ya se ha llegado a afirmar que el fraude es el crimen contra la propiedad más prevalente (Williams, 2016). En el contexto español, entre 2012 y 2017 el número de transacciones fraudulentas registradas por el Banco de España aumentó casi 100% en cifras absolutas y más del 100% en relación con el importe, alcanzando la cifra de 88 millones de euros en el 2018 (European Central Bank, 2018). En el mismo periodo, el número de estafas conocidas por los cuerpos policiales españoles creció alrededor del 130%[32]. Consecuentemente, existe una necesidad saliente de elaborar sólidas estrategias de prevención y respuesta basadas en la evidencia. Este proceso pasa por dibujar una imagen clara del problema y explorar el efecto de los factores asociados a la victimización. Lamentablemente, tal y como afirman algunos autores, los datos sobre victimización por fraude escasean en la era digital (Levi et al., 2017), dificultando la investigación empírica.

Aunque es posible que no dispongamos de todos los datos, ni de los de mejor calidad, lo

[32] Datos disponibles en el Portal Estadístico en la página web del Ministerio del Interior: https://estadisticasdecriminalidad.ses.mir.es/

que sí sabemos es que el fraude está siendo impulsado por el fomento de las oportunidades criminales del ciberespacio gracias a las características que lo definen, tales como la transnacionalidad, el anonimato, y, actualmente, las escasas barreras tecnológicas para iniciar una carrera delictiva (Button & Cross, 2017b; Holt & Bossler, 2015; Miró-Llinares, 2012; Yar & Steinmetz, 2019). Estos factores -y otros- fomentan que el contacto inicial entre las víctimas de fraude y sus agresores a menudo comience online y que adopte muchas formas. Sirvan de ejemplo las modalidades de fraude en tarjeta de crédito -con o sin presencia física de la tarjeta- que preocupan a Europol (2018), el creciente fraude en compra online (van Wilsem, 2013), el fraude telefónico que ha sido señalado como una seria amenaza (Policastro & Payne, 2015), y el robo de identidad que ya parece haberse generalizado (Golladay & Holtfreter, 2017).

La literatura científica ya puso de relieve cuáles eran algunos de los predictores de la victimización por fraude offline (por ejemplo: Schoepfer & Piquero, 2009; Titus et al., 1995; Van Wyk & Mason, 2001), y más recientemente ha analizado como afectan distintos factores a la victimización por fraude online (Correia, 2019; Leukfeldt & Yar, 2016; Whitty, 2019). Sin embargo, hasta donde alcanza el conocimiento de los autores, ningún trabajo ha examinado cómo varía el efecto de distintos predictores de la victimización entre el fraude online y offline en una misma muestra mediante metodologías cuantitativas. Un estudio de tales características permitiría responder a la siguiente pregunta: ¿es recomendable implementar campañas de concienciación de amplio espectro para prevenir el fraude o es preferible dirigir las campañas a grupos poblacionales concretos para formas de fraude específicas? Por otra parte, aunque se ha destacado que tanto el fraude offline (Titus & Gover, 2001) como el online (Bossler et al., 2020) causan daños considerables en las víctimas, la investigación sobre el efecto de los factores sociodemográficos sobre las consecuencias de sufrir una victimización de este tipo es escasa. ¿Qué factores son predictores de mayores pérdidas económicas o de un daño psicológico mayor? Responder a esta pregunta para ampliar el conocimiento sobre el impacto de la victimización por fraude puede ayudar a promover y mejorar los servicios de asistencia a las víctimas, que han sido calificados recientemente como escasos (Cross, 2019b). El presente trabajo pretende abordar estas carencias examinando cuantitativamente el efecto de los factores sociodemográficos sobre la victimización por fraude online, telefónico y en persona, así como de los factores asociados al impacto sufrido en consecuencia.

Con este objetivo, el trabajo comienza revisando la literatura actual sobre victimización por fraude y su impacto. Posteriormente se enumeran las hipótesis planteadas para el estudio, se describe la muestra utilizada, y las técnicas de análisis escogidas para el contraste de hipótesis. A continuación, se presentan los resultados del análisis estadístico en relación con las hipótesis planteadas y apoyados con técnicas de visualización de datos. Por último, la discusión y conclusiones giran en torno a las implicaciones prácticas del presente trabajo en materia de prevención del fraude y asistencia a las víctimas.

5.2 Estado de la cuestión

5.2.1 Victimización por fraude

Aunque ya son varios los estudios que han examinado los factores sociodemográficos asociados con la victimización por fraude offline, los resultados son poco consistentes y resulta difícil componer un perfil del defraudado (Holtfreter et al., 2008).

Posiblemente la edad sea el factor que ha generado mayor consenso entre los investigadores, habiéndose identificado -quizá de manera contraintuitiva- una mayor probabilidad de sufrir fraude offline en las personas jóvenes (Schoepfer & Piquero, 2009;

Titus et al., 1995; Van Wyk & Mason, 2001). Es posible que tal circunstancia se deba a una mayor propensión para socializar y asumir riesgos (Van Wyk & Mason, 2001). Además, Titus y colaboradores (1995) también encontraron que los jóvenes sufren mayores pérdidas económicas que las víctimas de mayor edad. Pero más allá de la edad, el perfil sociodemográfico de las víctimas de fraude es impreciso y está moldeado por una miríada de factores que -en el mejor de los casos- ha encontrado un respaldo científico eventual. Así, mientras la investigación de Copes y colaboradores (Copes et al., 2010) concluye que un nivel de educación más bajo está relacionado con menor probabilidad de sufrir una victimización y que las mujeres tienen una mayor probabilidad de ser victimizadas, otros trabajos no han hallado relaciones significativas en tal sentido (Schoepfer & Piquero, 2009; Titus et al., 1995; Van Wyk & Mason, 2001), ni entre otros factores como el nivel de ingresos o la etnia de las víctimas (Schoepfer & Piquero, 2009; Van Wyk & Mason, 2001). Y resultados similares arrojan los estudios sobre fraude telefónico. Por ejemplo, Policastro y Payne (2015) analizan una serie de factores sociodemográficos en relación con los estilos de vida de las personas concluyendo que las únicas variables relacionadas de forma significativa con sufrir una victimización son vivir en un barrio desfavorecido o trabajar a tiempo parcial. Así, reforzando los hallazgos de la literatura sobre fraude offline, los autores no encuentran relación entre otras variables demográficas como el nivel de ingresos o las actividades cotidianas y la victimización por fraude telefónico.

Ante la dificultad por determinar cuáles son los predictores sociodemográficos de la victimización por fraude offline y fraude telefónico, algunos autores han apuntado a la granularidad del análisis como uno de los posibles problemas. Schoepfer y Piquero (2009) subrayan la posibilidad de que los perfiles de las víctimas cambien en función del tipo de fraude que sufran. En este sentido, los autores indican que determinados tipos de fraude, como el telefónico o los *scams* que ofrecen premios gratuitos, son más comunes entre los desempleados o los estudiantes. En la misma línea, Copes y colaboradores (2010) discuten que la relación entre la etnia, el nivel de ingresos, y la victimización, puede variar en función de la modalidad de fraude que se estudie. Y es que, como se ha venido señalando, no existe una única modalidad de fraude, sino muchas formas de defraudar, tanto offline como online.

Ahora bien, los estudios sobre victimización por fraude online tampoco muestran resultados concluyentes. Por ejemplo, la literatura existente no ha encontrado relación clara entre el sexo de las víctimas y una mayor probabilidad de sufrir una victimización (Bolimos & Choo, 2017; Junger et al., 2017). Por otro lado, los factores socioeconómicos individuales como el nivel de ingresos, la situación profesional, o los activos financieros tampoco parecen estar relacionados con una mayor probabilidad de ser victimizado por fraude online (Junger et al., 2017; Pratt et al., 2010). Además, otras variables demográficas como el estado civil o la etnia parecen no guardar relación con el hecho de convertirse en víctima (Pratt et al., 2010). Y lo mismo ocurre con el nivel educativo. Frente a los hallazgos de van Wilsem (2013) que sugieren que los individuos con un nivel educativo mayor tienen un mayor riesgo de ser defraudados online, Leukfeldt y Yar (2016) señalan precisamente lo contrario. Y en línea con estos últimos, Junger y colaboradores (2017) destacan que el perfil tradicional de las víctimas jóvenes con un bajo nivel educativo puede no ser aplicable en el caso del cibercrimen.

La investigación sobre edad y victimización por fraude online constituye otro ejemplo paradigmático de obtención de resultados mixtos. Bolimos y Choo (2017) encontraron que las personas mayores tenían un mayor riesgo de convertirse en víctimas y sufrir una pérdida económica mayor. También Whitty (2019) ha identificado la edad como un factor predictor directo y significativo de la victimización por fraude online junto con algunos rasgos que definen una personalidad impulsiva. Pero frente a estos hallazgos, otros estudios han encontrado que existe una relación inversa entre la edad y la probabilidad de sufrir una victimización (Leukfeldt & Yar, 2016; van Wilsem, 2013). Por su parte, Junger y colaboradores (2017) añaden un interesante matiz a la discusión al señalar que el efecto de las variables demográficas puede variar en función del tipo de fraude online objeto de estudio, y señalan que mientras los individuos más jóvenes tienen una mayor probabilidad de ser victimizados por fraude en compra, las personas mayores son más propensas a ser víctimas de fraude en banca online.

Este es un apunte importante, ya que introduce en la discusión el debate sobre la relación entre las actividades cotidianas que realizan las personas y su probabilidad de convertirse en víctimas (Cohen & Felson, 1979). A este respecto, el estudio de Pratt y colaboradores (2010) muestra que los individuos más jóvenes se encuentran en una situación de riesgo significativamente mayor de ser defraudados online, pero que esta relación está mediada por sus actividades cotidianas; es decir, que los individuos más jóvenes tienden a involucrarse en actividades cotidianas que les exponen al fraude. En su estudio, Whitty (2019) también muestra que determinadas actividades cotidianas incrementan el riesgo de convertirse en víctima de *scam*, y resultados similares se desprenden de otro estudio sobre una muestra holandesa cuando se incluyen variables relacionadas con el autocontrol de los sujetos en el análisis (van Wilsem, 2013). A diferencia de los factores sociodemográficos, parece que las actividades cotidianas son un predictor más estable de la victimización por fraude online.

Adoptando un enfoque más ambicioso, otros estudios han comparado los factores relacionados con la victimización online, offline, y también con la no victimización (van de Weijer & Leukfeldt, 2017). El objetivo principal de su análisis se centra en la relación entre los rasgos de personalidad y los resultados de victimización, pero a los efectos del presente trabajo, los autores también presentan resultados interesantes en relación con los factores sociodemográficos de los participantes. En concreto, los investigadores apuntan que los jóvenes y las mujeres tienen una probabilidad significativamente menor de sufrir una victimización por fraude online. Curiosamente, y en contra de las expectativas de los autores, los resultados muestran que aquellos factores de la personalidad que se relacionaban con la victimización online también estaban asociados a la victimización offline.

En conjunto, la literatura muestra una amplia falta de consenso sobre la relación existente entre los factores sociodemográficos y la victimización por fraude, pero ¿qué sabemos sobre el impacto que causa este fenómeno?

5.2.2 Impacto del fraude

Diversas fuentes constatan el inmenso coste económico que supone el fraude para la sociedad. Por ejemplo, el Banco Central Europeo (ECB, por sus siglas en inglés), ha identificado transacciones fraudulentas por valor de 1.800 millones de euros en 2016 (ECB, 2018); el *UK Annual Fraud Indicator* ha estimado un volumen de pérdidas por valor de 190.000 millones de libras esterlinas en 2017, incluyendo 6.800 millones de pérdidas directas que afectan a nivel individual (Button et al., 2018); la Encuesta sobre la Delincuencia en Inglaterra y Gales (CSEW, por sus siglas en inglés) ha estimado más de 3,6 millones de incidentes de fraude en 2018[33]; y en Australia, se han comunicado a Scamwatch más de 107 millones de dólares australianos en pérdidas en 2018[34].

La investigación ha mostrado que las pérdidas económicas son una de las mayores

[33] Recuperado de: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2018#increase-in-the-volume-of-fraud-offences-in-the-last-year (último acceso: 26 de julio de 2019).

[34] Recuperado de: https://www.scamwatch.gov.au/about-scamwatch/scam-statistics?scamid=allydate=2018 (último acceso: 26 de julio de 2019).

preocupaciones para las víctimas de fraude (Button et al., 2014) y que, de hecho, las cifras conocidas pueden subestimar el alcance de tales pérdidas puesto que existe una importante cifra negra (Cross & Blackshaw, 2015; van de Weijer et al., 2018). Además de las pérdidas económicas sufridas por las víctimas de fraude, se ha señalado que el tiempo invertido y los costes económicos derivados de la recolección de pruebas para la denuncia, así como el contacto con las fuerzas del orden, y la participación en el proceso judicial correspondiente también se consideran costes derivados de la victimización (Bowles et al., 2009). Más allá del impacto inicial, la victimización por fraude también puede acarrear impactos secundarios como la pérdida del hogar, un empeoramiento de la calificación crediticia, o un incremento de las deudas (Button et al., 2014). También se ha apuntado que los costes indirectos del fraude y los costes derivados del pago de tasas judiciales pueden ser incluso mayores que los directos (Anderson et al., 2013). En este sentido, el mero hecho de disponer de agentes de policía para registrar todas las denuncias por fraude puede conllevar un coste significativo.

Aunque el impacto negativo más evidente para una víctima de fraude es el económico, las víctimas también son vulnerables al impacto psicológico y a otras consecuencias adversas (Schoepfer & Piquero, 2009). Por ejemplo, el impacto emocional y psicológico del fraude también puede derivar en estrés, ira, vergüenza, y malestar (Button et al., 2014; Cross et al., 2016). De hecho, en algunos casos incluso se han encontrado efectos negativos a nivel físico (Spalek, 1999). Algunos autores han subrayado que la relación entre las pérdidas económicas y el impacto económico, psicológico y emocional no siempre está muy clara y que, en algunos casos, varía en función de la situación económica de la víctima u otras variables (Button et al., 2014; Cross et al., 2016). En este sentido, es posible que las pérdidas económicas tengan un impacto mayor en personas jubiladas debido al malestar causado por la pérdida de la estabilidad e independencia económica o los ahorros reservados para la herencia de los hijos (Deevy et al., 2012).

Además, existe una cultura de culpabilización que estigmatiza a las víctimas como avariciosas o ingenuas, y que se suma a las consecuencias anteriormente descritas (Cross, 2019). Esta cultura puede aumentar la probabilidad de que las víctimas consideren no haber sufrido un delito, y de que se responsabilicen a sí mismas en lugar de al propio autor. En este sentido, se ha señalado que uno de los motivos principales por el cual no se denuncia el fraude en Internet es precisamente no reconocer haber sido víctima de un delito (Button y Cross, 2017).

En cuanto a los factores predictores del impacto sufrido como consecuencia de la victimización, la investigación sobre victimización offline muestra que el sexo femenino es un predictor de un mayor malestar psicológico como consecuencia de sufrir un robo callejero (Gale & Coupe, 2005) y un robo en vivienda (Maguire, 1980). En este mismo estudio, Maguire (1980) encontró que la inseguridad percibida también puede influir negativamente en la forma de afrontar una experiencia de victimización. Por otro lado, el análisis cuantitativo más comprehensivo realizado hasta la fecha sobre el impacto del fraude online fue llevado a cabo por Golladay y Holtfreter (2017). En su estudio sobre víctimas de robo de identidad los autores han encontrado que el impacto negativo que produce el fraude no es solamente económico, sino también emocional y físico. Dicho estudio muestra que una victimización previa por robo de identidad puede predecir consecuencias emocionales adversas, del mismo modo que otros factores como el volumen de pérdidas, la edad, y la etnia. Por el contrario, un elevado nivel de ingresos constituye un factor de protección frente a tales consecuencias. Respecto a las consecuencias físicas adversas, haber experimentado un robo de identidad se constituye como predictor. El estudio también muestra que estar casado y tener un elevado nivel de ingresos se relaciona inversamente con sufrir consecuencias físicas adversas tras la experiencia de victimización. Los autores concluyen subrayando la importancia de la investigación sobre el impacto del fraude como fuente de información para las estrategias de asistencia y tratamiento de las víctimas.

5.3 El presente estudio

Considerando el estado del arte de la investigación sobre fraude -tanto online como offline-, sus factores predictores y el impacto que causa en las víctimas -económico, psicológico y físico-, así como las carencias detectadas en la literatura, el presente trabajo pretende responder a las siguientes dos cuestiones: ¿cuáles son y cómo se diferencian los factores sociodemográficos predictores de la victimización por fraude en función de sus modalidades offline -en persona y telefónico- y online? y ¿qué factores están asociados con experimentar mayores molestias, así como un mayor impacto económico y psicológico tras una victimización por fraude?

Para ello, se formulan las siguientes hipótesis:

H_1 Los factores sociodemográficos predictores del fraude en persona y telefónico son distintos a los predictores del fraude online.

H_2 Algunos factores sociodemográficos son predictores de mayores molestias y de mayor impacto tanto económico como psicológico derivado del fraude.

Además, se plantea una hipótesis adicional que pretende contribuir a comprender mejor la percepción de las víctimas sobre su experiencia de fraude en España.

H_3 La consideración del fraude sufrido como delito depende del impacto económico y psicológico causado.

5.3.1 Muestra

La muestra proviene de las dos últimas ediciones, de 2015 y 2017, de la Encuesta de Seguridad Pública de Cataluña (ESPC) que se administra cada dos años en esa región. Cataluña es una Comunidad Autónoma con 7,6 millones de habitantes en el noreste de España, una cifra que representa alrededor del 16% de la población del país. La ESPC de 2015 fue administrada telefónicamente entre noviembre y diciembre a 6.214 participantes. La ESPC de 2017 también fue administrada entre noviembre y diciembre, tanto telefónicamente, a 5.918 participantes, como de forma autoadministrada a través de Internet, con 1.958 participantes. Ambas ediciones de la encuesta utilizaron un sistema de muestreo aleatorio con respuestas ponderadas para lograr la representatividad de la población de Cataluña[35].

En la ESPC se pregunta sobre experiencias de victimización y denuncia de una serie de delitos, así como sobre la percepción de seguridad a nivel local y las opiniones sobre las fuerzas del orden público. La muestra seleccionada para el presente trabajo comprende los registros de los participantes que afirmaron haber sido víctima de fraude en los últimos 12 meses. En la edición de 2015, 530 participantes (8,5%) afirmaron haber sido víctimas de fraude, mientras que, en la edición de 2017, 659 participantes (8,4%) realizaron la misma afirmación. Tras eliminar 12 registros con valores perdidos, la muestra total se compone de 1.177 víctimas de fraude.

[35] La selección de la muestra de la ESPC es aleatoria por sorteo a partir del Registro de población de Cataluña. Se utiliza extracción nominal, estratificada no proporcional con fijación de cuotas por territorio, sexo y grupo de edad. Las cuotas están fijadas en base al Registro de población de Cataluña de la Instituto de estadística de Cataluña. Las cuotas por territorio se basan en la población de las 9 regiones policiales. Se puede consultar la metodología de la encuesta en la presentación de los resultados, disponible en la página web de la Generalitat de Catalunya: https://interior.gencat.cat/web/.content/home/010_el_departament/publicacions/seguretat/estudis_i_enquestes/enquesta_de_seguretat_publica_de_catalunya/enquesta_de_seguretat_publica_de_catalunya_2017/PRESENTACIO-LLARGA-ESPC2017.pdf

5.3.2 Variables

La ESPC incluye preguntas sobre las características demográficas de los participantes como: el sexo, la edad, el lugar de nacimiento, el nivel educativo, la situación profesional, la situación económica, o una posible discapacidad. Además, se pregunta a los participantes qué tipo de fraude sufrieron -si en persona, telefónico u online-, si la víctima considera el acto como constitutivo de delito, el impacto económico -en términos de pérdidas sufridas- y psicológico experimentado, así como las molestias sufridas en consecuencia. El impacto psicológico y las molestias sufridas se miden en una escala de 0-10. Para los objetivos del presente trabajo y con base en la revisión bibliográfica, la pregunta sobre la percepción de la seguridad local también puede ser pertinente para el análisis del impacto de la victimización, por lo que también se ha incluido en el set de datos.

La Tabla 6 muestra las estadísticas descriptivas básicas de las variables seleccionadas para los análisis. Las variables están divididas en cuatro apartados: factores sociodemográficos, percepción, impacto y tipo de fraude. Para las variables cualitativas se muestran las frecuencias y porcentajes correspondientes a cada categoría, mientras que en el caso de las variables cuantitativas se muestra su rango -valores máximo (máx.) y mínimo (mín.)-, su media (M), su desviación típica (DT), y su mediana (Md). Como se indica en la Tabla 1, el fraude en Internet es el tipo más prevalente, representando 35,5% de los casos. El 13,7% de las victimizaciones por fraude no han podido ser incluidas dentro de una categoría registrada; es posible que algunas de ellas hayan ocurrido a través del correo postal. La edad media de la muestra es de 44,4 años con una desviación estándar de 15.

Table 6. **Estadísticas descriptivas de las variables en función de su operativización**

Variables (datos no ponderados)				Total (n = 1177)			
	n	%	mín.	M	DT	Md	máx.
Factores sociodemográficos							
Sexo							
Hombre	597	50,7					
Mujer	580	49,3					
Edad							
De 16 a 25	116	9,9					
De 26 a 40	433	36,8					
De 41 a 64	490	41,6					
Mayor de 65	138	11,7					
Total			17	44,4	15,0	41	90
Lugar de nacimiento							
España	1030	87,5					
Extranjero	147	12,5					
Nivel educativo							
Ninguno o educación primaria	188	16,0					
Educación secundaria	174	14,8					
Bachillerato o formación profesional	348	29,6					
Educación superior	467	39,7					
Situación profesional							
Estudiante	77	6,5					
Desempleado o empleado del hogar	151	12,8					
Jubilado	166	14,1					
Trabajador a tiempo completo	638	54,2					
Trabajador a tiempo parcial	124	10,5					
Otros	21	1,8					
Situación económica							
Muy buena	50	4,2					
Buena	627	53,3					
Ni buena ni mala	101	9,4					
Mala	274	23,3					
Muy mala	115	9,8					
Discapacidad							
Sí	105	8,9					
No	1072	91,1					
Percepción							
Seguridad local			0	6,7	2,1	7	10
El fraude constituye delito							
Sí	804	68,3					
No	373	31,7					
Impacto							
Económico			0	1411,0	12087,0	100	300000
$ln(\text{Económico} + 1)$			0	4,4	2,5	4,6	12,6
Psicológico			0	5,5	3,2	6	10
Molestias			0	7,6	2,4	8	10
Victimización							
Tipo de fraude							
Online	418	35,5					
Telefónico	310	26,3					
En persona	288	24,5					
Otros	161	13,7					

Fuente: datos de victimas de fraude extraídos de la Encuesta de Seguridad Pública 2015 y 2017.

5.3.3 Estrategia de análisis

Para someter a prueba la H_1, se ha categorizado la variable dependiente (VD) de la siguiente forma: si los participantes han sido víctima de fraude en persona -1-, si han sido víctima de fraude telefónico -2-, si han sido víctima de fraude online -3-, si esta información se desconoce -4-. Como variables independientes (VI) se han utilizado los factores sociodemográficos enumerados previamente. La técnica estadística seleccionada para realizar el análisis ha sido la regresión logística multinomial, ya que este tipo de regresión permite comparar más de un variable dependiente.

Para someter a prueba la H_2, se han utilizado las VD discretas ordinales impacto económico, impacto psicológico, y las molestias causadas. Como VI se han utilizado los tipos de fraude, los factores sociodemográficos, así como la percepción sobre la seguridad local. A la hora de modelizar el efecto de los factores seleccionados sobre el impacto psicológico y las molestias causadas, se han incluido como VI las pérdidas económicas -en su operativización cuantitativa-. Para normalizar la distribución de esta variable, se ha aplicado la fórmula $ln(x + 1)$, donde x representa la variable de interés. La técnica estadística seleccionada para realizar el análisis ha sido la regresión lineal, ya que este tipo regresión permite analizar el efecto de las VI sobre una VD discreta ordinal.

Para someter a prueba la H_3, se ha dicotomizado la VD de la siguiente forma: si los participantes consideran haber sido víctimas de un delito de fraude -1-, si no -0-. Como VI se han utilizado los tipos de fraude, los factores sociodemográficos, las consecuencias potenciales de la victimización, y la percepción sobre la seguridad local. En este caso el impacto económico se ha operativizado en intervalos. La técnica estadística seleccionada para realizar el análisis de la VD binaria ha sido la regresión logística binaria.

En la siguiente sección se visualizan los resultados de los modelos a través de los coeficientes B y sus errores estándar. Tanto la transformación como la visualización de los datos se ha llevado a cabo con las funcionalidades que ofrece el paquete tidyverse (versión 1.2.1, Wickham, 2017) en el software libre R (versión 3.6.1) a través de RStudio (versión 1.2.1335). En el Apéndice I se pueden consultar las tablas con los resultados completos.

5.4 Resultados

5.4.1 Hipótesis 1

Para contrastar la H_1 se han examinado las diferencias de los efectos de los factores sociodemográficos sobre los tipos de fraude descritos. Para ello, la técnica de análisis más apropiada es la regresión logística multinomial (Britt y Weisburd, 2010). La Figura 11 sintetiza gráficamente los resultados del análisis, en los cuales actúa como categoría de referencia el fraude online (Coeficiente B = 0). Los resultados muestran que las personas mayores tienen más probabilidad de sufrir una victimización por fraude telefónico o en persona que online, siendo las personas de 41 a 64 años más proclives a sufrir un fraude telefónico (OR = 2,14; $p < 0,05$), y las personas mayores de 65 más vulnerables al fraude en persona (OR = 2,95; $p < 0,05$). Por otro lado, un mayor nivel educativo de los participantes reduce sus probabilidades de sufrir un fraude telefónico y en persona frente a la modalidad online. Concretamente, haber recibido educación superior reduce tales probabilidades con un efecto moderado, pero estadísticamente significativo (OR = 0,42; $p < 0,01$ y OR = 0,38; $p < 0,001$ respectivamente). Pese a que las variables que describen tanto la situación profesional como la situación económica de los participantes muestran un efecto importante sobre el resultado de victimización, el rango que describen sus errores estándar es demasiado amplio, lo que impide extraer una interpretación clara de los resultados. Las categorías de referencia para cada VI se pueden consultar en la Tabla 12 del Apéndice I.

Los resultados obtenidos muestran apoyo para la H1, ya que los predictores de los fraudes telefónico y en persona difieren de los del fraude online en algunos casos.

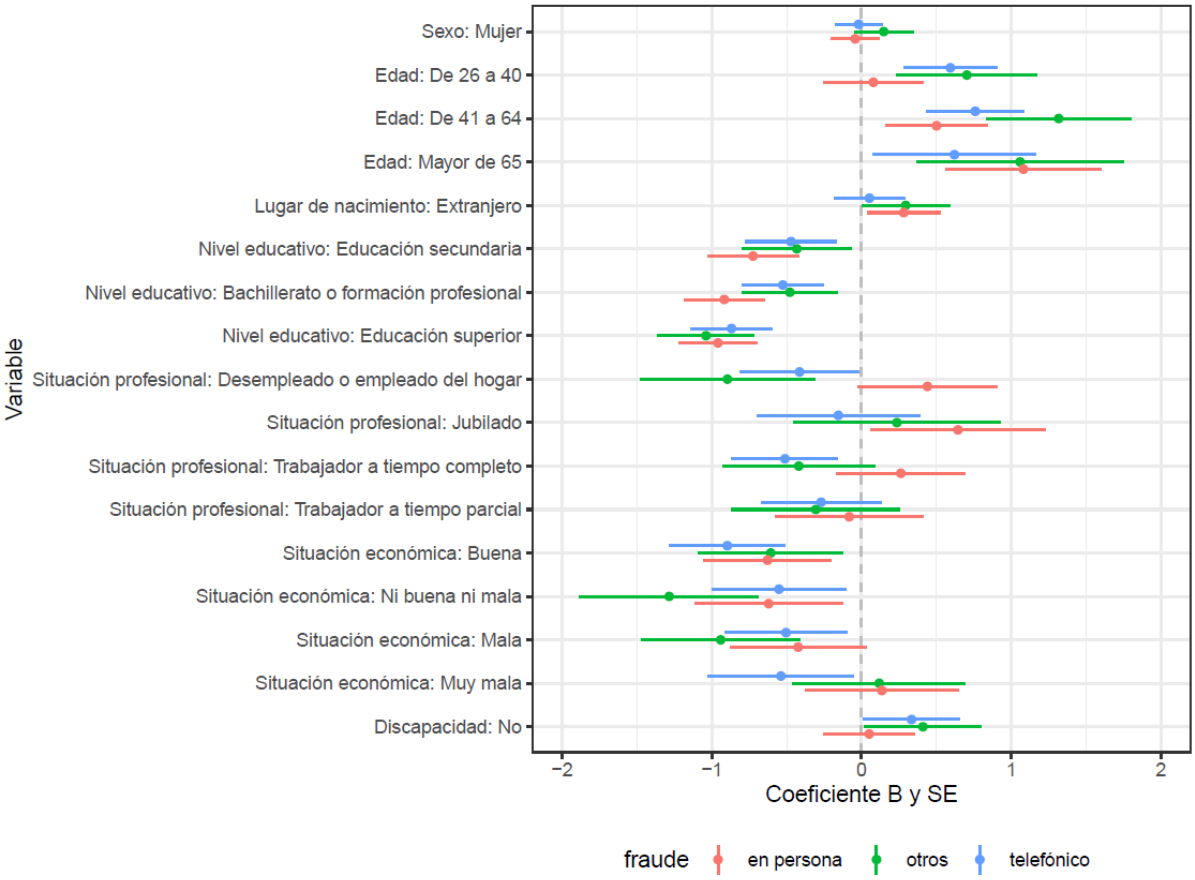

Figure 11. Comparativa de los efectos de las variables demográficas entre los modelos de regresión logística multinomial sobre la victimización por cada tipo de fraude.

5.4.2 Hipótesis 2

Para examinar los factores potencialmente relacionados con el impacto sufrido como consecuencia de la victimización por cada una de las modalidades de fraude analizadas en el presente trabajo, se han ejecutado tres regresiones lineales. La Figura 12 sintetiza los resultados obtenidos describiendo los efectos de las variables en cada modelo.

En cuanto al impacto económico del fraude, y con respecto a ser estudiante, todas las demás categorías que describen la situación profesional de los participantes están asociadas con una probabilidad considerablemente más alta de sufrir mayores pérdidas económicas, ya sean personas desempleadas o empleadas del hogar (OR = 3,64; p < 0,001), jubiladas (OR = 2,75; p < 0,05), trabajadoras a tiempo completo (OR = 3,55; p < 0,001) o parcial (OR = 2,73; p < 0,01). En sentido opuesto, no tener una discapacidad es un factor que reduce moderadamente las pérdidas económicas derivadas del fraude (OR = 0,58; p < 0,05).

Respecto al impacto psicológico, los resultados indican que la victimización por fraude telefónico incrementa significativamente dicho impacto frente a la victimización por fraude online (OR = 1,78; p < 0,05). A diferencia del modelo anterior, en este caso el sexo parece ser un factor determinante del impacto psicológico experimentado por los participantes. Así, ser mujer está relacionado con sufrir un impacto psicológico mayor (OR = 2,02; p < 0,001). Por otro lado, una peor situación económica también se relaciona positivamente con el impacto psicológico sufrido (OR = 0,70; p < 0,001). Y, en relación con lo anterior, mayores pérdidas económicas también generan un impacto psicológico derivado de la victimización significativamente mayor (OR = 1,40; p < 0,001). Frente a los factores de riesgo, también se han encontrado otros de protección. En este sentido, un nivel educativo más alto se relaciona con un menor impacto psicológico (OR = 0,69; p < 0,001). Del mismo modo, una mayor percepción de la seguridad local reduce el impacto psicológico como consecuencia de la victimización (OR = 0,86; p < 0,001).

En relación con el tercer modelo, los resultados indican que los predictores de las molestias derivadas de la victimización son similares a los del impacto psicológico, a excepción del nivel educativo de los participantes y tener una discapacidad que, en este caso, no se relacionan de forma significativa con el resultado. Los resultados del modelo sugieren que los factores que incrementan las molestias sufridas son: el tipo de fraude experimentado -concretamente el telefónico- (OR = 2,15; p < 0,001), ser mujer (OR = 2,17; p < 0,001), encontrarse en una mala situación económica (OR = 0,80; p < 0,001), y haber sufrido pérdidas económicas mayores (OR = 1,37; p < 0,001).

Por último, cabe mencionar que, aunque la variable edad exhibe significación estadística tanto en el modelo del impacto psicológico como de molestias, el tamaño del efecto es ínfimo. Y lo mismo ocurre con la percepción de la seguridad local respecto a las molestias sufridas. Esta circunstancia se puede observar en la Figura 12 cuando los puntos coloreados que representan los coeficientes B de cada variable se encuentran muy próximos al valor 0.

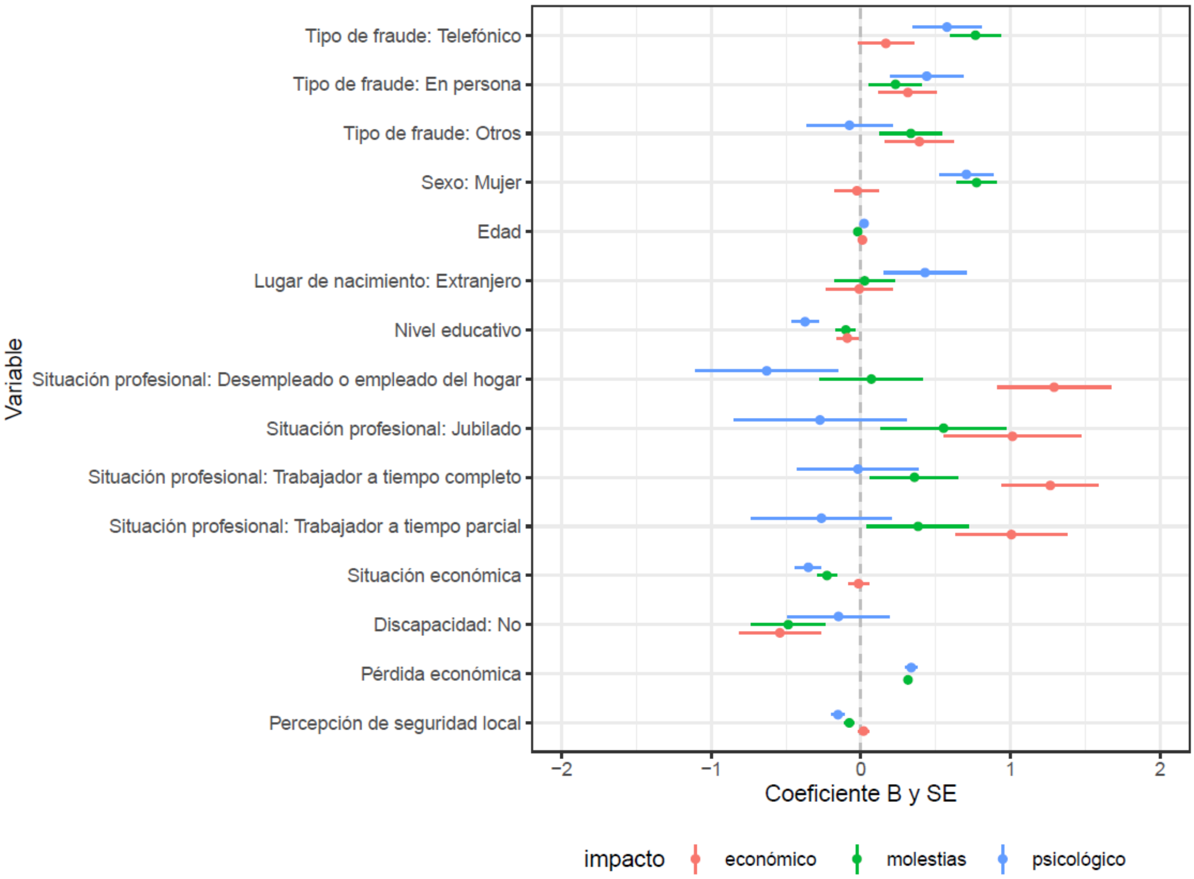

Figure 12. Comparativa de los efectos de las variables de tipo de fraude, demográficas, de impacto y de percepción entre los modelos de regresión lineal sobre el impacto de la victimización.

En síntesis, no se puede afirmar que todas las variables sociodemográficas sean buenos predictores de los distintos impactos derivados de la victimización por fraude, por lo que se debe rechazar la H_2. Ahora bien, el rendimiento de los modelos es sustancialmente mejor en los casos del impacto psicológico (R^2 ajustado = 0,15) y las molestias sufridas (R^2 ajustado = 0,17) que en el de las pérdidas económicas (R^2 ajustado = 0,03), lo que sugiere que los factores sociodemográficos son mejores predictores de los dos primeros impactos.

5.4.3 Hipótesis 3

Tal y como muestran las cifras de la Tabla 14, no todas las víctimas de fraude consideran haber sido víctimas de un delito, lo que sugiere que ciertos factores inciden de forma diferencial en la percepción de los participantes. La Figura 13 ilustra los efectos del conjunto de factores analizados en este sentido. El modelo de regresión logística binomial muestra que, respecto a sufrir un fraude online, experimentar un fraude telefónico o en persona está asociado negativa y significativamente con la percepción de haber sido víctima de un delito (OR = 0,29; $p < 0,001$ y OR = 0,26; $p < 0,001$ respectivamente), es decir, las victimas de fraude online tienen más probabilidad de considerar que los hechos son delictivos. Por otra parte, el impacto psicológico (OR = 1,13; $p < 0,001$), así como las molestias (OR = 1,16; $p < 0,001$) derivadas de la victimización incrementan significativamente las probabilidades de considerar haber sufrido un delito, aunque el efecto de estos factores sobre el resultado es muy pequeño. Por el contrario, los resultados muestran que la magnitud de las pérdidas económicas como consecuencia del fraude no está relacionada con tal consideración. Además, no tener una discapacidad se relaciona con no percibir que la experiencia de fraude es constitutiva de delito (OR = 0,54; $p < 0,05$). Las categorías de referencia para las VI categóricas se pueden consultar en la Tabla 14 del Apéndice I.

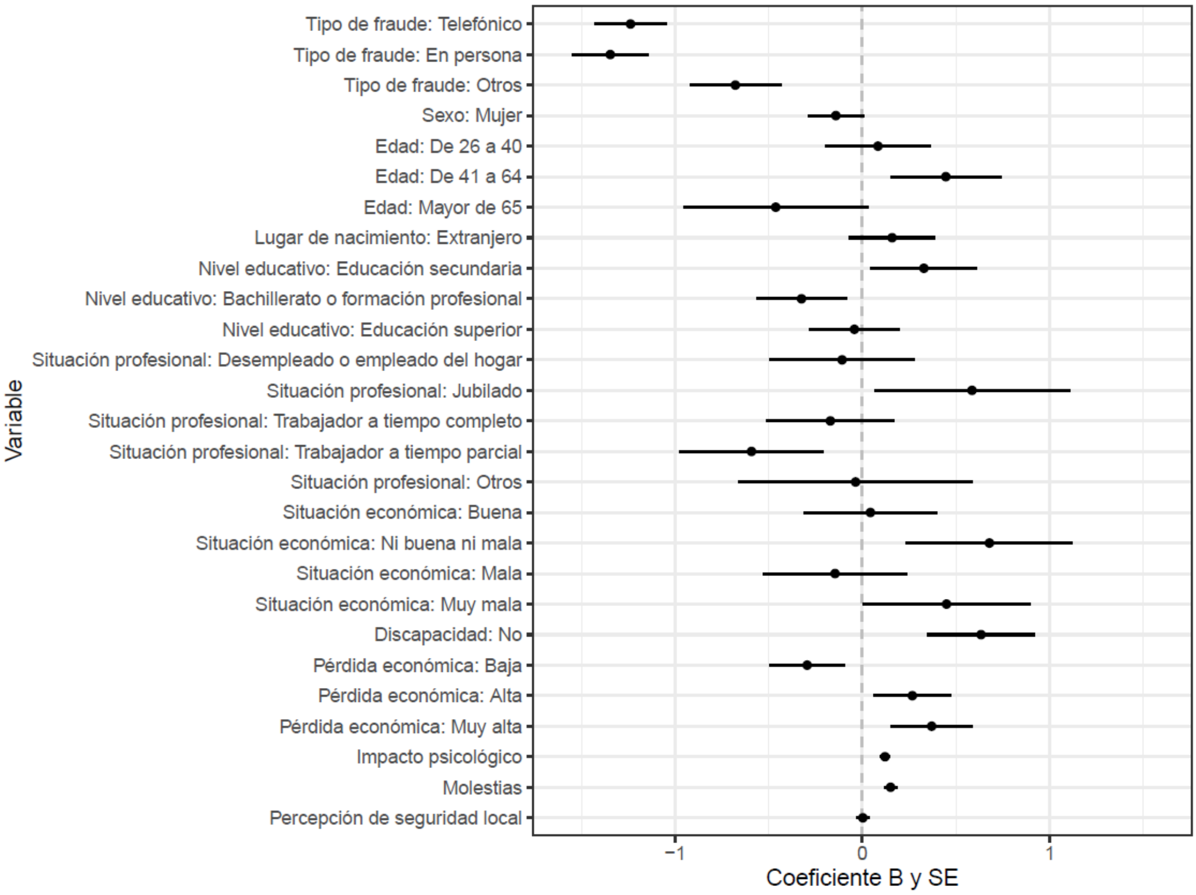

Figure 13. Efecto de las variables de tipo de fraude, demográficas, de impacto y de percepción en el modelo de regresión logística binomial sobre la percepción del fraude sufrido como delito.

En conjunto, los resultados muestran que la consideración del fraude como delito por parte de los participantes no depende de las pérdidas económicas sufridas, pero sí del impacto psicológico y de las molestias experimentadas en consecuencia. Por estos motivos, se debe rechazar la H_3 parcialmente.

5.5 Discusión y conclusiones

En este estudio se han comparado las características de las víctimas de fraude con el tipo de fraude experimentado (online, telefónico, y en persona), el impacto derivado de tal victimización (económico, psicológico y molestias), así como la percepción de haber sido víctima de un delito. A lo largo de las últimas dos décadas se ha discutido mucho sobre las diferencias entre el crimen offline y online y, en este sentido, el presente trabajo contribuye a la discusión mostrando que, en términos de perfiles sociodemográficos de las víctimas, las diferencias son limitadas. Además, el estudio muestra que el impacto del fraude tiene diversos predictores, aunque quizá no sean los esperados. Así, mientras los factores sociodemográficos analizados parecen tener poco poder explicativo del impacto económico, los resultados son considerablemente mejores en los casos del impacto psicológico y las molestias sufridas -si bien es cierto que siguen siendo limitados-.

Cabe destacar que los resultados obtenidos tienen importantes implicaciones en materia de prevención del fraude y políticas de respuesta frente al problema. En primer lugar, se debe enfatizar que mientras la tendencia de aumento del fraude se puede deber a su modalidad online (Caneppele y Aebi, 2017; Levi, 2017), la victimización por fraude telefónico y en persona sigue siendo saliente. Los registros de victimización de la ESPC sugieren que enfocar las campañas de concienciación, estrategias de prevención y recursos de asistencia a las víctimas únicamente a las modalidades de fraude online sería poco acertado, especialmente dado que el impacto psicológico derivado del fraude telefónico parece mayor. Respecto a los perfiles de las víctimas de fraude, al identificar pocos predictores claros los resultados del presente estudio se muestran consistentes con la literatura examinada. Esto implica que, en general, las estrategias de prevención de fraude deberían ser transversales para toda la población. Dicho eso, sobre la base de los resultados del presente estudio podría resultar útil dirigir las campañas de concienciación sobre los riesgos del fraude telefónico y en persona a las generaciones mayores ya que tienen más posibilidad de sufrir este tipo victimización, posiblemente porque utilizan Internet con menos frecuencia y el teléfono fijo con más frecuencia y porque pasan más tiempo en casa.

También resulta interesante destacar cómo los resultados obtenidos en relación con el impacto económico sufrido en función del tipo de fraude experimentado apuntan a los peligros de comparar pérdidas económicas medias entre distintos tipos de delitos. Con la muestra actual, las pérdidas económicas medias son de 986.40€ en el fraude online, 503.99€ en el fraude telefónico, y 1574.50€ en el fraude en persona. Atendiendo a estos datos, se podría concluir fácilmente que las pérdidas económicas son mayores en el fraude en persona. Sin embargo, las medianas arrojan resultados más equidistantes: 80.00€, 100.00€, y 100.00€ respectivamente. El modelo estadístico utilizado en el presente estudio no arroja resultados claros en este sentido, lo que parece indicar que todos los tipos de fraude tienen un impacto económico similar.

En cuanto al impacto psicológico y a las molestias causadas, se han encontrado diferencias significativas con importantes implicaciones para los servicios de asistencia a las víctimas. De modo acorde con la literatura, los resultados indican que los impactos mencionados están relacionados con la situación económica de las víctimas (Button et al., 2014; Cross et al., 2016) y, por tanto, la disponibilidad de los servicios de asistencia a las víctimas no debería depender únicamente de las pérdidas económicas sufridas en términos absolutos, ya que algunas víctimas están sufriendo un impacto psicológico grave debido a unas pérdidas económicas relativamente escasas. La victimización también se experimenta de forma distinta en función del género o el nivel educativo, lo que sugiere que, si los recursos son escasos para asistir a todas las víctimas de fraude, estos podrían ser redistribuidos hacia perfiles específicos y tener en cuenta la perspectiva de género. En cualquier caso, los resultados muestran claramente que el impacto la victimización afecta de manera desigual, lo que significa que idealmente los servicios de asistencia a las víctimas deberían estar preparados para atender cada caso de manera individualizada. Finalmente, las personas que perciben una mayor inseguridad local tienen mayores probabilidades de sufrir un mayor impacto psicológico como consecuencia de la victimización. Esto representa otra prueba de que no se puede entender el espacio físico y el espacio virtual como espacios aislados en cuanto a la delincuencia (Miró-Llinares, 2012).

Los resultados muestran que es más probable que las víctimas de fraude online consideren el fraude experimentado como un delito, lo que resulta poco coherente dado que el impacto psicológico y las molestias sufridas son mayores en las modalidades de fraude telefónico y en persona. Esto sugiere que el fraude online se percibe más como un delito, posiblemente como resultado de un proceso de normalización del fraude tradicional. Por tanto, sigue siendo necesario comunicar a los ciudadanos que los fraudes tradicionales continúan siendo lesivos y que deben denunciarse ante la policía y otras organizaciones competentes.

Este estudio también cuenta con algunas limitaciones relacionadas con los datos y la metodología utilizados. En primer lugar, sería interesante realizar un estudio similar con un conjunto de datos mayor para cada tipo de fraude, lo que podría revelar distintos predictores de la victimización y el impacto sufridos. Asimismo, podría ayudar a mejorar el rendimiento de los modelos estadísticos empleados. En segundo lugar, la codificación del tipo de fraude sufrido depende de la opinión de los participantes de la ESPC. Y es que se debe tener en cuenta que muchos de los fraudes son híbridos entre las modalidades online y offline (Caneppele y Aebi, 2017), lo que no parece quedar claro en los datos disponibles de la ESPC. Por ejemplo, algunos fraudes pueden comenzar inicialmente vía telefónica, pero después materializarse online. Esta circunstancia no ha sido recogida en la ESPC. En tercer lugar, se debe destacar que la variable situación económica se mide de forma subjetiva en la ESPC; es decir, los participantes no son preguntados por su nivel de ingresos, sino por cómo llegan a fin de mes. Es posible que los resultados de los análisis varíen si la situación económica fuera medida adicionalmente a través del nivel de ingresos, ya que parece improbable que los participantes que fueran incluidos de esta forma en el grupo de bajos ingresos percibidos pudieran ser víctimas de fraudes que supusieran grandes pérdidas económicas por motivos evidentes. Cuarto, es necesario apuntar que la investigación solo examina el fraude contra individuos y, por lo tanto, solo una parte del fenómeno. Futuros estudios podrían analizar las características de la victimización en el sector privado. Penúltimo, desafortunadamente la ESPC no recopila información sobre las actividades cotidianas de los participantes. La literatura revisada para el presente estudio apunta que estos factores pueden ser relevantes para explicar la victimización por fraude y, por lo tanto, se recomienda realizar investigaciones en España en esta línea. Finalmente, por cuestiones de acceso a la muestra el presente estudio no compara las víctimas del fraude con el conjunto de datos de la ESPC, lo cual representa una interesante línea para futuras investigaciones.

-blank page-

CHAPTER VI FRAUD REPORTING IN CATALONIA IN THE INTERNET ERA: DETERMINANTS AND MOTIVES

6.1 Introduction

As we start to learn more about Internet-era rising fraud trends (Levi, 2017; Tcherni et al., 2016) and the characteristics and routine activities that can help predict victimisation (Copes et al., 2010; Leukfeldt & Yar, 2016; Ngo & Paternoster, 2011; Pratt et al., 2010; van de Weijer & Leukfeldt, 2017; Whitty, 2019; Williams, 2016), it is also pertinent to continue researching the difficulties to combat the issue. The increased criminal opportunities in cyberspace related to, for example, transnationality, anonymity and low technological barriers to entry (Holt & Bossler, 2016; Miró-Llinares, 2012) represent a lucid impediment to fraud policing. A lack of preparedness to deal with online fraud has also been found in public police forces (Correia, 2019; Bossler et al., 2019; Hadlington et al., 2019). Yet, one of the most basic and, at the same time, biggest challenges to Internet-era fraud prevention and policing is relatively old. The issue of fraud underreporting was highlighted last century (Titus et al., 1995), is still very relevant today (Button & Cross, 2017; Caneppele & Aebi, 2017) and represents a salient impediment to police knowledge (van de Weijer et al., 2018).

Crime reporting and, therefore, reliable statistics are important for many reasons (Reep-van den Bergh & Junger, 2018). Firstly, they enable police and policymakers to understand crime trends (Baumer & Lauritsen, 2010; Bowles et al., 2009). In this sense, effective reporting provides more reliable data for the design and evaluation of crime prevention strategies (Copes et al., 2010; Isenring et al., 2015) and the allocation of resources (Torrente et al., 2017). More generally, reliable crime statistics also serve to inform public and academic debate (Reep-van den Bergh & Junger, 2018). Finally, crime reports are also often necessary to start police investigations (van de Weijer et al., 2018).

The present study deals with fraud in Catalonia, Spain, where fraud types appear to not differ greatly from those identified in international criminological literature (Kemp et al., 2020; Levi, 2017). Unfortunately, academic data is scarce, but data obtained from the Catalan police shows a 67% increase in reported bank card fraud in 2017 compared to 2016[36], while the head of the Catalan Cybersecurity Agency has recently highlighted a large increase in phishing attempts (Torruela, 2020). Many of these phishing attacks are related to typical frauds such as consumer products fraud, investment fraud, employment fraud, or charity fraud that have been adapted to take advantage of the fear and uncertainty generated by the coronavirus pandemic. It has also been noted that while online fraud in Catalonia has increased in recent years, offline fraud still makes up a considerable percentage of fraud victimisation (Kemp & Moneva, 2020). In this sense, Catalan police recently broke up an organised crime group that had defrauded more than half a million euros from elderly victims over the phone (Morena Cusac, 2020). As discussed later, fraud reporting rates in Catalonia are low, as in many other countries.

Various international sources show the immense financial costs of fraud for today's society, for example: the European Central Bank identified fraudulent transactions using bank cards worth €1.8 billion in 2016 (ECB, 2018); the UK Annual Fraud Indicator estimated losses of £190 billion for 2017, including £6.8 billion direct losses to

[36] Data requested from Catalan Ministry of Home Affairs.

individuals (Crowe, University of Portsmouth & Experian, 2018); the Crime Survey for England and Wales estimated well over 3 million fraud victims in 2018[37]; and in Australia, more than AU$107 million in losses were reported to Scamwatch in 2018[38]. In addition to direct losses suffered by crime victims, the time and monetary costs of collecting evidence, contacting the police and other relevant institutions or participating in judicial processes should also be considered (Bowles et al., 2009). Furthermore, fraud can have significant emotional, psychological or even physical impact on victims (Button et al., 2014; Cross et al., 2016; Golladay & Holtfreter, 2017). Given the consequences of fraud and its position as one of the most prevalent offences in the Internet era, it is vital to understand the factors associated with fraud reporting. Obtaining the clearest possible image of this costly issue through victim reporting is a fundamental first step to improving prevention and policing strategies.

Previous studies have stressed the need for further research into fraud victimisation reporting (Copes et al., 2001; Schoepfer & Piquero, 2009) as well as cybercrime reporting in general (Leukfeldt, 2017). In fact, the present study responds to three of the specific calls for further research by van de Weijer, Leukfeldt and Bernasco (2018): analysis of the influence of criminal event characteristics on the decision to report cybercrime; comparisons between reporting of cyber and traditional crimes that are substantially similar, such as online and offline fraud; and, examinations of the motives for reporting or not. The need to examine the reasons that drive fraud reporting or not reporting is also noted by Schoepfer and Piquero (2009). In response to these calls, this study seeks to

[37] Retrieved from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2018#increase-in-the-volume-of-fraud-offences-in-the-last-year
[38] Retrieved from: https://www.scamwatch.gov.au/about-scamwatch/scam-statistics?scamid=allanddate=2018

analyse factors that may influence online and offline fraud reporting and the reasons for not reporting.

Over the last twenty years there has been considerable debate regarding whether cybercrime is ‘old wine in new bottles’ (Grabosky, 2001). The analysis in the present paper compares online and offline fraud reporting in order to add to both this academic debate regarding the online/offline crime a/symmetry as well as the evidence base for the design of policies aimed at fostering fraud reporting. The paper begins by examining the current literature on crime reporting in general, and cybercrime and fraud reporting more specifically. The data, hypotheses and methods for the present study are then detailed. Next, the results of the statistical models are presented with regard to the determinants of fraud reporting and the reasons for not reporting. Finally, discussion and conclusions are provided with particular emphasis placed on the potential policy implications.

6.2 Crime reporting

6.2.1 Crime reporting in general

Crime reporting has been the subject of much criminological literature with most research focussing on the demographic factors associated with reporting or the effects of economic, psychological and context factors (Torrente et al., 2017).

With regard to victim characteristics for traditional crime reporting, age has generated greatest consensus. Numerous studies have identified older people to be more likely to report crime (Baumer & Lauritsen, 2010; Boateng, 2016; Goudriaan et al., 2006; Van Wyk & Mason, 2001). Females also appear more propense to informing the police of crime victimisation (Baumer & Lauritsen, 2010; Goudriaan et al., 2006; Gutierrez & Kirk, 2017). The relationship between education level and crime reporting to the police remains unclear (Baumer & Lauritsen, 2010), though regarding fraud in particular, higher education has been associated with greater reporting rates (Schoepfer & Piquero, 2009; Copes et al., 2001). And, while some studies have found native-born victims to report more (Goudriaan et al., 2006) or lower reporting in neighbourhoods with higher immigration (Gutierrez & Kirk, 2017), others have not found any clear conclusions regarding ethnicity (Baumer & Lauritsen, 2010) or have shown reporting to depend on the immigrant destination (Xie & Baumer, 2019). Employment status has also been associated with crime reporting in the sense that the unemployed (Boateng, 2016) or those who work less hours (Goudriaan et al., 2006) report more. Finally, the victim's relationship with the offender has produced mixed results. Tolsma, Blaauw and Te Grotenhuis (2012) and Baumer and Lauritsen (2010) found less reporting when the offender is known to the victim; however, Tarling and Morris' findings (2010) showed the effects to be unclear.

In economics terms, various authors have highlighted that crime reporting can involve a rational decision-making process, in other words, the victim weighs the perceived costs of reporting against the expected benefits when deciding whether to report (Bowles et al., 2009; Felson et al., 2002; Goudriaan et al., 2006; Skogan, 1976; Skogan, 1984; Tolsma et al., 2012; Torrente et al., 2017). The main costs the victim may consider when making their decision are opportunity costs (Bowles et al., 2009). These include the time and financial costs of collecting evidence, contacting the police or dedicated to the judicial process. In this sense, Tolsma et al. (2012) showed that offering the possibility of reporting via Internet or telephone in addition to physically in the police station can increase reporting since Internet or telephone can significantly reduce the opportunity costs. With regard to benefits, these can be intrinsic or extrinsic (Bowles et al., 2009). Intrinsic benefits may refer to the altruistic desire to protect others by identifying the perpetrator, or they can be related to the victim’s desire for retribution. Extrinsic benefits include recovering losses through an insurance claim or by the police apprehending the offender and reclaiming stolen property. For instance, being insured has been associated with higher reporting rates (Bowles et al., 2009; Tarling & Morris, 2010). Victims also consider whether reporting is likely to be successful in attaining their goals (Felson et al., 2002).

The impact of victimisation is relevant as a number of studies have shown that the financial or physical severity of the crime is positively related to reporting levels (Baumer, 2002; Baumer & Lauritsen, 2010; Bowles et al., 2009; Copes et al., 2001; Isenring et al., 2015; Tarling & Morris, 2010). In fact, some authors have found the severity of the crime to be the strongest predictor of whether a victim reports (Goudriaan et al., 2006; Gutierrez & Kirk, 2017; Robert et al., 2010). In the case of fraud, it should not be forgotten that the consequences for the victim are not only financial but also emotional, psychological or even physical (Button et al., 2014; Cross et al., 2016; Schoepfer & Piquero, 2009; Spalek, 1999), all of which may influence the reporting decision. Advances in behavioural economics have emphasized the limits of human rationality and the significant role of emotions and biases in decision-making (Kahneman, 2011). Shame or embarrassment for having been victimised represents one of the principal psychological factors associated with crime reporting (Bowles et al., 2009; Felson et al., 2002). In this case, the expected negative reporting experience acts as a barrier.

As for context factors, in general, the victim’s opinion with regard to the police has been found to significantly predict reporting. Confidence in the police has been associated with greater reporting rates (Boateng, 2016; Tyler & Fagan, 2008) or, in other words, negativity towards public security institutions decreases reporting (Robert et al., 2010;

Tolsma et al., 2012). Similarly, there may also be a stigma with regard to contacting the police in certain social settings (Bowles et al., 2009). However, Goudriaan et al. (2006) found no relationship between police confidence and reporting, though they do suggest that analysis for specific crime types may be a useful avenue of future research. Kääriäinen and Sirén (2010) conclude that trust in police alone was not associated with increased willingness to report crime, but they did find that this variable interacted with general trust in others to influence the reporting decision. Guzy and Hirtenlehner (2015) also show trust in police has no effect or a negative effect on police reporting. They warn this could be related to the methodology used in victimisation surveys, whereby respondents are asked about their opinion regarding the police after having reported. Lower trust in the police could in fact be related to the reporting experience for the crime in question rather than the reason for not reporting. As well as opinions towards the police, local area characteristics such as the crime rate may play a role in the reporting decision (Bowles et al., 2009).

6.2.2 Cybercrime reporting

It has been stated that cybercrime reporting may be lower than for traditional crime (Yar and Steinmetz, 2019), but specific research on cybercrime reporting is lacking. Van de Weijer et al. (2018) have conducted the most extensive study to date, in which they compare the demographic determinants of cybercrime and traditional crime reporting. They posit that cybercrime reporting could be influenced positively by the greater distance between perpetrator and victim and thus less fear of retaliation. Yet, they find cybercrime is reported to police less than traditional crimes (except vandalism) and that most differences in crime reporting between groups are not very large.

The authors find less reporting of traditional crime to be associated with the following victim characteristics: repeat victimisation, male, younger, higher education, lower income, immigrants, divorced and single. The study identifies several institutional or context characteristics that decrease reporting, namely living in urban areas that have less cohesion and more nuisance. They find those who feel safer in neighbourhood report more and a positive attitude towards police is related to higher reporting.

There are many differences in the cybercrime findings as males, non-westerners, the unemployed and lower incomes are shown to report more. The three victim characteristics that are determined to be significantly related to lower cybercrime reporting are more frequent victimisation, higher education level and, conversely to traditional crime, having a higher income. The results show male victims of online consumer fraud are more likely to report while there is significantly less likelihood of reporting when older, single, student or bisexual (van de Weijer et al., 2018).

6.2.3 Fraud underreporting

The focus of this paper is fraud reporting and, in this regard, underreporting has been highlighted as one of the biggest challenges for combatting the issue. Prior research has found that only 15% (Titus et al., 1995), 20% (Copes et al., 2010) or 43% (Schoepfer & Piquero, 2009) of Americans report fraud victimisation. In their most recent figures, the Office of National Statistics found that only 15% of victims in England and Wales reported to Action Fraud or the Police between April 2018 and 2019[39]. The previously-mentioned van de Weijer et al. study (2018) based on a large representative sample of the Dutch population showed that online identity theft victims report 26.3% of the time while online consumer fraud victims report 24%. This is lower than all traditional crimes included in their research except vandalism. Kemp, Miro-Linares and Moneva (2020)

[39] Retrieved from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2019#fraud-reporting-to-action-fraud

also found fraud to be reported considerably less than other property crimes in different European countries. It has been stated that fraud reporting differs between fraud types (Copes et al., 2001), yet to the authors' knowledge there is no prior research on the online/offline divergences.

A number of reasons have been identified as to why fraud and online fraud reporting may be low (Button et al., 2014; Caneppele & Aebi, 2017; Copes et al., 2001; Cross et al., 2016; Schoepfer & Piquero, 2009). Firstly, the victim may be unaware of their victimisation. For instance, in the case of bank card frauds, the fraudulent transaction may pass unnoticed or in an investment fraud the victim may be unaware the investment is not what they expected. Secondly, if the financial loss is insignificant, the victim may calculate the expected utility from reporting and decide against it. As has been highlighted previously, to a certain degree reporting may involve a rational decision therefore if the expected benefit of recovered losses is low, the perceived time costs related to reporting may be greater. Third, the victim may not know where to report or may not consider it necessary to report to police. Fraud can often be reported to a multitude of agencies, which can confuse victims and discourage reporting. The most recent data from the Office of National Statistics shows that in England and Wales the two most common reasons for not reporting were already having reported the fraud to the bank (40%) and assuming the incident would be reported by another authority (23%). Fourth, as noted in section 2.1, lack of confidence in the police may reduce reporting. Given the anonymity and transnationality of fraud in the digital era, victims may consider the police incapable of responding adequately even if they do report. Victims could also feel the police will not take their victimisation seriously or even blame them. This is related to the embarrassment or shame factor that can inhibit reporting. Research shows there is a significant victim blaming culture with regard to fraud (Button & Cross, 2017b). Finally, with cyber fraud, like cybercrimes in general, it may be that the victim is unwilling to share their Internet activity with the police and, therefore, prefers not to report.

6.3 The present research

The present study aims to extend the ‘old wine in new bottles’ debate to crime reporting by comparing reporting for the offline and online variants of one crime type. Empirical academic literature has highlighted the importance of certain socio-demographic, psychological, economic and contexts factors for crime reporting and qualitative studies suggest this may be the case for cybercrime and cyber fraud; however, little quantitative research has been conducted on fraud reporting in the Internet era and it is not known whether variation exists between online and offline fraud. Similarly, there is a gap in the literature with regard to the differences in motives between online and offline non-reporting.

Thus, this paper seeks to answer the following questions: Firstly, what are the socio-demographic, context and fraud event determinants of fraud reporting and how do these differ between online and offline fraud? And, secondly, what socio-demographic, context and fraud event factors are associated with specific reasons for not reporting fraud and are these similar for online and offline fraud?

6.3.1 Sample

The sample comes from the two most recent editions (2015 and 2017) of the Catalan Public Security Survey carried out biennially in Catalonia. Catalonia is an autonomous region of 7.6 million inhabitants in the north of Spain, thus accounting for 16% of the national population. The 2015 survey was carried out in November and December with 6,214 people via telephone and the 2017 edition involved 7,876 citizens in November and

December, 5,918 via telephone and 1,958 self-administered surveys via the Internet. Both editions used a random sample with weighted responses in order to be representative of the population for that region[40].

The survey enquired about victimisation and reporting for a number of crimes, as well as perceived local-level safety and opinions regarding public police forces. The present paper focuses on those individuals who reported having been the victim of a fraud or scam in the previous 12 months. In the 2015 edition, 530 individuals, or 8.5%, stated that they had been victims of a fraud or a scam, while in the 2017 survey, 659 respondents, 8.4%, had experienced a fraud or a scam. After removing 12 records containing multiple missing values, the resulting total final sample consisted of 1,177 fraud or scam victims.

6.3.2 Variables

The survey includes questions for the following demographic characteristics: gender, age, place of birth, education, professional situation, economic situation, disability. In addition, participants are asked for their opinion regarding safety in their local area and regarding the Catalan police force and the local police force. Respondents are also asked about factors regarding the fraud event: if the victim considers the act a crime, whether it was perpetrated on the Internet, via telephone or in person, the financial loss, annoyance and psychological impact caused by the victimisation, and whether they reported the fraud

[40] The survey ensures representativity for age, sex and police region. Methodology can be consulted (in Catalan or Spanish) at: https://interior.gencat.cat/web/.content/home/010_el_departament/publicacions/seguretat/estudis_i_enquestes/enquesta_de_seguretat_publica_de_catalunya/enquesta_de_seguretat_publica_de_catalunya_2017/PRESENTACIO-LLARGA-ESPC2017.pdf

to the police. If the victim stated that they had not reported the crime, they were asked to select the reasons for this.

Table 7. **Descriptive statistics of fraud victims.**

Variable	**Percentages (n=1177)**	**Mean**	**SD**
Gender		1.49	1.02
1. Male	50.7		
2. Female	49.3		
Age		44.42	15.02
Place of birth			
1. Catalonia/Spain	87.5		
2. Another country	12.5		
Education		3.91	1.12
1. No school or primary school	15.9		
2. Obligatory secondary school (until 16)	14.8		
3. Post-obligatory secondary school and further education	29.6		
4. Higher education	39.7		
Professional situation			
1. Student	6.6		
2. Unemployed/ Housekeeper	12.8		
3. Retired	14.1		
4. Full time	54.2		
5. Part time	10.5		
6. Other/No response	1.7		
Financial situation		2.81	1.14
1. Very Good	4.2		
2. Good	53.3		
3. Neither bad nor good	9.4		
4. Bad	23.3		
5. Very bad	9.8		
Disability			
1. Yes	8.9		
2. No	90.1		
Opinion regarding safety in local area (0-10)		6.64	2.09
Opinion regarding Catalan police (0-10)		7.19	2.17
Opinion regarding local police (0-10)		6.56	2.16

Table 7 shows the descriptive statistics for demographic and crime event characteristics. These are displayed in percentages, except for the responses regarding the respondents' opinion on safety in their local area, the Catalan police, and the local police. These use a scale of 0-10, with 0 being the most negative response and 10 the most positive. Table 8 provides a description of the fraud event and the consequences suffered by respondents. The largest quantity of fraud was committed on the Internet, with over 35.5%. Telephone and In-person fraud were experienced by approximately a quarter of respondents respectively. The category of other is 11%, for which further information is unfortunately not available. For example, it is possible that some may have taken place through traditional mail. More than two thirds consider the fraud or scam they suffered constitutes a criminal offence. Regarding consequences, the mean level of annoyance caused is 7.58 from a rating scale of 0-10, whereas psychological impact was lower at 5.53. The mean financial loss was €1,411 with a standard deviation of €12,363 and the median was €100. The maximum quantity lost was €300,000 and the minimum was €0.

Table 8. **Descriptive statistics of fraud event and consequences.**

Variable	**Percentages**	**Mean**	**SD**	**Median**
Modus operandi				
1. *Internet*	35.5			
2. *Telephone*	26.3			
3. *In person*	24.5			
4. *Other*	11.6			
5. *Don't know*	2.1			
Fraud = crime				
1. *Yes*	68.3			
2. *No*	31.7			
Annoyance		7.58	2.41	8
Psychological impact		5.53	3.29	6
Financial impact (n=1125)		€1410.92	€12363.75	€100

Table 9 shows the breakdown of reporting rates. Fraud in general is only reported in 15.2% of cases. However, this rises to 21% for the frauds that the victim considered to be a crime. For Internet fraud the reporting rate is 26.1%, for those who considered it a crime 32%. This is considerably higher than reporting for telephone fraud (3.2% and 5.3%) and in-person fraud (12.6% and 16.9%). This difference appears partially explained by the fact the victim is more likely to consider Internet fraud a crime (78.5%) than the other two (61.3% and 59.7%).

Table 9. **Fraud reporting rates**

Fraud	**Reporting rate (%)**
Total for sample (n=1177)	15.2
Respondents who consider their fraud a crime (n=804)	21
Telephone fraud (n=310)	3.2
Telephone fraud considered a crime (n=190; % total telephone fraud = 61.3%)	5.3
In-person fraud (n=288)	12.6
In-person fraud considered a crime (n=172; % total in-person = 59.7%)	16.9
Internet fraud (n=418)	26.1
Internet fraud considered a crime (n=328; % total Internet fraud = 78.5%)	32

Table 10 presents the number of times each reason was selected by respondents who did not report their crime. Multiple responses were possible.

Table 10. **Non-reporting reasons**

Reasons for not reporting	**Percentage**
Reason A. It was very complicated, laziness, too much bureaucracy, process too long	61.9
Reason F. It was insignificant	54.1
Reason C. There is little the police can do	53.3
Reason E. Lack of confidence in the justice system	38.6
Reason D. Lack of confidence in the police	19.6
Reason B. Fear of reprisal or making things worse	7.1

6.3.3 Analysis strategy

Question 1: what are the socio-demographic, psychological, context and fraud event determinants of fraud reporting and how do these differ between online and offline fraud?

The first binary logistic regression model seeks to determine the factors associated with fraud reporting. To this end, the dependent variable (DV) is a binary variable that has been dichotomised as: if the respondent did not report the fraud = 0, if they did = 1. The independent variables (IV) are all the socio-demographic, psychological, context and fraud event variables enumerated in Table 1.

As not all participants considered their fraud a crime, it was considered useful to analyse the factors that predict reporting when controlling for the consideration of the event as a crime. With this objective, a second model, identical to the first with regard to DV and IV, was conducted on those respondents who considered their fraud a crime.

Next, two logistic regressions were carried out for the fraud modus operandi (MO). In this sense, using the same DV and IV as in the previous models, logistic regressions were conducted on two subsamples created for those respondents who stated they had been the victim of fraud that occurred via the Internet and fraud that was perpetrated offline. It was considered necessary to only conduct one model for offline fraud, which combines telephone fraud with in-person fraud, and not these two MO's individually because the number of participants who reported their telephone or in-person fraud was very small.

Finally, a fifth model was conducted to identify the factors that are associated with a fraud being considered a crime, in other words, what might make a fraud victim consider the event a crime. In this case, the DV is dichotomised as fraud considered a crime = 0, fraud not considered a crime = 1. The IV are all the socio-demographic, psychological, context and other fraud event variables enumerated in Table 1

Question 2: what socio-demographic, psychological, context and fraud event factors are associated with specific reasons for not reporting fraud and are these similar for both online and offline fraud?

To analyse the determinants of the reasons for not reporting a binary logistic regression was conducted for each reason. In each model the DV is whether the respondent selected that reason for not reporting: 0 = no, 1 = yes. The IV are all the socio-demographic, police and safety and fraud event factors, including the MO.

Given the academic interest in understanding reporting motives, analysis was also carried out on the relationships between the different reasons given. To this end, a further binary logistic regression model was performed for each of the six reasons. The DV is whether the respondent had selected that reason for not reporting: 0 = no, 1 = yes and the IV are the other reasons.

6.4 Results

Figure 1 plots the odds ratios for those variables that were statistically associated with reporting (or approached significance) in model 1 for fraud reporting in the whole sample as well as model 2 for just those respondents who considered the fraud a crime. It should be noted that in all figures, the reference category of the variable is indicated when categorical independent variables are non-binary, in other words when the variable has more than two categories. In the case of continuous variables, the odds ratio indicates the effect of a one unit increase in the IV. The reference value is 1 in all variables. It should also be highlighted that figures include the margin of error for the odds ratios. This displays the range within which the odds ratio falls to a confidence interval of 95%; therefore, when interpreting the statistically significant results, it should be borne in mind that the odds ratio may be slightly lower or higher than that indicated by the point in the figures and detailed in the Annexes.

The results for model 1 show that the odds of reporting are significantly lower for frauds that occurred in person or on the telephone in comparison to those perpetrated on the Internet. Furthermore, in line with the descriptive analysis provided in Table 8, if the victim considered the act a crime, the likelihood of reporting is higher than if they did not. The only other variable that reached statistical significance was financial impact, which was also associated with increased reporting, though the effect was minimal. Annoyance approached significance, but psychological impact appears to offer no predictive value for reporting in the whole sample of fraud victims. None of the demographic or opinion variables were significantly correlated with fraud reporting.

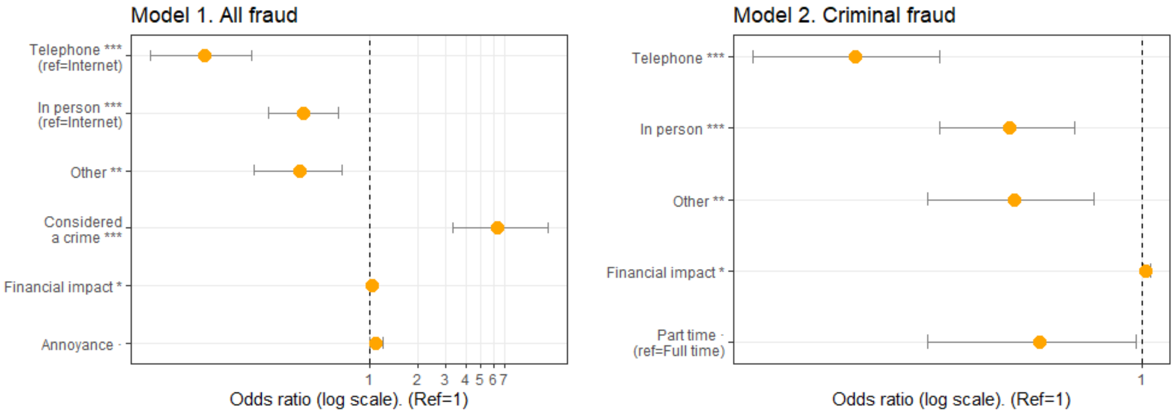

Figure 14. Fraud reporting determinants.

The consideration of the fraud as criminal could be considered a logical predictor of reporting behaviour. In order to identify relevant determinants while controlling for this consideration, a similar model was performed for frauds considered a crime. Model 2, which only includes respondents who considered the fraud a crime, shows similar results since MO is the variable with the greatest effect followed by financial impact. In this sense, in comparison to the reference category of fraud perpetrated on the Internet, fraud considered a crime is reported at a significantly lower rate when it occurred in person or on the telephone. The model finds financial impact to be associated with greater reporting levels, although the effect is negligible; however, annoyance and psychological impact show no significant correlation with reporting to the police. The respondents' opinion regarding the police and safety in their local area do not appear to be statistically significant explanatory variables and neither do the demographic characteristics of respondents. The complete table with all odds ratios can be found in Annex I.

Given that the strongest predictor in these models was the fraud modus operandi, analysis of the individual MO's could provide further information on the determinants of reporting. Figure 15 shows the results of the logistic regression models for the online and offline fraud subsamples with the same DV (except MO as these are MO subsets) and IV as in the previous models. Online fraud reporting may be influenced by considering the fraud a crime, the financial impact, annoyance, and age. All of these variables are related to higher reporting, though the effects of financial impact and annoyance are relatively small, and the effect of age is very small. As regard offline fraud, the relevant variables are all related to the incident and its impact: considering it a crime, financial impact and psychological impact.

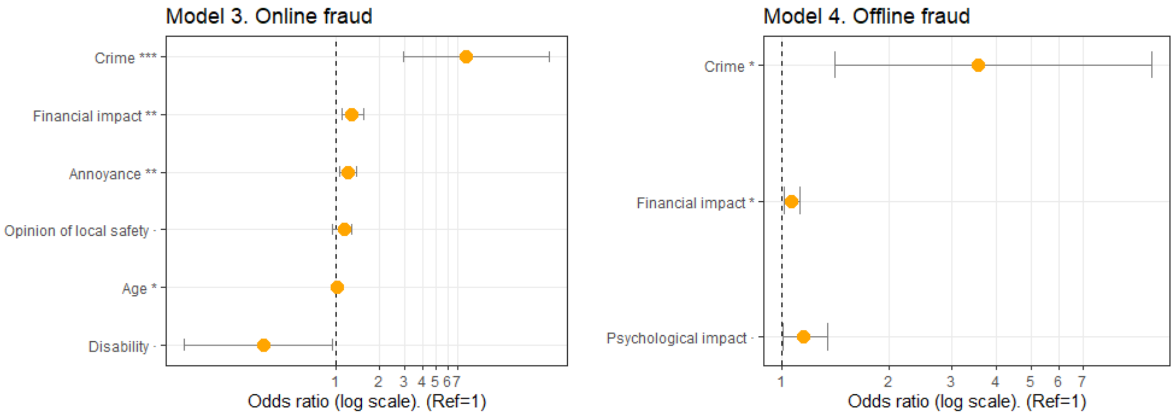

Figure 15. Online and offline fraud reporting determinants.

Unsurprisingly, the prior findings show that considering the fraud a crime is a significant predictor of reporting to the police. Yet, it also relevant to know why fraud victims consider their event a crime. Figure 16 shows the results of the fifth model and as can be observed, the variable with the greatest effect over whether a fraud is considered a crime is whether it was perpetrated on the Internet, in person or on the telephone. In this sense, frauds occurring via telephone or in person are less likely to be considered a crime than those on the Internet. Annoyance and psychological impact also showed a strong positive statistical association, although with a more reduced effect size. It is notable that there is a statistically significant correlation between the DV and annoyance and psychological impact but not financial impact.

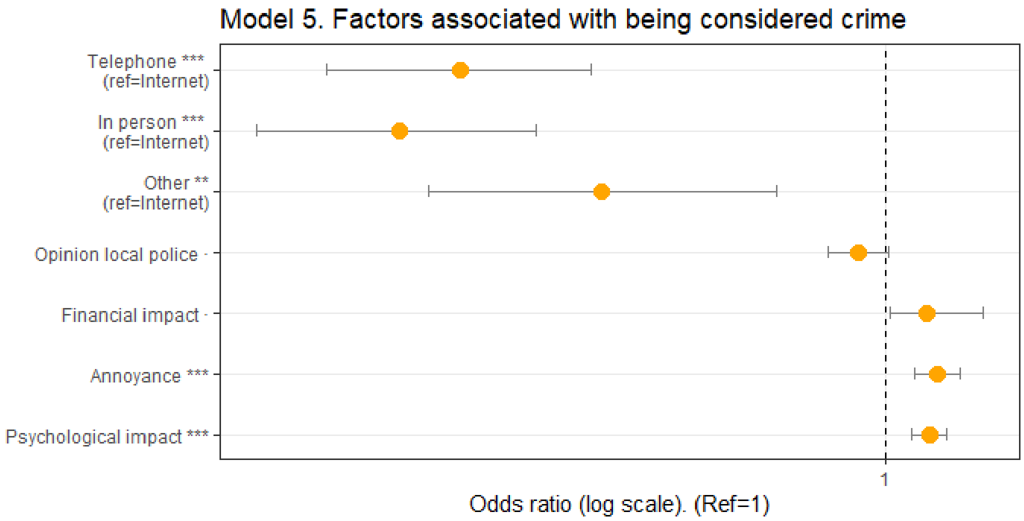

Figure 16. Factors associated with consideration of fraud as criminal.

Having identified some of the variables associated with fraud reporting, the final phase of the analysis centred on the reasons for not reporting. Figure 17 presents the results of the 6 logistic regression models, in which only the statistically significant variables are presented to facilitate the reader's task. All odds ratios are available in annex II.

In accordance with model 6 in figure 17, three variables are related to the fraud victim considering the reporting process excessively complex. On the one hand, it is more common among those who have suffered a telephone fraud than an Internet fraud and among those who are foreign born. On the other hand, females are less likely to view the reporting process in this manner. Regarding model 7, psychological impact and being retired significantly increase the odds that a fraud victim will explain their decision not to report by fear of worsening the situation. A more positive opinion of the local police is correlated with a decrease in this fear explanation. Model 8 shows fraud victims who did not report because they believed there was little the police can do were more likely to have suffered a fraud via telephone than Internet and greater annoyance, though the latter only has a small effect. Individuals less likely to explain not reporting by this reason have a more positive opinion of the Catalan and local police, are older, or are students.

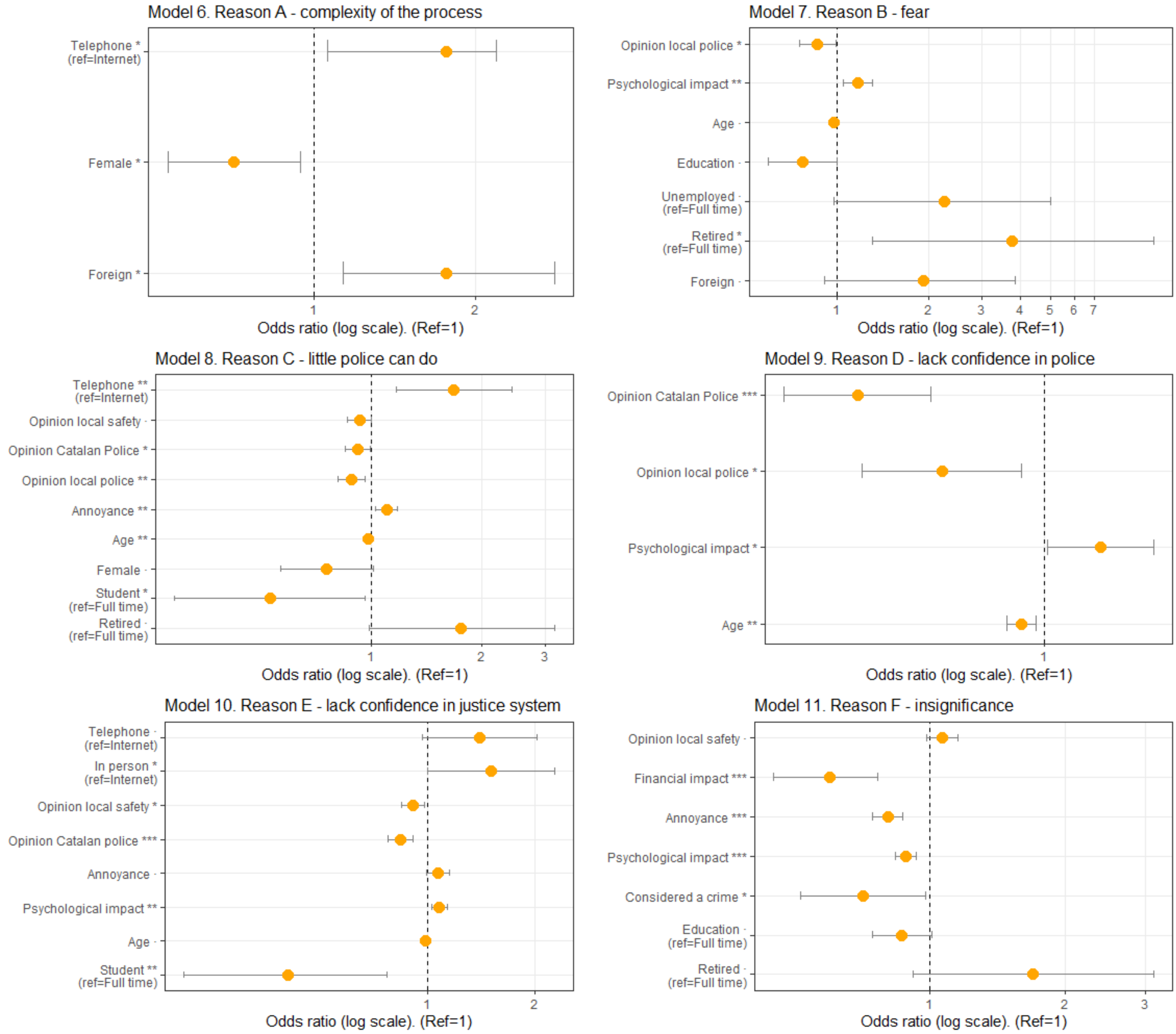

Figure 17. Determinants of reasons for not reporting.

In figure 17 model 9, we can see that those who have a good opinion of the Catalan and local police and those who are older are less likely to express a lack of confidence in the police to explain their non-reporting of a fraud. On the other hand, those persons who reported higher psychological impact are more likely to not report for this reason. As shown in model 10, psychological impact and in-person frauds tend to push victims to renounce reporting because of a ‘lack of confidence in the justice system’. On the other hand, having a more positive opinion of local-area safety or the Catalan police, or being a student reduce the odds of explaining non-reporting by this reason. Finally, model 11 shows, unsurprisingly, that victims stating the insignificance of the fraud event as a reason for not reporting suffer less financial impact, annoyance, psychological impact or are less likely to consider the fraud a crime.

Table 11 shows the associations between the different reasons for non-reporting. Firstly, it is notable how the perceived complexity of the process interacts with the insignificance of the impact and the belief that police can do little to help in the decision not to report a fraud. In addition, those who consider the process too complex also lack confidence in the justice system. Secondly, the three reasons related to the police or justice system are correlated, thereby showing that people who believe the police can do little also lack confidence in the police and the justice system as a whole. Interestingly, fear of reprisals or making the situation worse is positively correlated with the belief that the police can do little.

Table 11. **Relationship between different reasons.**

	Reason A Complexity	Reason B Fear	Reason C Police can do little	Reason D Lack of confidence police	Reason E Lack of confidence CJS	Reason F Insignificance
Reason A Complexity	—	1.083	2.055***	1.212	1.972***	2.001***
Reason B Fear	1.058	—	2.597**	1.433	1.218	0.633·
Reason C Police can do little	2.057***	2.566**	—	2.951***	3.905***	0.952

Reason D Lack of confidence police	1.168	1.430	2.917***	———	13.332***	1.026
Reason E Lack of confidence CJS	1.977***	1.164	3.899***	13.544***	———	0.706*
Reason F Insignificance	1.993***	0.635·	0.947	1.063	0.712*	———
R^2	0.08	0.05	0.17	0.29	0.27	0.02

Signif. codes: 0‘***’ 0.001‘**’ 0.01‘*’ 0.05‘·’ 0.1‘ ’

6.5 Discussion

Considering the importance of crime reporting for the design and evaluation of crime prevention and reaction strategies, the present study has produced a number of interesting findings with implications for policy and practice.

Firstly, the simplest of these is that online fraud reporting was found to be higher than its traditional counterparts. Given academic research has found cybercrime reporting to be particularly low, this finding is surprising. Higher online fraud reporting is not correlated with greater financial impact in absolute terms as there is no statistically significant difference in losses between the fraud modi operandi. Rather, online fraud appears more likely to be considered a crime in general. This ties in with Pepinsky's view (1980) of crime reporting as a reflection of the definitions citizens give to potentially deviant acts. One possible explanation for higher online fraud reporting is that it may be easier to provide evidence of online victimisation since electronic transactions and conversations are more easily registered. Alternatively, it could be that online fraud victims consider they have been defrauded, while more telephone or in-person fraud victims believe they have let themselves be defrauded, in other words, they are more likely to blame themselves for their victimisation and therefore refrain from reporting. Unfortunately, the survey used for the present research does not enquire about the level of responsibility fraud victims attribute themselves. This would be an interesting line of future research. In any case, it appears necessary to increase reporting for fraud that occurs via telephone or in person, thus, awareness-raising campaigns should ensure they do not only focus on online fraud.

Secondly, the literature review highlighted the rationality of reporting and the results of the present study indicate that the costs and benefits of reporting influence the decision-making process of many fraud victims. This conclusion can be reached because, on the one hand, financial or psychological impact are significant variables (although with small effect sizes) in almost all the models detailed in this study and, on the other hand, because, the inconvenience and length of the process is the most common explanation for not reporting. In addition, this reason is often given along with the insignificance of losses and the belief that police can do little to help, both of which tie in with economic decision-making. These findings suggest that strategies to increase reporting should focus on reducing opportunity costs and increasing the perceived benefits of the reporting process. It has also been found that increased annoyance is related to the aforementioned reasons for not reporting. It could follow that victims' frustration with the perceived complexity of the reporting process, their belief that the police can do little and their subsequent decision to not report increases their annoyance with the fraud victimisation overall. In this sense, Catalonia or Spain do not have a centralised reporting system such as Action Fraud in the UK, the Canadian Anti-Fraud Centre or the Australian Cybercrime Online Reporting Network. It could be the moment to evaluate the benefits of adapting these practices to the Spanish context and organising the fight against fraud and victim support in a centralised manner. Furthermore, it has been highlighted that centralised reporting centres are essential for crime analysis and criminological research that can foster data-driven policy (Strom & Smith, 2017).

Third, in some cases annoyance or psychological impact appear to influence the decision to report a fraud. Thus, victim support services should be aware of possible suffering and avoid victim blaming and stigmatisation which can generate secondary victimisation. They should aim to reduce the harm suffered by victims and publicize that this is a benefit of reporting. There is a salient need to consider the non-monetary consequences of fraud (Button & Cross, 2017b). On the other hand, the results also indicate that lack of confidence in the police or justice system is correlated with greater annoyance and psychological harm, which suggests that a perceived lack of institutional support makes victimisation worse. In short, strategies seeking to stimulate fraud reporting should improve the support available to victims and emphasize the benefits of reporting.

Finally, there appears to be no clear general demographic profile of the fraud reporter, though certain factors are associated with certain reasons for not reporting. In this sense, older people are less likely to believe the police cannot do anything or to lack confidence in the police while females are less likely to consider the process excessively arduous. Consequently, if, for example, reporting is to be stimulated among younger generations, one recommendable strategy would involve improving confidence in the police among this demographic. As shown by the results, the image of the Catalan police is more relevant than the municipal police force in this regard. There also appears to be a significant group of people who choose not to report due to a combined lack of confidence in the police and the criminal justice system as well as a belief in the inability of the police to help. An interesting avenue of future research may shed light on the characteristics of this group, thereby allowing targeted interventions to improve confidence.

6.6 Conclusion and limitations

The present paper has responded to calls for fraud reporting research posed in previous studies (Copes et al., 2001; Schoepfer & Piquero, 2009; van de Weijer et al., 2018) by analysing and comparing the determinants of fraud reporting and the reasons for non-reporting, including the crime event characteristics. Online and offline reporting were compared, thus, the paper contributes to the 'old wine in new bottles' cybercrime debate and, more specifically, by examining the applicability of the scientific literature on crime reporting to fraud and online fraud, it strengthens the evidence base for policies that aim to stimulate reporting for an especially prevalent crime in the digital age.

However, in achieving these goals the study also faces limitations. Firstly, it would be interesting to perform the study with larger datasets for each fraud modus operandi or for different fraud types. This may reveal further determinants and permit conclusions for more specific fraud MO's. Secondly, the assignation of the category for the fraud MO depends on the opinion of the victim and, moreover, cannot be clearly captured in the survey. Many frauds are online/offline hybrids (Caneppele & Aebi, 2017) but this is not an option in the categories available in the survey and it is likely survey participants assign the MO category according to different criteria. For instance, some frauds may initially begin via telephone but involve the Internet to a large degree. Some respondents may adjudge this to be online fraud and others consider it telephone. Alternatively, it may be that the rather large 'other' category (11.6%) includes many hybrid frauds. This information is unfortunately not available in the present data, though future qualitative studies could look to fill the gap. Thirdly, the temporal order of crime reporting and victimisation surveys means respondents are being asked about annoyance or psychological impact after having reported the crime. In this sense, for example, respondents who have had a negative reporting experience may manifest greater psychological impact which could be influenced by the reporting process and not solely the crime. Finally, the present study does not examine the perceived benefits of fraud reporting and the reasons that victims give for doing so. This constitutes an interesting avenue of future research that is supported by the literature on the rationality of crime reporting.

-blank page-

CHAPTER VII GENERAL RESULTS, DISCUSSION AND CONCLUDING REMARKS

This thesis set out to examine and elucidate the issue of fraud against individuals in the Internet era. To achieve this general objective, a number of facets of fraud against individuals have been analysed via descriptive statistics and statistical modelling, specifically: trends, victimisation correlates, impact and reporting. By establishing key debates, themes and gaps in the existing literature on fraud, CHAPTER I laid the foundations for the empirical research that was conducted in the articles that form this compendium of publications. Based on the areas identified in the literature, CHAPTER II synthesized the general objectives, research questions and hypotheses that guided the present thesis. Subsequently, CHAPTER III presented an overview of the data sources and methods used to respond to the questions previously posed and test the hypotheses derived from these. CHAPTERS IV, V and VI put all of this into practice in the form of three articles that have been published in academic criminology journals of the highest impact, both nationally and internationally. The current chapter will now compile the general results and provide a general discussion of the findings.

The key discussions in relation to fraud against individuals start from the very bottom: what is it exactly? As with all crime, it is often extremely complex to delineate behaviour into dichotomous categories of criminal or not criminal; crime is a social construct after all (Hillyard & Tombs, 2007). Nevertheless, researching criminal or harmful phenomena requires a working definition in order to determine what does or does not constitute the object of analysis. This thesis employed a diversity of sources to this end, ultimately stating that “fraud is an act of wilful deception that produces an economic benefit (or evasion of a loss) for the deceiver and a loss for the victim” (CHAPTERS I and IV), and establishing individuals as the main subject for the analysis conducted herein. As advocated by Felson and Eckert (2020), the thesis also differentiated fraud in accordance with the modus operandi for contact between victim and offender: Internet, telephone, or in-person. The analysis, which approached the subject from both a macro and micro perspective, pivoted on the themes of trends, victimisation and reporting and was guided by four general research questions. We will now examine how the thesis has responded to each of these in turn.

7.1 RQ$_1$ How has fraud against individuals evolved during the Internet era?

With regard to RQ$_1$, it has been shown that fraud against individuals is rising. In CHAPTER IV, official police statistics and bank statistics combined with victimisation surveys from Spain and abroad indicated that fraud is prevalent in comparison to other property crimes and is rising in the Internet era. It was hypothesized (GH$_1$) that this may be the result of increases in fraud that involve digital environments, and the data provided in CHAPTER IV suggest that this is indeed the case: It appears motived offenders are capitalizing on the fraud opportunities afforded by digital technologies. The triangulation of different data sources showed that while there is no marked decrease in traditional fraud, there is a pronounced increase in fraud that is conducted via the Internet. This has profound implications for crime control in the twenty-first century. Above all, if fraud is one of, if not, the most prevalent property crimes in digital society, are sufficient resources being allocated to prevention, policing and harm reduction, and who is responsible for providing these resources? CHAPTER IV highlighted a notable discrepancy between official fraud data and victimisation survey fraud rates, which suggests the possibility of poorly designed institutional responses since these are often informed by official data. However, rising, widespread fraud appears to be a negative externality of the technological boom that is characterised by multinational tech giants that hold greater economic power than most nation-states and that are certainly better equipped than local police forces to disrupt transnational crime. Thus, it may be time to shift responsibility onto those who unintentionally generate the criminogenic situations (Tilley, 2018), especially since CHAPTER IV indicates that law enforcement agencies have serious difficulties to even obtain a clear picture of the criminal landscape in the Internet era. This will be no easy task unless there is a definite economic incentive to prevent crime; profit-making enterprises respond to incentives that increase their profits. Nevertheless, if dating sites can be a hotspot for romance fraud (Whitty, 2015), they should be forced to raise awareness and maximise protection for their clients. If online shopping is a predictor of consumer fraud (CHAPTER I), more needs to be invested by the sites and the financial institutions that facilitate the transactions. If large troves of stolen data can be bought at a very modest price (Holt & Lampke, 2010) and used in fraud for a considerable profit (Holt et al., 2016), all the actors involved in the data infrastructure must better protect the data they hold. Best practices exist in these areas, but the analysis provided in CHAPTER IV suggests not enough is being done and that improved collaboration and cooperation is required between the myriad of actors who participate in fraud prevention, policing and victim support.

7.2 RQ_2 What factors influence fraud victimisation in the Internet era?

Having identified the growth and widespread prevalence of fraud in the Internet era, the subsequent phase of analysis sought to zoom in on the micro level factors associated with these macro trends. The review of the literature on correlates of fraud victimisation identified a lack of consensus regarding the demographic profile of fraud victims, but that certain online activities may be associated with greater risk of victimisation. In this sense, RQ_2 enquired about the factors associated with fraud victimisation in the Internet era, to which CHAPTER V sought to respond. The hypothesis was that the correlates of online and offline fraud would be distinct, therefore, Internet, telephone and in-person fraud were compared. The findings showed that there were some differences, with younger people and individuals with a higher education level more likely to be affected by online fraud. These results tie in with some of the more concordant associations found from a routine activities approach to online fraud victimisation since younger people are more likely to carry out the activities associated with victimisation, such as online shopping or simply general Internet use.

The difficulty to identify a general fraud victim profile relates to the 'name fallacy' described in CHAPTER I of this thesis. Fraud, like cybercrime, encompasses many different conducts so there is no blanket profile for those who are more likely to suffer from it. Rather, profiles and correlates begin to emerge when we disaggregate fraud into smaller categories. Felson & Eckert (2020) argue for studies that focus on crime modus operandi in order to improve prevention and, therefore, CHAPTERS V and VI broke fraud down into the principal method used by the perpetrator to contact the victim: Internet, telephone or in-person. Identifying certain factors associated with fraud victimisation by different MO allows for potentially more effective targeted prevention interventions. For example, the statistical analysis indicates that telephone and in-person fraud more frequently affect older people, which could justify awareness-raising campaigns for this particular demographic. It should also be remembered that the results of this thesis show that the Internet is the most common method used by offenders to contact victims, but telephone and face-to-face techniques are still frequent and, therefore, should continue to form part of prevention and reaction interventions.

7.3 RQ_3 How does fraud in the Internet era impact victims?

Establishing factors associated with victimisation advances knowledge on what may be driving the previously unveiled fraud trends, and this leads us to the two-pronged issue of the consequences of victimisation. Firstly, there are more fraud victims now than a decade ago, which likely means the total harm generated is also greater. To reduce the damage caused we first need to understand how the process of victimisation is experienced. Secondly, fraud impacts are inextricably tied to reporting. Better understanding the impact of fraud at an individual level can help comprehend why the macro level trends of underreporting are so pronounced. In this regard, CHAPTER V aimed to respond to RQ_3 on the consequences of fraud in the Internet era. International literature highlights that the impact of fraud on individuals can extend far beyond merely financial losses to emotional, psychological and even physical harm. As found in the data from the Catalan Public Security Survey, many people report relatively high levels of annoyance and psychological impact. However, it was also shown in the literature that crime affects different people in different ways and, therefore, GH_3 stated that certain sociodemographic characteristics and crime event factors are correlated with increased impact of fraud victimisation. After conducting the analysis of the survey data, this hypothesis was accepted since a number of correlates were found for impact. The financial consequences were greater for all professional categories in comparison to students as well as for persons with disability in comparison to those without. For their part, annoyance and psychological impact were higher for telephone fraud in comparison to online fraud, for women, older people and those who had suffered greater financial losses. These non-financial impacts were lower for people in a more positive financial situation and with a more positive opinion of safety in their local area. In addition, higher education level was correlated with lower psychological impact. The findings suggest that certain sectors of the population suffer greater harm than others and targeted support interventions could help ameliorate the consequences of fraud.

Fraud appears to be the volume crime of the Internet era and researching its impacts is central to designing effective responses. It has been shown that the consequences of fraud against individuals are often misunderstood, that victims are often blamed for failing foul to fraudulent schemes (Cross, 2015) and that this weakens victim support services (Cross, 2018b). Inadequate victim assistance is problematic for two main reasons. On the one hand, it means that the harm caused by fraud may be aggravated and can even lead to secondary victimisation. A lack of support can worsen the financial, emotional and psychological fallout from fraud experiences. If the institutions that are meant to provide support engage in victim blaming, the harm from fraud can become more acute. On the other hand, the impact of fraud is closely related to reporting. If we better understand the victimisation experience, we can improve victim support services, which may encourage greater reporting. As we have seen throughout the thesis, fraud reporting is one of the greatest challenges to anti-fraud strategies. Facilitating fraud reporting and designing effective reporting channels requires an evidence base on how fraud is experienced. CHAPTER V takes a step in that direction.

7.4 RQ$_4$ What factors are associated with fraud reporting in the Internet era?

After examining the factors associated with victimisation and impact, Research Question 4 focussed specifically on fraud reporting, which was the subject of CHAPTER VI. The review of the existing literature on crime reporting established that there may be demographic, economic, psychological and context factors that are related to the decision to report. The existence of fraud underreporting was underscored along with some of the possible explanations and motives. Furthermore, it was also determined that there may be notable differences in reporting patterns for cybercrime versus traditional crime. Thus, GH$_4$ was formulated as "Certain sociodemographic characteristics and crime event factors are correlated with the decision to report fraud". After performing the statistical models found in CHAPTER VI, the null hypothesis is rejected because the findings showed that various factors may indeed determine the reporting decision. Firstly, though demographic characteristics of reporting were uncommon, age was associated with a small positive effect on Internet fraud reporting. Secondly, the financial impact of fraud appears to positively influence the decision to report. This was also highlighted in the analysis of the motives for reporting and is related to the economic decision making that may drive some fraud reporting. Greater psychological consequences and annoyance in certain circumstances also appear associated with increased reporting. Relatedly, the subjective consideration of the fraud as a crime was also highly significant. CHAPTER V showed that this is related to the psychological impact and annoyance, but surprisingly the relationship between the financial consequences and considering the fraud a crime was unclear in our sample. Finally, context factors such as the opinion regarding the police, the criminal justice system or safety in the local area may determine the decision to contact law enforcement about a fraud experience. To the author's best knowledge, the analysis conducted in CHAPTER VI is the first quantitative study on the predictors and motives of fraud reporting using a sample of fraud victims, not only in Spain but also internationally, therefore, these findings make an important contribution to the beginnings of an evidence base with which to design interventions that aim to improve and increase fraud reporting.

The response to RQ_4 unites the circular loop of macro and micro level analysis presented in this doctoral project. The general aim of elucidating an underresearched criminal issue began with an examination of the potential disparity between official police fraud statistics and bank data and victimisation surveys, seeking to get closer to a more reliable approximation of the prevalence of fraud. It was established that the prevalence in Spain is likely far higher than law enforcement statistics indicate, thereby justifying the individual level research into the factors associated with greater risk of victimisation, the elements that help configure the financial and non-financial impact of fraud, and the determinants and motives of reporting and non-reporting. The importance of fraud reporting has been emphasized on both an individual and societal level. Individual in that reporting is necessary to recover losses or access victim support services and, thus, reduce the individual harms of fraud. At a societal level, in the sense that crime reporting is necessary for the design and implementation of public policy. Without a clear picture of the threats faced by citizens, it is much more complex to define strategies to minimize risks and reduce the consequences of crime. This is particularly salient in fraud, because many individual victimisations are for relatively small amounts, but these form part of the criminal strategies of organised groups who collectively amass very large amounts in illicit earnings. Without reporting, it is very complicated to identify the patterns in offending that can lead to successful criminal justice interventions. In short, understanding what drives fraud reporting is paramount to effective responses.

7.5 Contribution to wider debates

While the focus of this thesis was one specific crime category, this does not impede the results from also adding to broader discussions in international criminology. At the start of this thesis it was proposed that researching fraud in the Internet era could contribute to wider criminological debates, so let us now evaluate how this has been achieved. Firstly, CHAPTER I identified research requesting that crime trends be placed on the criminological centre stage (Baumer et al., 2018) as well as an overview of the extensive crime drop literature, which highlighted the consensus around the existence of a drop and the lack of consensus regarding the causal mechanisms. However, it has been stated that it is necessary to explain crime drop patterns in relation to different crime types (Baumer et al., 2018; Matthews & Minton, 2017). Given it is one of the most prevalent offences, research on a potential property crime drop should include fraud in the analysis and, therefore, CHAPTER IV makes a significant contribution to this discussion. We have seen that fraud is not falling, in fact, quite the opposite: it appears to be rising and fast. This adds a very salient nuance to previous research and supports authors who have emphasized differing trends between crime types. In addition, it adds further fuel to the debate regarding possible explanatory mechanisms for the documented drop in some offences and the rise in others. Regarding fraud, the growth appears to be driven by increases in fraud that involves digital technologies and environments. It may be that the criminogenic opportunities in the Internet era are changing and with them the criminal landscape (Miró-Llinares & Moneva, 2019). Understanding the role of lifestyles, routine activities and crime opportunities is essential to both short-term and long-term crime prevention interventions, and so as to comprehend their role, it is first necessary to have a sufficiently clear picture of crime trends. CHAPTER IV helps illuminate these trends with regard to fraud and emphasizes the need for both academia and criminal justice institutions to look beyond police statistics when analysing crime patterns.

Secondly, the introduction to the thesis presented the decades-old yet ever-expanding debate on traditional and cybercrime a/symmetries. Is fraud “old wine in new bottles” or is it something completely new? Unfortunately, the answer is not that simple. We have seen that online fraud is increasing while traditional offline fraud remains stable or is declining slightly (CHAPTER IV). We have seen that there are some small but relevant differences in the factors associated with victimisation and that the strategy used to contact the victim and perpetrate fraud (Internet, telephone, or in-person) is related to divergent levels of impact (CHAPTER V). And, the sample analysed in the present thesis showed differences with regards to the MO and reporting practices (CHAPTER VI). Based on the findings of these three chapters, it appears that certain aspects of fraud differ when the digital component is present or not (or present in an essential manner for the commission of the offense or not). Yet, despite these distinctions it is still not clear if it is the fraud that has changed or the bottle that holds it or both. Maybe it does not matter. Social events in cyberspace are not the same as interactions in the physical world (Miró-Llinares, 2012), so they require criminological interventions to be modified. Theories and findings based on research on traditional crimes may be applicable and helpful, but they will likely need to be adapted to some degree. However, this is also true for traditional crimes of a differing nature. Cybercrime is not one thing, fraud is not one thing, and, for example, traditional theft is not one thing. It seems, as Clarke (2010) suggests, we need to be more crime specific for crime interventions and a binary division between traditional and cyber does not automatically contribute something new or help advance from either a theoretical or an applied criminology perspective. Given that drawing a line between our online and offline life is growing ever more complicated (Floridi, 2015), maybe criminologists should also employ other forms of categorisation (McGuire, 2019), such as that presented in CHAPTER IV.

Finally, based on its victim-centred approach, the thesis set out to add to the criminological literature on crime reporting and succeeded in doing so from both a macro and micro perspective. The dark figure of fraud in Spain is now not quite so opaque, and this is vital to understand crime in the Internet era. Fraud is the high-volume property crime of the twenty-first century, and the profound changes to work and leisure that have taken place in 2020 are likely to exasperate this further. To understand why fraud reporting is low and, therefore, why it is underrepresented in official crime data, it was necessary to examine the different factors and motives that can influence reporting on an individual level. These can be compared to other property crimes and strategies can be put in place to increase reporting. In this sense, the initial diagnostic is clear: fraud reporting must be facilitated, and citizens must view reporting as something that provides a realistic benefit, both to themselves and to others. The archipelago of institutions that can provide support to fraud victims has been termed the "Fraud Justice Network" (Button et al., 2013) and many countries have sought to connect the institutional islands through a centralised reporting system. For instance, the UK has Action Fraud, Canada the Canadian Anti-Fraud Centre and Australia implemented the Australian Cybercrime Online Reporting Network. Spain and Catalonia could look to these models for inspiration and adapt them to their context. Centralised reporting systems are by no means the panacea, with the expectations of reporters often not matching reality (Cross, 2018b), but the dark figure of fraud identified in this thesis suggest that a change of strategy is required. Regarding unmet expectations from fraud reporters, centralised reporting centres need to be sympathetically honest with users about short term expectations, but they should also be prepared to emphasize the potential societal crime control benefits of reporting criminal activity. This is one of the first academic projects on fraud in Catalonia and Spain and it makes no pretensions to provide all the answers. At the same time, it has made a strong positive contribution to fraud research both here and abroad as well as a number of other areas of criminological inquiry.

7.6 Limitations

In responding to the aforementioned questions and contributing to wider debates, this thesis also faced limitations that are addressed individually in each of the articles, but which are briefly summarized in this section. In general terms, and an obstacle that faces almost all criminological endeavours, the data used herein make robust unequivocal conclusions challenging and, as such, the thesis has sought to avoid causal claims, instead mainly referring to predictors, correlates, associations and indications. The data are related to an issue that is illicit and possibly embarrassing by nature, often retrieved from institutions whose main objective is not to collect data, or via surveys from individuals whose subjectivity will always be present. This has to be acknowledged. But then, robust unequivocal conclusions were never the objective. This social science doctoral thesis aimed to examine, to analyse, to elucidate, to put forward conclusions that even though they may be tentative indications, advance knowledge in manner that can have practical applications. In fact, one of the main aims was to show that something was wrong with the original police data and provide some possible explanations why. In this sense, it is undeniable that the data employed has limitations, but not limitations that impede the attainment of the research objectives. While the data are imperfect, they provide timely conclusions and a blueprint for future fraud studies to combine sources so as to answer questions of social relevance. Some potential lines of future research are discussed next.

7.7 Future research

This doctoral thesis advances fraud research in Spain one step forward; but, this is a journey that has no clear end and the hope is that the sources, methods and findings found here will encourage others to join. As a result of the progress made in this research work, a number of avenues for future research have emerged with regard to the object of study.

Firstly, research on more specific forms of fraud has been advocated from a crime science perspective. How do fraud trends for specific types compare? What factors are associated with victimisation? How do they affect victims? These are some of the questions that could also be asked of individual fraud types, and it seems unlikely that the responses in relation to, for example, romance fraud or consumer fraud or employment fraud will be the same. The crime script and factors correlated with each of these examples will likely differ, as will the consequences. The emotional or psychological toll of discovering you are being defrauded by someone you believed to be a romantic partner is unlikely to be the same as purchasing consumer goods from a non-existent online store. Analysis focussed on specific fraud types can assist in the design of effective responses and prevention strategies. Similarly, in addition to fraud types, it may also be useful to approach fraud research in terms of the place where it occurs. Environmental criminologists have shown that crime can be concentrated in small geographical areas and propose the use of targeted crime reduction interventions (Braga et al., 2016; Sherman et al., 1989). There have already been some promising applications of this perspective to fraud (Moneva & Caneppele, 2020) that could help guide theory and practice.

Furthermore, frauds should also be examined in accordance with the victim. This thesis only deals with individual victims, but organisations also suffer fraud, and this can also have many negative effects on people’s lives. It would be interesting to consider the dark figure of fraud against businesses and what influences victimisation, impact and reporting. There has been a lack of research on organisational fraud victims, not least because of the difficulty to obtain data. An organisation's reputation can often depend on its perceived ability to protect its clients and being a fraud victim is not positive in this regard. To overcome this obstacle and advance knowledge on fraud in the Internet era, new innovative forms of data collection are needed, as well as convincing strategies for building collaborations between academia, policymakers, law enforcement and the private sector.

One possible avenue to foster cooperation and collaboration is through evaluations of what works in fraud prevention and reaction. This type of research may provide the economic benefits necessary to awaken the interests of public and private organisations that hold data on fraud: Assisting organizations to prevent fraud losses can have a positive effect on the bottom line (Tunley, 2014). Many systematic reviews have evaluated crime reduction interventions. For example: Welsh and Farrington (2004) analysed the effectiveness of CCTV in preventing crime; Braga et al. (2019) assessed the effects of hot spots policing; and, Simpson et al. (2014) evaluated the impact of corporate crime deterrence interventions. Situational crime prevention (Cornish & Clarke, 2003) has been put forward as a potential framework for economic crime prevention in the Internet era (Leukfeldt & Jansen, 2019; Miró-Llinares, 2012). Qualitative studies have also begun to evaluate the effects of fraud reporting centres from the perspective of the victim (Cross, 2018b) and the fraud justice network professionals (Cross, 2020a). Yet, what works to prevent fraud and what is the best reaction? These questions so far remain unanswered.

Finally, in the pages that comprise the thesis we have not, until now, discussed the potential root causes of fraud. Opportunities have been noted as the driving force behind fraud, and while some consider that "opportunity makes the thief" (Clarke, 2012; M. Felson & Clarke, 1998), theories of criminality may provide further explanation for the rising levels of fraud we are currently witnessing. For instance, global inequalities and capitalist ideals may create anomic situations (Tade & Aliyu, 2011) or provide neutralisation techniques for offenders in economically poorer African nations to target people in Europe and North America (Warner, 2011; Whitty, 2018). Or, the organised groups that commit fraud likely provide the environmental conditions for the elements of social learning theory (Akers, 1977) to materialise. And maybe these fraud organisations can be understood as delinquent subcultures (Cloward & Ohlin, 1960). This missing viewpoint of fraud in the Internet era is undoubtedly an interesting avenue for future research.

7.8 Concluding remarks

This doctoral thesis has analysed fraud against individuals in the Internet era with regard to trends and the factors associated with victimisation, impact and reporting. It has been shown that fraud against individuals is growing in digital society and that there is a clear inconsistency between, on the one hand, the official criminal justice statistics and, on the other hand, data from financial institutions and the results of victimisation surveys. The latter two sources show levels of fraud many times greater than their criminal justice counterparts, thereby emphasizing the need to form policy decisions on the basis of a variety of sources and not only the data available from law enforcement institutions. While we have seen that data on fraud is limited in general, there are enough sources to obtain a superior picture of this high-volume property crime in Spain and, therefore, enough sources to aspire to improved policy decisions or to encourage the actors that generate fraud-related criminogenic externalities to participate in combatting the issue. Fraud opportunities seem likely to continue to grow, meaning it is time to better design the response.

Understanding the factors associated with fraud victimisation can help improve prevention strategies. We have seen that fraudsters often employ different methods to contact potential victims in accordance with the profile of the target, but that there may well be a fraud for everyone. Fraud offenders take advantage of the opportunities available in particular circumstances, which emphasizes the need for prevention and reaction strategies to be focussed and fraud specific in order to be effective. Fraud is a broad category and focussing on smaller fraud types based on the modus operandi or other categorisations related to the nature or environment of the fraud can identify patterns of fraudulent activity and profiles of people at higher risk.

Furthermore, examining the impact of fraud is essential for the design of effective responses and can provide valuable insight on what might be driving the dark figure of fraud. This thesis has indicated that victims of fraud can suffer considerable financial losses as well as psychological consequences. It is not a victimless crime as popular myths may lead to believe and many factors can be associated with the impacts of fraud. We have seen that fraud affects different people in different ways and that the dynamics of the non-financial consequences are far more complex than just being a function of financial losses. Greater comprehension of how fraud affects people allows the consequences to be understood from a victim-centred perspective and urges new reporting and victim support systems.

Finally, in accordance with the statistical analysis conducted in this thesis, the impacts of fraud influence reporting, but so do the expected costs and benefits of reporting. If it is perceived that law enforcement will be unable to recover losses, that the perpetrators will not be identified or that the reporting process will be complex or embarrassing, reporting is less likely. It appears many people do not believe the police can provide a worthwhile response to their crime report, which means the dark figure of fraud grows, which, in turn, means insufficient resources are allocated to the issue and the cycle perpetuates. Studying the determinants and motives that influence fraud reporting aids the design of reporting channels that meet victims' expectations and the needs of the relevant criminal justice institutions. Only through better understanding can we break the cycle and better prepare for one of the most relevant criminal threats in the twenty-first century.

-blank page-

REFERENCES

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2017). Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys*, *50*(3), 44:1–44:41. https://doi.org/10.1145/3054926

Aebi, M. F., & Linde, A. (2010). Is There a Crime Drop in Western Europe? *European Journal on Criminal Policy and Research*, *16*(4), 251–277. https://doi.org/10.1007/s10610-010-9130-y

Aebi, M. F., & Linde, A. (2014). The persistence of lifestyles: Rates and correlates of homicide in Western Europe from 1960 to 2010: *European Journal of Criminology*, *11*(5), 552–577. https://doi.org/10.1177/1477370814541178

Aebi, M. F., & Linde, A. (2010). El Misterioso Caso de la Desaparición de las Estadísticas Policiales Españolas. *Revista Electrónica de Ciencia Penal y Criminología*, *12–07*, 30.

Agustina, J. R. (2015). Understanding Cyber Victimization: Digital Architectures And The Disinhibition Effect. *International Journal of Cyber Criminology*, *9*(1). https://doi.org/10.5281/ZENODO.22239

Akanle, O., & Richard Shadare, B. (2020). Why has it been so difficult to Counteract Cyber Crime in Nigeria? Evidence from an Ethnographic Study. *International Journal of Cyber Criminology*, *14*(1). https://doi.org/10.5281/zenodo.3738962

Akers, R. L. (1977). *Deviant Behavior: A Social Learning Approach*. Wadsworth Publishing Company.

Alshalan, A. (2008). *Cyber-Crime Fear and Victimization: An Analysis of A National Survey*. VDM Verlag Dr. Müller.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the Cost of Cybercrime. In R. Böhme (Ed.), *The Economics of Information Security and Privacy* (pp. 265–300). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-39498-0_12

Angrist, J. D., & Pischke, J.-S. (2009). *Mostly Harmless Econometrics*. Princeton University Press. https://press.princeton.edu/books/paperback/9780691120355/mostly-harmless-econometrics

Bachman, R. D., & Paternoster, R. (2020). *Statistics for Criminology and Criminal Justice* (4th ed.). Sage. https://uk.sagepub.com/en-gb/eur/statistics-for-criminology-and-criminal-justice/book248806

Baumer, E. P. (2002). Neighborhood Disadvantage and Police Notification by Victims of Violence. *Criminology, 40*(3), 579–616. https://doi.org/10.1111/j.1745-9125.2002.tb00967.x

Baumer, E. P., & Lauritsen, J. L. (2010). Reporting Crime to the Police, 1973–2005: A Multivariate Analysis of Long-Term Trends in the National Crime Survey (ncs) and National Crime Victimization Survey (ncvs). *Criminology, 48*(1), 131–185. https://doi.org/10.1111/j.1745-9125.2010.00182.x

Baumer, E. P., Vélez, M. B., & Rosenfeld, R. (2018). Bringing Crime Trends Back into Criminology: A Critical Assessment of the Literature and a Blueprint for Future

Inquiry. *Annual Review of Criminology*, *1*(1), 39–61. https://doi.org/10.1146/annurev-criminol-032317-092339

Beals, M., DeLiema, M., & Deevy, M. (2015). *Framework for a Taxonomy of Fraud*. Stanford Center on Longevity. http://longevity.stanford.edu/2015/07/30/framework-for-a-taxonomy-of-fraud/

Blumstein, A., & Wallman, J. (Eds.). (2005). *The Crime Drop in America* (2nd ed.). Cambridge University Press. https://doi.org/10.1017/CBO9780511616167

Boateng, F. D. (2016). Crime Reporting Behavior: Do Attitudes Toward the Police Matter?: *Journal of Interpersonal Violence*. https://doi.org/10.1177/0886260516632356

Bolimos, I. A., & Choo, K.-K. R. (2017). Online fraud offending within an Australian jurisdiction. *Journal of Financial Crime*, *24*(2), 277–308. https://doi.org/10.1108/JFC-05-2016-0029

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, *38*(3), 227–236. https://doi.org/10.1016/j.jcrimjus.2010.03.001

Bossler, A. M., Holt, T. J., Cross, C., & Burruss, G. W. (2020). Policing fraud in England and Wales: Examining constables' and sergeants' online fraud preparedness. *Security Journal*, *33*(2), 311–328. https://doi.org/10.1057/s41284-019-00187-5

Bowles, R., Garcia Reyes, M., & Garoupa, N. (2009). Crime Reporting Decisions and the Costs of Crime. *European Journal on Criminal Policy and Research*, *15*(4), 365–377. https://doi.org/10.1007/s10610-009-9109-8

Braga, A. A., Cave, B., Lawton, B., Gill, C., Telep, C. W., Lum, C., Weisburd, D., Groff, E. R., Rengert, G., Bruinsma, G., Ratcliffe, J. H., Eck, J. E., Hinkle, J. C., Hibdon, J., Bowers, K., Johnson, S. D., Yang, S.-M., & Taniguchi, T. (Eds.). (2016). Crime Places within Criminological Thought. In *Place Matters: Criminology for the Twenty-First Century* (pp. 1–15). Cambridge University Press. https://doi.org/10.1017/CBO9781139342087.002

Braga, A. A., Turchan, B., Papachristos, A. V., & Hureau, D. M. (2019). Hot spots policing of small geographic areas effects on crime. *Campbell Systematic Reviews*, *15*(3), e1046. https://doi.org/10.1002/cl2.1046

Brenner, L., Meyll, T., Stolper, O., & Walter, A. (2020). Consumer fraud victimization and financial well-being. *Journal of Economic Psychology*, *76*, 102243. https://doi.org/10.1016/j.joep.2019.102243

Briggs, P., Jeske, D., & Coventry, L. (2017). Chapter 6—Behavior Change Interventions for Cybersecurity. In L. Little, E. Sillence, & A. Joinson (Eds.), *Behavior Change Research and Theory* (pp. 115–136). Academic Press. https://doi.org/10.1016/B978-0-12-802690-8.00004-9

Britt, C. L., & Weisburd, D. (2010). Logistic Regression Models for Categorical Outcome Variables. In A. R. Piquero & D. Weisburd (Eds.), *Handbook of Quantitative Criminology* (pp. 649–682). Springer New York. https://doi.org/10.1007/978-0-387-77650-7_31

Brottsförebyggande. (2018). *Swedish Crime Survey 2017* (p. 24). Brottsförebyggande.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2020). Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. *European Societies*, Online First 2020. https://doi.org/10.1080/14616696.2020.1804973

Button, M., & Cross, C. (2017a). Chapter 4: Technology and fraud: the ‘fraudogenic’ consequences of the Internet revolution. In Michael McGuire & T. J. Holt

(Eds.), *The Routledge handbook of technology, crime and justice*. Routledge, Taylor & Francis Group. https://ebookcentral.proquest.com/lib/surrey/detail.action?docID=4813465

Button, M., & Cross, C. (2017b). *Cyber Frauds, Scams and their Victims*. Routledge. https://researchportal.port.ac.uk/portal/en/publications/cyber-frauds-scams-and-their-victims(b34ba86f-210a-49af-a7e4-fbadc33abc37)/export.html

Button, M., Gee, J., & Mothershaw, N. (2018). *Annual Fraud Indicator 2017: Identifying the cost of fraud to the UK economy*. Crowe; University of Portsmouth; Experian.

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, *27*(1), 36–54. https://doi.org/10.1057/sj.2012.11

Button, M., Tapley, J., & Lewis, C. (2013). The ‘fraud justice network’ and the infra-structure of support for individual fraud victims in England and Wales. *Criminology & Criminal Justice*, *13*(1), 37–61. https://doi.org/10.1177/1748895812448085

Caneppele, S., & Aebi, M. F. (2017). Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes. *Policing: A Journal of Policy and Practice*, *13*(1), 66–79. https://doi.org/10.1093/police/pax055

Centraal Bureau voor de Statistiek. (2018). *Veiligheidsmonitor 2017*. Centraal Bureau voor de Statistiek.

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior, 70*, 291–302. https://doi.org/10.1016/j.chb.2017.01.003

Christie, N. (1986). The Ideal Victim. In E. A. Fattah (Ed.), *From Crime Policy to Victim Policy: Reorienting the Justice System* (pp. 17–30). Palgrave Macmillan UK. https://doi.org/10.1007/978-1-349-08305-3_2

Clarke, R. V. (2010). Crime Science. In *The SAGE Handbook of Criminological Theory* (pp. 271–283). SAGE Publications Ltd. https://doi.org/10.4135/9781446200926

Clarke, R. V. (2012). Opportunity makes the thief. Really? And so what? *Crime Science*, *1*(1), 3. https://doi.org/10.1186/2193-7680-1-3

Clough, J. (2015). *Principles of Cybercrime* (2nd ed.). Cambridge University Press. https://doi.org/10.1017/CBO9781139540803

Cloward, R. A., & Ohlin, L. E. (1960). *Delinquency and Opportunity: A theory of delinquent gangs* (p. 220). Free Press.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588–608. JSTOR. https://doi.org/10.2307/2094589

Copes, H., Kerley, K. R., Huff, R., & Kane, J. (2010). Differentiating identity theft: An exploratory study of victims using a national victimization survey. *Journal of Criminal Justice*, *38*(5), 1045–1052. https://doi.org/10.1016/j.jcrimjus.2010.07.007

Copes, H., Kerley, K. R., Mason, K. A., & Wyk, J. V. (2001). Reporting behavior of fraud victims and black’s theory of law: An empirical assessment. *Justice Quarterly*, *18*(2), 343–363. https://doi.org/10.1080/07418820100094931

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, Precipitators and Criminal Decisions: A Reply to Wortley’s Critique of Situational Crime Prevention. In M.

J. Smith & D. B. Cornish (Eds.), *Theory for Practice in Situational Crime Prevention, Crime Prevention Studies* (Vol. 16, pp. 111–124). Monsey.

Correia, S. G. (2019). Responding to victimisation in a digital world: A case study of fraud and computer misuse reported in Wales. *Crime Science, 8*(1), 4. https://doi.org/10.1186/s40163-019-0099-7

Croall, H. (2016, May 1). *What Is Known and What Should Be Known About White-Collar Crime Victimization?* The Oxford Handbook of White-Collar Crime. https://doi.org/10.1093/oxfordhb/9780199925513.013.4

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology, 21*(2), 187–204. https://doi.org/10.1177/0269758015571471

Cross, C. (2018a). (Mis)Understanding the Impact of Online Fraud: Implications for Victim Assistance Schemes. *Victims & Offenders, 13*(6), 757–776. https://doi.org/10.1080/15564886.2018.1474154

Cross, C. (2018b). Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice, 55*, 1–12. https://doi.org/10.1016/j.ijlcj.2018.08.001

Cross, C. (2019a). Is online fraud just fraud? Examining the efficacy of the digital divide. *Journal of Criminological Research, Policy and Practice, 5*(2), 120–131. https://doi.org/10.1108/JCRPP-01-2019-0008

Cross, C. (2019b). Online Fraud. In *Oxford Research Encyclopedia of Criminology and Criminal Justice*. https://doi.org/10.1093/acrefore/9780190264079.013.488

Cross, C. (2020a). Responding to individual fraud: Perspectives of the fraud justice network. In R. Leukfeldt & T. J. Holt (Eds.), *The Human Factor of Cybercrime* (pp. 359–388). Routledge.

https://www.taylorfrancis.com/books/9780429864186/chapters/10.4324/9780429460593-16

Cross, C. (2020b). ‘Oh we can’t actually do anything about that’: The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice*, *20*(3), 358–375. https://doi.org/10.1177/1748895819835910

Cross, C., & Blackshaw, D. (2015). Improving the Police Response to Online Fraud. *Policing*, *9*(2), 119–128. https://doi.org/10.1093/police/pau044

Cross, C., Dragiewicz, M., & Richards, K. (2018). Understanding Romance Fraud: Insights From Domestic Violence Research. *The British Journal of Criminology*, *58*(6), 1303–1322. https://doi.org/10.1093/bjc/azy005

Cross, C., Richards, K., & Smith, R. G. (2016). *Improving the Response to Online Fraud Victims: An Examination of Reporting and Support*. Criminology Research Advisory Council. http://crg.aic.gov.au/reports/1617/29-1314-FinalReport.pdf

Danielsson, P., & Näsi Matti. (2018). *Kansallisen Rikosuhritutkimuksen Tuloksia 2017*. Institute of Criminology and Legal Policy, University of Helsinki. https://helda.helsinki.fi/bitstream/handle/10138/260559/Katsauksia_31_Danielsson_N%C3%A4si_2018.pdf

Davies, P., & Francis, Peter. (2018). Doing Criminological Research. In Davies, Pamela & P. Francis (Eds.), *Doing Criminological Research* (3rd ed.). SAGE Publications Ltd. https://uk.sagepub.com/en-gb/eur/doing-criminological-research/book243822

Deevy, M., Lucich, S., & Beals, M. (2012). *Scams, schemes and swindles: A review of consumer financial fraud research*. Financial Fraud Research Center.

http://longevity.stanford.edu/wp-content/uploads/2017/01/Scams-Schemes-Swindles-FINAL-On-Website.pdf

Dijk, J. V., Tseloni, A., & Farrell, G. (2012). *The International Crime Drop—New Directions in Research*. Palgrave Macmillan UK. https://www.palgrave.com/gp/book/9780230302655

Donohue, J. J., & Levitt, S. D. (2001). The Impact of Legalized Abortion on Crime. *The Quarterly Journal of Economics*, *116*(2), 379–420. https://doi.org/10.1162/00335530151144050

Duggan, M. (2001). More Guns, More Crime. *Journal of Political Economy*, *109*(5), 1086–1114. https://doi.org/10.1086/322833

Dupont, B. (2017). Bots, cops, and corporations: On the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, Law and Social Change*, *67*(1), 97–116. https://doi.org/10.1007/s10611-016-9649-z

ECB. (2018). *Fifth report on card fraud, September 2018*. European Central Bank. https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport201809.en.html

Europol. (2018). *Internet Organised Crime Threat Assessment* (IOCTA) 2017. Europol. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017

Europol. (2020). *Internet Organised Crime Threat Assessment (IOCTA) 2019*. Europol. https://www.europol.europa.eu/iocta-report

Fafinski, S., Dutton, W. H., & Margetts, H. Z. (2010). Mapping and Measuring Cybercrime. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1694107

Farrell, G., & Birks, D. (2018). Did cybercrime cause the crime drop? *Crime Science, 7*(1), 8. https://doi.org/10.1186/s40163-018-0082-8

Farrell, G., Tseloni, A., Mailley, J., & Tilley, N. (2011). The Crime Drop and the Security Hypothesis: *Journal of Research in Crime and Delinquency*. https://doi.org/10.1177/0022427810391539

Fattah, E. A. (1997). The Thorny Issue of Defining Crime. In E. A. Fattah (Ed.), *Criminology: Past, Present and Future: A Critical Overview* (pp. 29–43). Palgrave Macmillan UK. https://doi.org/10.1007/978-1-349-25838-3_2

Felson, M., & Clarke, R. V. G. (1998). *Opportunity makes the thief: Practical theory for crime prevention*. Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate.

Felson, M., & Eckert, M. A. (2020). *Crime and Everyday Life* (6th ed.). SAGE Publications, Ltd. https://us.sagepub.com/en-us/nam/crime-and-everyday-life/book255558

Felson, R. B., Messner, S. F., Hoskin, A. W., & Deane, G. (2002). Reasons for Reporting and Not Reporting Domestic Violence to the Police. *Criminology, 40*(3), 617–648. https://doi.org/10.1111/j.1745-9125.2002.tb00968.x

Fernández-Molina, E., & Gutiérrez, R. B. (2018). Juvenile crime drop: What is happening with youth in Spain and why?: *European Journal of Criminology*. https://doi.org/10.1177/1477370818792383

Fiscalía General del Estado. (2019). *Memoria Anual del Fiscalía General del Estado 2018*. Fiscalía General del Estado. https://www.fiscal.es/memorias/memoria2019/FISCALIA_SITE/index.html

Fischer, P., Lea, S. E. G., & Evans, K. M. (2013). Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. *Journal of Applied Social Psychology*, *43*(10), 2060–2072. https://doi.org/10.1111/jasp.12158

Floridi, L. (Ed.). (2015). *The Onlife Manifesto: Being Human in a Hyperconnected Era*. New York: Springer International Publishing. https://doi.org/10.1007/978-3-319-04093-6

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, *30*(2), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Fraud Act 2006, The | The Crown Prosecution Service. (n.d.). Retrieved 19 June 2020, from https://www.cps.gov.uk/legal-guidance/fraud-act-2006

Gadd, D., Karstedt, S., & Steven F. Messner. (2012). Editorial Introduction. In Gadd, David, Karstedt Susan, & Steven F. Messner (Eds.), *The SAGE Handbook of Criminological Research Methods* (pp. 1–8). SAGE Publications Ltd. https://uk.sagepub.com/en-gb/eur/the-sage-handbook-of-criminological-research-methods/book234136

Gale, J. A., & Coupe, T. (2005). The Behavioural, Emotional and Psychological Effects of Street Robbery on Victims. *International Review of Victimology*, *12*(1), 1–22. https://doi.org/10.1177/026975800501200101

Golladay, K., & Holtfreter, K. (2017). The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes. *Victims & Offenders*, *12*(5), 741–760. https://doi.org/10.1080/15564886.2016.1177766

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime* (pp. xvi, 297). Stanford University Press.

Goudriaan, H., Wittebrood, K., & Nieuwbeerta, P. (2006). Neighbourhood Characteristics and Reporting Crime: Effects of Social Cohesion, Confidence in Police Effectiveness and Socio-Economic Disadvantage1. *The British Journal of Criminology*, *46*(4), 719–742. JSTOR.

Grabosky, P. N. (2001). Virtual Criminality: Old Wine in New Bottles? Social and Legal Studies, *10*(2), 243–249. https://doi.org/10.1177/a017405

Graham, R., & Triplett, R. (2017). Capable Guardians in the Digital Environment: The Role of Digital Literacy in Reducing Phishing Victimization. *Deviant Behavior*, *38*(12), 1371–1382. https://doi.org/10.1080/01639625.2016.1254980

Green, B., Gies, S., Bobnis, A., Piquero, N. L., Piquero, A. R., & Velasquez, E. (2020). The Role of Victim Services for Individuals Who Have Experienced Serious Identity-Based Crime. *Victims & Offenders*, *0*(0), 1–24. https://doi.org/10.1080/15564886.2020.1743804

Grolemund, G., & Wickham, H. (2016). *R for Data Science*. O'Reilly Media, Inc. https://r4ds.had.co.nz/

Gruszczyńska, B., & Heiskanen, M. (2018). Trends in Police-Recorded Offenses at the Beginning of the Twenty-First Century in Europe. *European Journal on Criminal Policy and Research*, *24*(1), 37–53. https://doi.org/10.1007/s10610-018-9370-9

Gutierrez, C. M., & Kirk, D. S. (2017). Silence Speaks: The Relationship between Immigration and the Underreporting of Crime. *Crime & Delinquency*, *63*(8), 926–950. https://doi.org/10.1177/0011128715599993

Hadlington, L., Lumsden, K., Black, A., & Ferra, F. (2018). A Qualitative Exploration of Police Officers' Experiences, Challenges, and Perceptions of Cybercrime. *Policing: A Journal of Policy and Practice*, *090*. https://doi.org/10.1093/police/pay090

Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: The Initial Results from a Natural Experiment. *American Journal of Criminal Justice*. https://doi.org/10.1007/s12103-020-09534-4

Hillyard, P., & Tombs, S. (2007). From ‘crime’ to social harm? *Crime, Law and Social Change*, *48*(1), 9–25. https://doi.org/10.1007/s10611-007-9079-z

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization*. Pensacola: Ballinger Publishing Company.

Holt, T. J., & Bossler, A. M. (2008). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behavior*, *30*(1), 1–25. https://doi.org/10.1080/01639620701876577

Holt, T. J., & Bossler, A. M. (2015). *Cybercrime in Progress: Theory and prevention of technology-enabled offenses*. Routledge. https://doi.org/10.4324/9781315775944

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2017). *Cybercrime and Digital Forensics: An Introduction*. Taylor & Francis Group. http://ebookcentral.proquest.com/lib/bibliouocsp-ebooks/detail.action?docID=5107356

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies*, *23*(1), 33–50. https://doi.org/10.1080/14786011003634415

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). Exploring and Estimating the Revenues and Profits of Participants in Stolen Data Markets. *Deviant Behavior*, *37*(4), 353–367. https://doi.org/10.1080/01639625.2015.1026766

Holt, T. J., & Turner, M. G. (2012). Examining Risks and Protective Factors of On-Line Identity Theft. *Deviant Behavior*, *33*(4), 308–323. https://doi.org/10.1080/01639625.2011.584050

Holtfreter, K., Reisig, M. D., & Blomberg, T. G. (2005). Consumer Fraud Victimization in Florida: An Empirical Study. *St. Thomas Law Review*, *18*, 761.

Holtfreter, K., Reisig, M. D., Piquero, N. L., & Piquero, A. R. (2010). Low Self-Control and Fraud: Offending, Victimization, and Their Overlap. *Criminal Justice and Behavior*. https://doi.org/10.1177/0093854809354977

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low Self-Control, Routine Activities, and Fraud Victimization. *Criminology*, *46*(1), 189–220. https://doi.org/10.1111/j.1745-9125.2008.00101.x

Hutchings, A., & Hayes, H. (2009). Routine Activity Theory and Phishing Victimisation: Who Gets Caught in the 'Net'? *Current Issues in Criminal Justice*, *20*(3), 433–452. https://doi.org/10.1080/10345329.2009.12035821

Isenring, G. L., Mugellini, G., & Killias, M. (2015). The willingness to report employee offences to the police in the business sector: *European Journal of Criminology*. https://doi.org/10.1177/1477370815623569

Jansen, J, Junger, M, Kort, J, Leukfeldt, R, Veenstra, S, van Wilsem, J, & van der Zee, S. (2017). Victims. In Leukfeldt, R (Ed.), *Research agenda the human factor in cybercrime and cybersecurity*. Eleven International Publishing.

Jansen, J., & van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies*, *123*, 40–55. https://doi.org/10.1016/j.ijhcs.2018.10.004

Johnstone, P. (1998). Serious white-collar fraud: Historical and contemporary perspectives. *Crime, Law and Social Change*, *30*(2), 107–130. https://doi.org/10.1023/A:1008349831811

Junger, M., Montoya, L., Hartel, P., & Heydari, M. (2017). Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in europe. *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 1–8. https://doi.org/10.1109/CyberSA.2017.8073391

Jupp, V., Davies, P., & Francis, P. (2000). *Doing Criminological Research*. SAGE Publications, Ltd. https://doi.org/10.4135/9780857024404

Kääriäinen, J., & Sirén, R. (2010). Trust in the police, generalized trust and reporting crime: *European Journal of Criminology, 8*(1), 65–81. https://doi.org/10.1177/1477370810376562

Kahneman, D. (2011). *Thinking, Fast and Slow*. Farrar, Straus and Giroux. https://us.macmillan.com/thinkingfastandslow/danielkahneman/9780374533557

Kemp, S., Miró-Llinares, F., & Moneva, A. (2020). The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research*. https://doi.org/10.1007/s10610-020-09439-2

Kemp, S., & Moneva, A. (2020). Fraude online vs. offline: Factores predictores de victimización y su impacto. *InDret, 1.2020*. https://indret.com/fraude-online-vs-offline-factores-predictores-de-victimizacion-y-su-impacto/

Kemp, S. (2020). Fraud reporting in Catalonia in the Internet era: Determinants and motives. *European Journal of Criminology*, Online First 2020. https://doi.org/10.1177/1477370820941405

Kerstens, J., & Jansen, J. (2016). The Victim–Perpetrator Overlap in Financial Cybercrime: Evidence and Reflection on the Overlap of Youth’s On-Line Victimization and Perpetration. *Deviant Behavior*, *37*(5), 585–600. https://doi.org/10.1080/01639625.2015.1060796

Kranenbarg, M. W., Holt, T. J., & Gelder, J.-L. van. (2019). Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap. *Deviant Behavior*, *40*(1), 40–55. https://doi.org/10.1080/01639625.2017.1411030

Kruize, P. (2018). *Internetkriminalitet 2017*. The Faculty of Law, University of Copenhagen. https://dkr.dk/media/13026/internetkriminalitet-2017-final.pdf

Larrauri, E. (2019). *Introducción a la criminología y al sistema penal* (2nd ed.). Trotti. http://www.trotta.es/libros/introduccion-a-la-criminologia-y-al-sistema-penal/9788498797664

Lea, S. E. G., Fischer, P., & Evans, K. M. (2009). *The psychology of scams: Provoking and committing errors of judgement*. Office of Fair Trading. https://ore.exeter.ac.uk/repository/handle/10871/20958

Leukfeldt, E. R., & Roks, R. A. (2020). Cybercrimes on the Streets of the Netherlands? An Exploration of the Intersection of Cybercrimes and Street Crimes. *Deviant Behavior*, *0*(0), 1–12. https://doi.org/10.1080/01639625.2020.1755587

Leukfeldt, E. R. (2014). Phishing for Suitable Targets in The Netherlands: Routine Activity Theory and Phishing Victimization. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), 551–555. https://doi.org/10.1089/cyber.2014.0008

Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of

Financial Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research*, *23*(3), 287–300. https://doi.org/10.1007/s10610-016-9332-z

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Leukfeldt, E. R., Notté, R. J., & Malsch, M. (2020). Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes. *Victims & Offenders*, *15*(1), 60–77. https://doi.org/10.1080/15564886.2019.1672229

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Leukfeldt, E. R. (2017). *The Human Factor Examined: Directions for Future Research. In: Leukfeldt R (ed.) Research Agenda. The Human Factor in Cybercrime and cybersecurity.* https://www.elevenpub.com/criminology/catalogus/research-agenda-the-human-factor-in-cybercrime-and-cybersecurity-1

Leukfeldt, E. R., & Jansen, J. (2016). Cyber Criminal Networks And Money Mules: An Analysis Of Low-Tech And High-Tech Fraud Attacks In The Netherlands. *International Journal of Cyber Criminology*, *9*(2). https://doi.org/10.5281/ZENODO.56210

Leukfeldt, E. R., & Jansen, J. (2019). Financial cybercrimes and situational crime prevention. In Eric Rutger Leukfeldt & T. J. Holt (Eds.), *The Human Factor of Cybercrime* (1st ed., pp. 216–239). Routledge, Taylor & Francis Group. https://doi.org/10.4324/9780429460593-10

Leukfeldt, E. R., Veenstra, S., & Stol, W. (2013). High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands. *International Journal of Cyber Criminology, 7*(1), 17.

Levi, M. (2008). Organized fraud and organizing frauds: Unpacking research on networks and organization. *Criminology & Criminal Justice*, *8*(4), 389–419. https://doi.org/10.1177/1748895808096470

Levi, M. (2012). Assessing the Cost of Fraud. In D. Gadd, S. Karstedt, & S. Messner (Eds.), *The SAGE Handbook of Criminological Research Methods* (pp. 461–474). SAGE Publications Ltd. https://doi.org/10.4135/9781446268285.n30

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: Overview and Issues: In Cybercrimes, Cybercriminals and Their Policing, in Crime, Law and Social Change. *Crime, Law and Social Change*, *67*(1), 3–20. https://doi.org/10.1007/s10611-016-9645-3

Levi, M., & Burrows, J. (2008). Measuring the Impact of Fraud in the UKA Conceptual and Empirical Journey. *The British Journal of Criminology*, *48*(3), 293–318. https://doi.org/10.1093/bjc/azn001

Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. (2017). Cyberfraud and the implications for effective risk-based responses: Themes from UK research. *Crime, Law and Social Change*, *67*(1), 77–96. https://doi.org/10.1007/s10611-016-9648-0

Levi, M., & Leighton Williams, M. (2013). Multi-agency partnerships in cybercrime reduction: Mapping the UK information assurance network cooperation space. *Information Management & Computer Security*, *21*(5), 420–443. https://doi.org/10.1108/IMCS-04-2013-0027

Levi, M., & Pithouse, A. (1992). The Victims of Fraud. In D. Downes (Ed.), *Unravelling Criminal Justice: Eleven British Studies* (pp. 229–246). Palgrave Macmillan UK. https://doi.org/10.1007/978-1-349-22044-1_10

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Maguire, M. (2012). Criminal Statistics and the Construction of Crime [in] The Oxford handbook of criminology. In R. Morgan, R. Reiner, & M. Maguire (Eds.), *The Oxford handbook of criminology* (5th ed, pp. 206–244). Oxford University Press. https://contentstore.cla.co.uk/secure/link?id=7630482e-969e-e611-80c7-005056af4099

Maguire, M. (1980). The impact of burglary upon victims. *The British Journal of Criminology*, *20*(3), 261–275. https://doi.org/10.1093/oxfordjournals.bjc.a047171

Maguire, M., & McVie, S. (2017). 7. Crime data and criminal statistics: A critical reflection. In A. Liebling, S. Maruna, & L. McAra (Eds.), *The Oxford Handbook of Criminology* (6th ed., pp. 163–189). Oxford University Press. https://doi.org/10.1093/he/9780198719441.003.0008

Maras, M. H. (2017). *Cybercriminology*. Oxford University Press.

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior*, *92*, 139–150. https://doi.org/10.1016/j.chb.2018.11.002

Matthews, B., & Minton, J. (2017). Rethinking one of criminology's 'brute facts': The age–crime curve and the crime drop in Scotland: *European Journal of Criminology*, *15*(3), 296–320. https://doi.org/10.1177/1477370817731706

Mawby, R. I., & Walklate, S. (1997). The Impact of Burglary: A Tale of Two Cities. *International Review of Victimology*, *4*(4), 267–295. https://doi.org/10.1177/026975809700400403

Mayhew, P., & Dijk, J. V. (2012). Assessing Crime through International Victimization Surveys. In D. Gadd, S. Karstedt, & S. Messner (Eds.), *The SAGE Handbook of Criminological Research Methods* (pp. 253–267). SAGE Publications Ltd. https://doi.org/10.4135/9781446268285.n17

McGuire, D. M., & Dowling, S. (2013a). *Cyber-dependent crimes (Cyber crime: A review of the evidence Chapter 1)* (p. 35). Home Office. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf

McGuire, D. M., & Dowling, S. (2013b). *Cyber-enabled crimes—Fraud and theft (Cyber crime: A review of the evidence Research Report 75)* (p. 27). Home Office. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

McGuire, M. (2019). *It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime*. The Human Factor of Cybercrime; Routledge. https://doi.org/10.4324/9780429460593-1

McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence* (Home Office Research Report 75 Research Report 75; Home Office Research Report

75). Home Office. https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence

Medina-Ariza, J., & Barberet, R. (2003). Intimate Partner Violence in Spain: Findings From a National Survey. *Violence Against Women*, *9*(3), 302–322. https://doi.org/10.1177/1077801202250073

Ministère de l'Intérieur. (2018). *Rapport d'enquête « Cadre de vie et sécurité » 2017*. Ministère de l'Intérieur. https://www.interieur.gouv.fr/Interstats/Actualites/Rapport-d-enquete-Cadre-de-vie-et-securite-2017

Ministerio del Interior. (2020). *Estudio sobre la Cibercriminalidad en España 2019*. Ministerio del Interior. http://www.interior.gob.es/documents/10180/9814700/Estudio+sobre+la+Cibercriminalidad+en+Espa%C3%B1a+2019.pdf/24bd3afb-5a8e-4767-9126-c6c3c256982b

Miró-Llinares, F. (2015). Cibercrimen y vida diaria en el mundo 2.0. *Cibercrimen y Vida Diaria En El Mundo 2.0.*, 415–455.

Miró-Llinares, F. (2011). La oportunidad criminal en el ciberespacio: Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. *Revista electrónica de ciencia penal y criminología*, *13*, 7.

Miró-Llinares, F. (2012). *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons. http://www.atelierlibros.es/libros/el-cibercrimen-fenomenologia-y-criminologia-de-la-delincuencia-en-el-ciberespacio/9788415664185

Miró-Llinares, F. (2013). La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phishing. *Revista Electrónica de Ciencia Penal y Criminología*, *15*(12), 1–53.

Miró-Llinares, F., & Moneva, A. (2019). What about cyberspace (and cybercrime alongside it)? A reply to Farrell and Birks “Did cybercrime cause the crime drop?” *Crime Science*, *8*(1), 12. https://doi.org/10.1186/s40163-019-0107-y

Moneva, A., & Caneppele, S. (2020). 100% sure bets? Exploring the precipitation-control strategies of fixed-match informing websites and the environmental features of their networks. *Crime, Law and Social Change*, *74*(1), 115–133. https://doi.org/10.1007/s10611-019-09871-4

Morena Cusac, J. (2020, February 26). Desarticulat un grup que estafava persones grans per telèfon. *Betevé*. https://beteve.cat/societat/desmantellen-grup-estafa-persones-grans-telefon/

National Academies of Sciences, E. (2016). *Modernizing Crime Statistics: Report 1: Defining and Classifying Crime*. https://doi.org/10.17226/23492

Newman, G. R., & Clarke, R. V. (2003). *Superhighway Robbery: Crime Prevention and E-commerce Crime*. Willan Publishing. https://www.iberlibro.com/9781843920182/Superhighway-Robbery-Crime-Prevention-E-commerce-1843920182/plp

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, *5*(1), 21.

Norris, G., Brookes, A., & Dowell, D. (2019). The Psychology of Internet Fraud Victimisation: A Systematic Review. *Journal of Police and Criminal Psychology*, *34*(3), 231–245. https://doi.org/10.1007/s11896-019-09334-5

Office for National Statistics. (2018). *Overview of fraud and computer misuse statistics for England and Wales—Crime Survey for England and Wales*. Office for National Statistics. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudandcomputermisusestatisticsforenglandandwales/2018-01-25

Payne, B. K. (2020). Criminals Work from Home during Pandemics Too: A Public Health Approach to Respond to Fraud and Crimes against those 50 and above. *American Journal of Criminal Justice*. https://doi.org/10.1007/s12103-020-09532-6

Pepinsky, H. E. (1980). *Crime Control Strategies: An Introduction to the Study of Crime*. Oxford University Press.

Policastro, C., & Payne, B. K. (2015). Can You Hear Me Now? Telemarketing Fraud Victimization and Lifestyles. *American Journal of Criminal Justice*, *40*(3), 620–638. https://doi.org/10.1007/s12103-014-9279-x

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267–296. https://doi.org/10.1177/0022427810365903

Pratt, T. C., & Turanovic, J. J. (2016). Lifestyle and Routine Activity Theories Revisited: The Importance of “Risk” to the Study of Victimization. *Victims & Offenders*, *11*(3), 335–354. https://doi.org/10.1080/15564886.2015.1057351

Pratt, T. C., Turanovic, J. J., Fox, K. A., & Wright, K. A. (2014). Self-Control and Victimization: A Meta-Analysis. *Criminology*, *52*(1), 87–116. https://doi.org/10.1111/1745-9125.12030

PricewaterhouseCoopers. (2020). *PwC’s Global Economic Crime and Fraud Survey 2020* (p. 14).

Pridemore, W. A., Makel, M. C., & Plucker, J. A. (2018). Replication in Criminology and the Social Sciences. *Annual Review of Criminology*, *1*(1), 19–38. https://doi.org/10.1146/annurev-criminol-032317-091849

Reep-van den Bergh, C. M. M., & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science*, *7*(1), 5. https://doi.org/10.1186/s40163-018-0079-3

Reisig, M. D., & Holtfreter, K. (2013). Shopping fraud victimization among the elderly. *Journal of Financial Crime*, *20*(3), 324–337. https://doi.org/10.1108/JFC-03-2013-0014

Reisig, M. D., Pratt, T. C., & Holtfreter, K. (2009). Perceived Risk of Internet Theft Victimization: Examining the Effects of Social Vulnerability and Financial Impulsivity. *Criminal Justice and Behavior*. https://doi.org/10.1177/0093854808329405

Reyns, B. W. (2013). Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses. *Journal of Research in Crime and Delinquency*. https://doi.org/10.1177/0022427811425539

Reyns, B. W., & Henson, B. (2015). The Thief with a Thousand Faces and the Victim With None: Identifying Determinants for Online Identity Theft Victimization With Routine Activity Theory. *International Journal of Offender Therapy and Comparative Criminology*. https://doi.org/10.1177/0306624X15572861

Robert, P., Zauberman, R., Miceli, L., Névanen, S., & Didier, E. (2010). The Victim’s Decision to Report Offences to the Police in France: Stating Losses or

Expressing Attitudes: *International Review of Victimology*, *17*(2). https://doi.org/10.1177/026975801001700203

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rosenfeld, R. (2018). Studying Crime Trends: Normal Science and Exogenous Shocks. *Criminology*, *56*(1), 5–26. https://doi.org/10.1111/1745-9125.12170

Russell G. Smith. (2010). Identity Theft and fraud. In Y. Jewkes & M. Yar (Eds.), *Handbook of Internet Crime* (pp. 273–301). Routledge.

Savolainen, J., & VanEseltine, M. (2018). Replication and Research Integrity in Criminology: Introduction to the Special Issue. *Journal of Contemporary Criminal Justice*, *34*(3), 236–244. https://doi.org/10.1177/1043986218777288

Savona, E. U., & Mignone, M. (2004). The Fox and the Hunters: How IC Technologies Change the Crime Race. *European Journal on Criminal Policy and Research*, *10*(1), 3–26. https://doi.org/10.1023/B:CRIM.0000037562.42520.d7

Schoepfer, A., & Piquero, N. L. (2009). Studying the correlates of fraud victimization and reporting. *Journal of Criminal Justice*, *37*(2), 209–215. https://doi.org/10.1016/j.jcrimjus.2009.02.003

Schreck, C. J. (1999). Criminal victimization and low self-control: An extension and test of a general theory of crime. *Justice Quarterly*, *16*(3), 633–654. https://doi.org/10.1080/07418829900094291

Sherman, L. W., Gartin, P. R., & Buerger, M. E. (1989). Hot Spots of Predatory Crime: Routine Activities and the Criminology of Place*. *Criminology*, *27*(1), 27–56. https://doi.org/10.1111/j.1745-9125.1989.tb00862.x

Simpson, S. S., Rorie, M., Alper, M., Schell-Busey, N., Laufer, W. S., & Smith, N. C. (2014). Corporate Crime Deterrence: A Systematic Review. *Campbell Systematic Reviews*, *10*(1), 1–105. https://doi.org/10.4073/csr.2014.4

Skogan, W. G. (1976). Citizen Reporting of Crime: Some National Panel Data. *Criminology*, *13*(4), 535–549. https://doi.org/10.1111/j.1745-9125.1976.tb00685.x

Skogan, W. G. (1977). Dimensions of the Dark Figure of Unreported Crime. *Crime & Delinquency*, *23*(1), 41–50. https://doi.org/10.1177/001112877702300104

Skogan, W. G. (1984). Reporting Crimes to the Police: The Status of World Research: *Journal of Research in Crime and Delinquency*, *21*(2). https://doi.org/10.1177/0022427884021002003

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. *International Journal of Information Security and Privacy (IJISP)*. www.igi-global.com/article/a-meta-analysis-of-studies-on-protection-motivation-theory-and-information-security-behaviour/145408

Sorell, T., & Whitty, M. (2019). Online romance scams and victimhood. *Security Journal*, *32*(3), 342–361. https://doi.org/10.1057/s41284-019-00166-w

Spalek, B. (1999). Exploring the Impact of Financial Crime: A Study Looking into the Effects of the Maxwell Scandal upon the Maxwell Pensioners. *International Review of Victimology, 6*(3), 213–230. https://doi.org/10.1177/026975809900600304

Spanish Criminal Code. Retrieved 6 July 2020, from https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

Stajano, F., & Wilson, P. (2011). Understanding scam victims: Seven principles for systems security. *Communications of the ACM, 54*(3), 70–75. https://doi.org/10.1145/1897852.1897872

Levitt, S. D. & Dubner, S. J. (2005). *Freakonomics: A Rogue Economist Explores the Hidden Side of Everything*. William Morrow.

Strom, K. J., & Smith, E. L. (2017). The Future of Crime Data. *Criminology & Public Policy, 16*(4), 1027–1048. https://doi.org/10.1111/1745-9133.12336

Suler, J. (2004). The Online Disinhibition Effect. *CyberPsychology & Behavior*, *7*(3). https://doi.org/10.1089/1094931041291295

Sweeten, G. (2020). Standard Errors in Quantitative Criminology: Taking Stock and Looking Forward. *Journal of Quantitative Criminology, 36*(2), 263–272. https://doi.org/10.1007/s10940-020-09463-9

Tade, O., & Aliyu, I. (2011). Social Organization of Internet Fraud among University Undergraduates in Nigeria. *International Journal of Cyber Criminology*, *5*(2), 16.

Tarling, R., & Morris, K. (2010). Reporting Crime to the Police. *The British Journal of Criminology*, *50*(3), 474–490. JSTOR.

Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2016). The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave? *Justice Quarterly*, *33*(5), 890–911. https://doi.org/10.1080/07418825.2014.994658

Tilley, N. (2018). Privatizing Crime Control. *The ANNALS of the American Academy of Political and Social Science, 679*(1), 55–71. https://doi.org/10.1177/0002716218775045

Tilley, N., Farrell, G., & Tseloni, A. (2018). Doing Quantitative Data Analysis in Criminological Research. In P. Davies & P. Francis (Eds.), *Doing Criminological Research* (3rd ed.). SAGE Publications Ltd.

Titus, R. M., & Gover, A. R. (2001). Personal Fraud: The Victims and the Scams. In G. Farrell & K. Pease (Eds.), *Repeat Victimization*. Criminal Justice Press.

Titus, R. M., Heinzelmann, F., & Boyle, J. M. (1995). Victimization of Persons by Fraud. *Crime & Delinquency*, *41*(1), 54–72. https://doi.org/10.1177/0011128795041001004

Tolsma, J., Blaauw, J., & te Grotenhuis, M. (2012). When do people report crime to the police? Results from a factorial survey design in the Netherlands, 2010. *Journal of Experimental Criminology*, *8*(2), 117–134. https://doi.org/10.1007/s11292-011-9138-4

Tonry, M. (2014). Why Crime Rates Are Falling throughout the Western World. *Crime and Justice*, *43*(1), 1–63. https://doi.org/10.1086/678181

Torra, V., Domingo-Ferrer, J., Mateo-Sanz, J. M., & Ng, M. (2006). Regression for ordinal variables without underlying continuous variables. *Information Sciences*, *176*(4), 465–474. https://doi.org/10.1016/j.ins.2005.07.007

Torrente, D., Gallo, P., & Oltra, C. (2017). Comparing crime reporting factors in EU countries. *European Journal on Criminal Policy and Research*, *23*(2), 153–174. https://doi.org/10.1007/s10610-016-9310-5

Torruela, O. (2020, May 4). La ciberseguretat, clau en la societat digital. *El País*. https://cat.elpais.com/cat/2020/04/05/opinion/1586110025_924538.html

Tseloni, A., Farrell, G., Thompson, R., Evans, E., & Tilley, N. (2017). Domestic burglary drop and the security hypothesis. *Crime Science*, *6*(1), 3. https://doi.org/10.1186/s40163-017-0064-2

Tseloni, A., Mailley, J., Farrell, G., & Tilley, N. (2010). Exploring the international decline in crime rates: *European Journal of Criminology*. https://doi.org/10.1177/1477370810367014

Tunley, M. (2014). *Mandating the Measurement of Fraud—Legislating against Loss*. Palgrave Macmillan UK. https://www.palgrave.com/gp/book/9781137406279

Tyler, T. R., & Fagan, J. (2008). Legitimacy and Cooperation: Why Do People Help the Police Fight Crime in Their Communities. *Ohio State Journal of Criminal Law*, *6*, 231–275.

UK Finance. (2018). *Fraud the Facts 2018*. UK Finance. https://www.ukfinance.org.uk/wpcontent/ uploads/2018/07/Fraud-the-facts-Digital-version-August-2018.pdf

United Nations Office on Drugs and Crime. (2015). *International classification of crime for statistical purposes.* United Nations Office on Drugs and Crime.

van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, *123*, 29–39. https://doi.org/10.1016/j.ijhcs.2018.11.003

van de Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big Five Personality Traits of Cybercrime Victims. *Cyberpsychology, Behavior, and Social Networking*, *20*(7), 407–412. https://doi.org/10.1089/cyber.2017.0028

van de Weijer, S. G. A., Leukfeldt, R., & Bernasco, W. (2018). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology*, 1477370818773610. https://doi.org/10.1177/1477370818773610 van de Weijer, S., Leukfeldt, R., & Van der Zee, S. (2020). Reporting cybercrime victimization: Determinants, motives, and previous experiences. *Policing: An International Journal*, *43*(1), 17–34. https://doi.org/10.1108/PIJPSM-07-2019-0122

van Dijk, J., & Tseloni, A. (2012). Global Overview: International Trends in Victimization and Recorded Crime. In J. van Dijk, A. Tseloni, & G. Farrell (Eds.), *The International Crime Drop: New Directions in Research* (pp. 11–36). Palgrave Macmillan UK. https://doi.org/10.1057/9781137291462_2

van Dijk, J. V. (2015). The case for survey-based comparative measures of crime: *European Journal of Criminology*. https://doi.org/10.1177/1477370815585446

van Wilsem, J. (2013). 'Bought it, but Never Got it' Assessing Risk Factors for Online Consumer Fraud Victimization. *European Sociological Review*, *29*(2), 168–178. https://doi.org/10.1093/esr/jcr053

Van Wyk, J., & Benson, M. L. (1997). Fraud victimization: Risky business or just bad luck? *American Journal of Criminal Justice*, *21*(2), 163–179. https://doi.org/10.1007/BF02887448

Van Wyk, J., & Mason, K. A. (2001). Investigating Vulnerability and Reporting Behavior for Consumer Fraud Victimization: Opportunity as a Social Aspect of Age. *Journal of Contemporary Criminal Justice*, *17*(4), 328–345. https://doi.org/10.1177/1043986201017004003

Wall, D. S. (2007). Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace (revised May 2010). *Police Practice and Research*, *8*(2), 183–205. https://doi.org/10.1080/15614260701377729

Wall, D. S. (2008). *Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime* (SSRN Scholarly Paper ID 1124662). Social Science Research Network. https://papers.ssrn.com/abstract=1124662

Warner, J. (2011). Understanding Cyber-Crime in Ghana: A View from Below. *International Journal of Cyber Criminology*, *5*(1), 14.

Weber, M. (1904). *"Objectivity" in Social Science and Social Policy*. Methodology of Social Sciences; Routledge. https://doi.org/10.4324/9781315124445-2

Webster, J., & Drew, J. M. (2017). Policing advance fee fraud (AFF): Experiences of fraud detectives using a victim-focused approach. *International Journal of Police Science & Management*, *19*(1), 39–53. https://doi.org/10.1177/1461355716681810

Welsh, B. C., & Farrington, D. P. (2004). Evidence-based Crime Prevention: The Effectiveness of CCTV. *Crime Prevention and Community Safety*, *6*(2), 21–33. https://doi.org/10.1057/palgrave.cpcs.8140184

Weulen Kranenbarg, M., Ruiter, S., & Van Gelder, J.-L. (2019). Do cyber-birds flock together? Comparing deviance among social network members of cyber-dependent offenders and traditional offenders. *European Journal of Criminology*, Online First 2019. https://doi.org/10.1177/1477370819849677

Whitty, M. T. (2013). The Scammers Persuasive Techniques ModelDevelopment of a Stage Model to Explain the Online Dating Romance Scam. *The British Journal of Criminology*, *53*(4), 665–684. https://doi.org/10.1093/bjc/azt009

Whitty, M. T. (2015). Anatomy of the online dating romance scam. *Security Journal*, *28*(4), 443–455. https://doi.org/10.1057/sj.2012.57

Whitty, M. T. (2018). 419 – It'S Just A Game: Pathways To Cyber-Fraud Criminality Emanating From West Africa. *International Journal of Cyber Criminology*, *12*(1). https://doi.org/10.5281/ZENODO.1467848

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277–292. https://doi.org/10.1108/JFC-10-2017-0095

Wickham, H. (2014). Tidy Data. *Journal of Statistical Software*, *59*(1), 1–23. https://doi.org/10.18637/jss.v059.i10

Wickham, H. (2016). *ggplot2: Elegant Graphics for Data Analysis* (2nd ed.). Springer International Publishing. https://doi.org/10.1007/978-3-319-24277-4

Wickham, H. (2017). *Tidyverse: Easily Install and Load the 'Tidyverse'.* https://CRAN.R-project.org/package=tidyverse

Wickham, H., Averick, M., Bryan, J., Chang, W., McGowan, L. D., François, R., Grolemund, G., Hayes, A., Henry, L., Hester, J., Kuhn, M., Pedersen, T. L., Miller, E., Bache, S. M., Müller, K., Ooms, J., Robinson, D., Seidel, D. P., Spinu, V., … Yutani, H. (2019). Welcome to the Tidyverse. *Journal of Open Source Software*, *4*(43), 1686. https://doi.org/10.21105/joss.01686

Will, S. (2013). America's Ponzi Culture. In S. Will, S. Handelman, & D. C. Brotherton (Eds.), *How They Got Away with It* (pp. 45–67). Columbia University Press; JSTOR. https://doi.org/10.7312/will15690.7

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, *120*, 1–13. https://doi.org/10.1016/j.ijhcs.2018.06.004

Williams, M. L. (2016). Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level.

The British Journal of Criminology, *56*(1), 21–48. https://doi.org/10.1093/bjc/azv011

Wolpaw Reyes, J. (2007). Environmental Policy as Social Policy? The Impact of Childhood Lead Exposure on Crime. *The B.E. Journal of Economic Analysis & Policy*, *7*(1). https://doi.org/10.2202/1935-1682.1796

Wright, R., & Jaques, S. (2017). Property Crime. In *Oxford Bibliographies*. Oxford University Press. https://www.oxfordbibliographies.com/view/document/obo-9780195396607/obo-9780195396607-0016.xml

Xie, M., & Baumer, E. P. (2019). Neighborhood immigrant concentration and violent crime reporting to the police: A multilevel analysis of data from the National Crime Victimization Survey. *Criminology*, *57*(2), 237–267. https://doi.org/10.1111/1745-9125.12204

Yar, M. (2005). The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407–427. https://doi.org/10.1177/147737080556056

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and Society*. New York: SAGE Publications Ltd. https://uk.sagepub.com/en-gb/eur/cybercrime-and-society/book260644

Zimring, F. E. (2007). The Great American Crime Decline. In *The Great American Crime Decline*. Oxford University Press. https://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780195181159.001.0001/acprof-9780195181159

APPENDICES

Appendix A. Tables with the results for the regression analyses in CHAPTER V

Table 12. **Resultados de la regresión logística multinomial realizada para contrastar la H$_1$**

Variable	Fraude telefónico					Fraude en persona					Otros				
	B	SE	OR	95% CI		B	SE	OR	95% CI		B	SE	OR	95% CI	
Sexo (ref = Hombre)															
Mujer	-0,02	0,16	0,98	[0,72, 1,34]		-0,04	0,16	0,96	[0,70, 1,32]		0,15	0,20	1,16	[0,79, 1,71]	
Edad (ref = De 16 a 25)															
De 26 a 40	0,59	0,31	1,81	[0,98, 3,33]		0,08	0,33	1,08	[0,57, 2,07]		0,70	0,47	2,02	[0,80, 5,07]	
De 41 a 64	0,76	0,33	2,14	[1,13, 4,05]	*	0,50	0,34	1,65	[0,85, 3,20]		1,32	0,48	3,73	[1,45, 9,59]	**
Mayor de 65	0,62	0,54	1,86	[0,64, 5,38]		1,08	0,52	2,95	[1,07, 8,16]	*	1,06	0,69	2,88	[0,74, 11,22]	
Lugar de nacimiento (ref = España)															
Extranjero	0,05	0,24	1,05	[0,66, 1,68]		0,28	0,24	1,33	[0,82, 2,14]		0,29	0,29	1,34	[0,76, 2,38]	
Nivel educativo (ref = Ninguno o educación primaria)															
Educación secundaria	-0,47	0,30	0,62	[0,34, 1,13]		-0,72	0,30	0,48	[0,27, 0,88]	*	-0,43	0,37	0,65	[0,32, 1,34]	
Bachillerato o formación profesional	-0,53	0,27	0,59	[0,35, 1,01]		-0,92	0,27	0,40	[0,24, 0,68]	**	-0,48	0,32	0,62	[0,33, 1,16]	
Educación superior	-0,87	0,27	0,42	[0,25, 0,71]	**	-0,96	0,26	0,38	[0,23, 0,64]	***	-1,04	0,32	0,35	[0,19, 0,67]	**
Situación profesional (ref = Estudiante)															
Desempleado o empleado del hogar	-0,41	0,40	0,66	[0,30, 1,45]		0,44	0,46	1,55	[0,63, 3,85]		-0,90	0,59	0,41	[0,13, 1,29]	
Jubilado	-0,16	0,54	0,86	[0,29, 2,49]		0,64	0,58	1,90	[0,61, 5,95]		0,24	0,69	1,27	[0,33, 4,90]	
Trabajador a tiempo completo	-0,51	0,35	0,60	[0,30, 1,20]		0,26	0,43	1,30	[0,56, 3,02]		-0,42	0,51	0,66	[0,24, 1,78]	
Trabajador a tiempo parcial	-0,27	0,40	0,76	[0,35, 1,67]		-0,08	0,49	0,92	[0,35, 2,41]		-0,31	0,56	0,74	[0,25, 2,21]	
Otros [a]	-	-	-	- -		-	-	-	- -		-	-	-	- -	
Situación económica (ref = Muy buena)															
Buena	-0,90	0,39	0,41	[0,19, 0,87]	*	-0,63	0,43	0,53	[0,23, 1,23]		-0,61	0,48	0,55	[0,21, 1,41]	
Ni buena ni mala	-0,55	0,45	0,58	[0,24, 1,39]		-0,62	0,50	0,54	[0,20, 1,42]		-1,28	0,60	0,28	[0,09, 0,89]	*
Mala	-0,50	0,41	0,60	[0,27, 1,35]		-0,42	0,45	0,65	[0,27, 1,59]		-0,94	0,53	0,39	[0,14, 1,10]	
Muy mala	-0,54	0,49	0,58	[0,23, 1,51]		0,14	0,51	1,15	[0,42, 3,14]		0,12	0,58	1,13	[0,36, 3,48]	
Discapacidad (ref = Sí)															

No	0,33	0,32	1,40	[0,74,	2,64]	0,05	0,31	1,05	[0,58,	1,91]	0,41	0,39	1,51	[0,70,	3,25]
(Constante)	0,46	0,60	1,59	[0,49,	5,14]	0,15	0,65	1,17	[0,33,	4,13]	-0,82	0,76	0,44	[0,10,	1,96]
Desviación residual															2984,46
AIC															3098,46

Nota: B = coeficientes; SE = error estándar; OR = odds ratio; CI = intervalo de confianza; * p < 0,05, ** p < 0,01, *** p < 0,001; AIC = Criterio de información de Akaike,

[a] No se muestran los resultados de esta categoría por tener un número de casos demasiado bajo (*n* = 21)

Table 13. **Resultados de las regresiones lineales realizadas para contrastar la H2**

Variable	Impacto económico					Impacto psicológico					Molestias				
	B	SE	OR	95% CI		B	SE	OR	95% CI		B	SE	OR	95% CI	
Tipo de fraude (ref = Online)															
Telefónico	0,17	0,18	1,18	[0,82, 1,70]		0,58	0,23	1,78	[1,13, 2,79]	*	0,77	0,17	2,15	[1,55, 2,99]	***
En persona	0,31	0,19	1,37	[0,94, 2,00]		0,44	0,24	1,55	[0,97, 2,49]		0,23	0,18	1,26	[0,89, 1,78]	
Otros	0,39	0,23	1,48	[0,94, 2,32]		-0,08	0,29	0,93	[0,53, 1,63]		0,33	0,21	1,40	[0,93, 2,10]	
Sexo (ref = Hombre)															
Mujer	-0,03	0,15	0,97	[0,73, 1,30]		0,71	0,18	2,02	[1,42, 2,89]	***	0,77	0,13	2,17	[1,67, 2,81]	***
Edad	0,01	0,01	1,01	[1,00, 1,02]		0,02	0,01	1,02	[1,00, 1,04]	*	-0,02	0,01	0,98	[0,97, 0,99]	***
Lugar de nacimiento (ref = Español)															
Extranjero	-0,01	0,22	0,99	[0,64, 1,53]		0,43	0,28	1,53	[0,89, 2,64]		0,03	0,20	1,03	[0,69, 1,52]	
Nivel educativo	-0,09	0,07	0,91	[0,79, 1,05]		-0,37	0,09	0,69	[0,58, 0,82]	***	-0,10	0,07	0,90	[0,80, 1,03]	
Situación profesional (ref = Estudiante)															
Desempl, o empl, hogar	1,29	0,38	3,64	[1,73, 7,63]	***	-0,63	0,47	0,53	[0,21, 1,35]		0,07	0,34	1,07	[0,55, 2,11]	
Jubilado	1,01	0,46	2,75	[1,12, 6,80]	*	-0,27	0,58	0,76	[0,25, 2,36]		0,55	0,42	1,74	[0,76, 3,96]	
Trab, tiempo completo	1,27	0,32	3,55	[1,89, 6,65]	***	-0,02	0,40	0,98	[0,44, 2,16]		0,36	0,29	1,43	[0,80, 2,54]	
Trab, tiempo parcial	1,01	0,37	2,73	[1,31, 5,69]	**	-0,26	0,47	0,77	[0,31, 1,92]		0,38	0,34	1,47	[0,75, 2,86]	
Otros [a]	-	-	-	- -		-	-	-	- -		-	-	-	- -	
Situación económica	-0,02	0,07	0,98	[0,86, 1,13]		-0,35	0,09	0,70	[0,59, 0,83]	***	-0,23	0,06	0,80	[0,70, 0,90]	***
Discapacidad (ref = Sí)															
No	-0,54	0,27	0,58	[0,34, 0,99]	*	-0,15	0,34	0,86	[0,44, 1,68]		-0,49	0,25	0,62	[0,38, 1,00]	
Pérdida económica	-	-	-	- -		0,34	0,04	1,40	[1,30, 1,50]	***	0,31	0,03	1,37	[1,30, 1,44]	***
Percepción de la seg, local	0,02	0,04	1,02	[0,95, 1,09]		-0,15	0,04	0,86	[0,79, 0,94]	***	-0,08	0,03	0,93	[0,87, 0,99]	*
(Constante)	3,87	0,78	48,11	[10,39, 222,74]	***	2,91	0,98	18,35	[2,66, 126,76]	**	6,37	0,72	586,27	[143,57, 2393,97]	***
RSE					2,43					3,03					2,21
R^2 ajustado					0,03					0,15					0,17

Nota: B = coeficientes; SE = error estándar; OR = odds ratio; CI = intervalo de confianza; * p < 0,05, ** p < 0,01, *** p < 0,001; RSE = error estándar residual

[a] No se muestran los resultados de esta categoría por tener un número de casos demasiado bajo (*n* = 21),

Table 14. **Resultados de la regresión logística binomial realizada para contrastar la H_3**

Variable	B	SE	OR	95% CI		
Tipo de fraude (ref = Online)						
Telefónico	-1,24	0,19	0,29	[0,20,	0,42]	***
En persona	-1,35	0,20	0,26	[0,17,	0,39]	***
Otros	-0,68	0,24	0,51	[0,32,	0,82]	**
Sexo (ref = Hombre)						
Mujer	-0,14	0,15	0,87	[0,65,	1,16]	
Edad (ref = De 16 a 25)						
De 26 a 40	0,08	0,28	1,09	[0,62,	1,88]	
De 41 a 64	0,45	0,30	1,56	[0,87,	2,78]	
Mayor de 65	-0,46	0,49	0,63	[0,24,	1,64]	
Lugar de nacimiento (ref = Español)						
Extranjero	0,16	0,23	1,17	[0,76,	1,85]	
Nivel educativo (ref = Ninguno o educación primaria)						
Educación secundaria	0,33	0,28	1,39	[0,80,	2,43]	
Bachillerato o formación profesional	-0,32	0,24	0,72	[0,45,	1,15]	
Educación superior	-0,04	0,24	0,96	[0,60,	1,53]	
Situación profesional (ref = Estudiante)						
Desempleado o empleado del hogar	-0,11	0,38	0,90	[0,42,	1,90]	
Jubilado	0,59	0,52	1,80	[0,65,	5,06]	
Trabajador a tiempo completo	-0,17	0,34	0,84	[0,43,	1,63]	
Trabajador a tiempo parcial	-0,59	0,38	0,55	[0,26,	1,17]	
Otros	-0,04	0,62	0,96	[0,29,	3,45]	
Situación económica (ref = Muy buena)						
Buena	0,04	0,36	1,04	[0,51,	2,08]	
Ni buena ni mala	0,68	0,44	1,97	[0,82,	4,72]	
Mala	-0,15	0,38	0,86	[0,40,	1,81]	
Muy mala	0,45	0,45	1,57	[0,65,	3,75]	
Discapacidad (ref = Sí)						
No	0,63	0,29	1,88	[1,07,	3,28]	*
Pérdida económica (ref = Muy baja)						
Baja	-0,29	0,20	0,74	[0,50,	1,11]	
Alta	0,27	0,21	1,31	[0,87,	1,96]	
Muy alta	0,37	0,22	1,45	[0,94,	2,23]	
Impacto Psicológico	0,12	0,03	1,13	[1,07,	1,19]	***
Molestias	0,15	0,03	1,16	[1,09,	1,24]	***
Percepción de seguridad local	0,00	0,04	1,00	[0,93,	1,08]	
(Constante)	-0,77	0,65	0,46	[0,13,	1,67]	
Desviación residual						1188,10
AIC						1244,10

Nota: B = coeficientes; SE = error estándar; OR = odds ratio; CI = intervalo de confianza; * p < 0,05, ** p < 0,01, *** p < 0,001; AIC = Criterio de información de Akaike,

Appendix B. Tables with odds ratios for CHAPTER VI

Table 15. **Odds rates for fraud reporting statistical models**

Variable	**Fraud reporting Model 1**	**Crime Report Model 2**	**Online fraud reporting Model 4**	**Offline fraud reporting Model 5**	**Crime factors Model 3**
Modus operandi (ref=Internet)					
Telephone	0.092***	0.101***	———	———	0.310***
In-person	0.385***	0.346***	———	———	0.272***
Other	0.365**	0.360**	———	———	0.462**
Don’t know	1.524	1.695	———	———	1.054
Positive opinion local safety	1.048	1.054	1.139·	0.985	1.013
Positive opinion Catalan police	1.086	1.078	1.105	1.063	1.040
Positive opinion local police	0.992	1.002	0.956	1.002	0.930·
Considered a crime	6.278***	———	8.093***	3.556*	———
Financial impact	1.030*	1.031*	1.287**	1.059*	1.129 ·
Annoyance	1.094·	1.065	1.207**	0.960	1.154***
Psychological impact	1.025	1.045	0.955	1.152·	1.129***
Age	1.013	1.012	1.027*	0.993	1.005
Female	0.921	0.835	1.233	1.349	1.051
Financial situation	0.948	0.941	1.010	1.043	1.041
Education	0.981	0.995	1.052	0.830	0.951
Professional situation (ref=Full time)					
Student					
Unemployed /	1.427	0.724	1.424	0.001	0.836
Housekeeper	0.973	0.933	1.170	0.705	1.113
Retired	1.515	0.675	1.203	0.326	0.981
Part time	0.705	0.441·	0.493	0.379	0.587
Other/No response	1.855	1.303	2.25E-07	1.615	1.765
Foreign	0.741	0.749	0.500	0.952	1.113
Disabled	0.822	0.814	0.318·	1.841	0.694
	n=1177	n=804	n=418	n=598	n=1177
Pseudo-R^2	0.20	0.13	0.18	0.15	0.11

Signif. codes: 0‘***’ 0.001‘**’ 0.01‘*’ 0.05‘·’ 0.1‘ ’

Table 16. ***Odds ratios for non-reporting reasons statistical models***

Variable	**Reason A** **Complexity** **Model 6**	**Reason B** **Fear** **Model 7**	**Reason C** **Police can do little** **Model 8**	**Reason D** **Lack of confidence in police** **Model 9**	**Reason E** **Lack of confidence in CJS** **Model 10**	**Reason F** **Insignificance** **Model 11**
Modus operandi (ref=Internet)						
Telephone	1.155*	1.194	1.677**	1.125	1.397·	0.835
In-person	0.870	1.450	1.212	1.041	1.511*	1.149
Other	1.081	1.541	1.373	1.322	1.403	0.782
Don’t know	0.519	------	0.597	0.405	0.473	0.634
Positive opinion local safety	1.030	1.010	0.928·	0.992	0.909*	1.068·
Positive opinion Catalan police	1.009	1.066	0.917*	0.798***	0.839***	1.037
Positive opinion local police	0.981	0.866*	0.881**	0.883*	0.951	1.002
Financial impact	0.980	0.984	1.051	1.013	1.005	0.602***
Annoyance	1.042	1.170	1.098**	1.055	1.068·	0.810***
Psychological impact	1.034	1.627**	1.031	1.070*	1.080**	0.886***
Considered a Crime	0.982	0.979	1.106	1.209	1.134	0.714*
Age	0.989	0.977·	0.981**	0.972**	0.988·	0.996
Female	0.709*	0.886	0.754·	0.916	0.871	0.854
Financial situation	1.020	0.992	0.966	1.062	1.083	0.992
Education	0.922	0.776·	0.937	1.027	0.953	0.870·
Professional situation (ref=Full time)						
Student	0.791	1.114	0.526*	0.609	0.405**	0.965
Unemployed / Housekeeper	1.209	2.246·	1.231	1.430	1.006	1.092
Retired	1.030	3.751*	1.761·	1.103	1.192	1.690·
Part time	0.935	0.977	1.194	0.810	0.941	1.320
Other/No response	1.764	3.098	0.388·	1.710	1.115	1.128
Foreign	1.760*	1.920·	1.115	1.434	0.972	1.134
Disabled	0.862	0.636	0.658	0.942·	0.744	1.032
	n=567	n=63	n=481	n=184	n=357	n=499
Pseudo-R²	0.04	0.11	0.08	0.13	0.09	0.14

Signif. codes: 0‘***’ 0.001‘**’ 0.01‘*’ 0.05‘·’ 0.1‘’