# Cybercrime law

Dumortier, Franck

*Published in:*
Digital finance

*Publication date:*
2015

*Document Version*
Publisher's PDF, also known as Version of record

# Cybercrime Law: the Payment Fraud Example

Franck Dumortier

Senior Researcher (UNamur – CRIDS)

## I. Introduction

The aim of this contribution is to provide an introductory overview of how criminal law and criminal procedure law deal with cybercrime and to highlight some challenges in this area. The broadness of this topic, as well as the context of this workshop, brought me to illustrate the relations between cybercrime and law through one specific–and very representative–example : payment fraud.

In 2012, criminals acquired EUR 1.33 billion from payment card fraud using cards issued within the Single Euro Payments Area.[1] In 2013, the total value of these fraudulent transactions increased by 8% on the previous year to reach EUR 1.44 billion, representing approximately 3.3% of the EUR 43.6 billion worth of payments in the EU.[2] Everyone will thus agree that, increasingly, payment fraud is a highly profitable criminal activity for their perpetrators as well as a very damageable one for the banking industry and their customers.

The example of payment fraud not only was chosen because of its economic impact, but also because it perfectly illustrates the constantly-evolving relationship between cybercrime, technology and criminal law. In its 2015 Internet Organized Crime Threat Assessment (iOCTA), Europol argues that "the growing proportion of non-cash payments has encouraged an arms race between new attack methods devised by entrepreneurial cybercriminals and the countermeasures and security features implemented by the card industry to protect their customers and business".[3] Clearly, from the private sector perspective–in particular the banking industry–the payment fraud phe-

[1] Europol (2014), "The Internet Organized Crime Threat Assessment (iOCTA)", 2014, p. 34, available at www.europol.europa.eu/iocta/2014/toc.html.

[2] The growth was driven by a 20.6% increase in card-not-present (CNP) fraud. Of the total fraud value, 66% of value resulted from CNP payments, 20% from point-of-sale (PoS) transactions and 14% from transactions at ATMs. See Europol (2015), "The Internet Organized Crime Threat Assessment (iOCTA)", 2015, p. 33, available at www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2015.pdf.

[3] Europol (2015), *op. cit.*

nomenon raises cybersecurity considerations related to the improvement of "technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access".[4] On the other hand, from the law enforcement perspective, a recent study commissioned by the EU Parliament concludes that "the key cybercrime concern for law enforcement is legal in nature rather than simply technical and technological" and describes the key challenge for law enforcement as being "the lack of an effective legal framework for operational activities that guarantees the fundamental rights principles enshrined in EU primary and secondary law".[5] In other words, without denying the fact that technological means available to criminals to protect their identities create challenges for law enforcement agencies (LEAs) to track and prosecute them, it seems that the main difficulty for LEAs in this area is non-technical in nature as it is related to the difficulties of carrying out investigations in multiple jurisdictions: "the whole concept of a territorially based investigative approach conflicts with the borderless nature of cybercrime."[6] In the same way, in its 2012 situation report on payment card fraud in the European Union, Europol concluded that organized crime groups clearly benefit from globalization, using foreign payment card data to purchase on-line goods and services.[7]

In order to fulfil its aims, this contribution is divided into the following main sections: Section II briefly describes the fraud payment phenomenon, Section III provides for an overview of the International, European and Belgian legal framework combatting credit card fraudsters and, finally, Section IV highlights some current challenges faced by LEAs in this area.

## II. Payment Fraud in Practice

Traditionally, two payment fraud types are distinguished depending on whether the payment card is physically present or not *during* the fraudulent transaction:

- Card Present (CP) fraud consists of fraudulent transactions where the card and cardholder are present during the payment processing, typically at ATMs and Point-of-Sale terminals. In this case, the methodology of criminals involves the duplication of a card's magnetic strip with the use of dedicated fraud systems such as ATM Malware. This is often referred to as "skimming".

[4] Art. 16 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[5] F. RAGAZZI and S. SIMON, "The Law Enforcement Challenges of Cybercrime: Are We Really Playing Catch-Up?". This study was commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee. Available at www.europarl.europa.eu/RegData/etudes/STUD/2015/536471/IPOL_STU(2015)536471_EN.pdf.

[6] Europol (2014), *op. cit.*

[7] Europol, "Situation report – Payment card fraud in the European Union: perspective of law enforcement agencies", 2012, available at www.europol.europa.eu/sites/default/files/publications/1public_full_20_sept.pdf.





- Card-Not-Present (CNP) fraud transactions can potentially happen when the cardholder does not or cannot present the actual card for face-to-face examination by a merchant during payment processing (*e.g.* mail-order transactions by mail or fax, telephone orders or orders completed over the Internet). This criminal activity is often referred to as "carding".

Most European countries have already observed an increasing shift from CP towards CNP fraud[8] thanks to the implementation of EMV[9] technology and regional card blocking (also known as geo-blocking), which significantly reduce the risk of successful ATM compromise.[10]

On the other hand, CNP fraud continues to grow steadily as compromised card details stemming from data breaches, social engineering attacks and data stealing malware become more readily available. The media commonly referred to 2014 as the "Year of the data breach", and so far 2015 hasn't been far behind.[11] In the majority of CNP fraud investigations supported by Europol, the primary source of illegal data is data breaches within private industry, often facilitated by insiders and/or malicious software.[12] In addition, payment card data (the credit or debit card number, the security code printed on the card and the expiration date) remains an ideal illicit digital commodity as it is internationally transferable on online carding forums–some of these forums being on the Darknet–facilitating communication and trade between sellers and buyers of compromised data.[13] According to Europol, credit card information and bank account credentials are the most advertised goods on the underground economy's servers.[14]

Finally, payment fraud occurs in a context in which it is easier to steal anonymously than tracking down someone over the net and prosecute the criminals. The possibilities to encrypt data and communications, to connect to the Internet via VPNs,[15] to communicate through services such as Skype, Whatsapp or alike, to share stolen records via

[8] According to card scheme operators Visa and Mastercard, 67% and 69% of losses respectively in 2014 occurred as a result CNP fraud, including online, postal and telephone orders. See Visa Europe 2014 Annual Report, available at http://annualreport.visaeurope.com/Riskmanagement/index.html.

[9] EMV (Europay, MasterCard, Visa) – a global standard for payment cards based on chip-and-PIN technology.

[10] Although ATM-related fraud incidents within the EU decreased by 26% in 2014, overall losses were up 13%. This is mainly due to the cashing out of compromised cards in jurisdictions outside of the EU where EMV (chip and pin) protection has not yet been fully implemented. See Europol (2015), *op. cit.*

[11] See Verizon, "2015 Data Breach Investigations Report", available at www.verizonenterprise.com/DBIR/2015/.

[12] Europol (2014), *op. cit.*

[13] A search query for the term "cvv shop" generates hundreds of relevant results.

[14] Europol (2012), *op. cit.*

[15] A Virtual Private Network (VPN) is a network technology that creates a secure network connection over a public network such as the Internet or a private network owned by a service provider. It is the most common way of hiding your personal information, as well as your location and Internet Protocol address (IP address).

cloud services such as Pastebin,[16] to run or have access to hidden services on Tor,[17] to use anonymous pre-paid debit cards[18] and cryptocurrencies such as bitcoins[19] are examples of technological means that are available to fraudsters to protect their identities when conducting their activities.

After this brief description of the payment fraud phenomenon, the next section provides an overview of the International, European and Belgian legal framework regulating the fight against cybercrime in general and payment fraud in particular.

## III. The Legal Framework

At the international level, the Convention on Cybercrime[20] of the Council of Europe (CoE), known as the Budapest Convention, is the reference binding instrument providing a framework for combatting cybercrime in general (and thus also payment fraud). The Convention on Cybercrime is an international treaty that seeks to harmonize national laws on cybercrime, improve national capabilities for investigating such crimes, and increase cooperation on investigations. The Convention, which is open for worldwide accession, has been ratified by 47 countries, including eight non-members of the Council of Europe such as Australia and the US.[21] Even though three EU Member States (Greece, Ireland and Sweden) still have to ratify it, the Budapest Convention covers a significant "territory" and has an important harmonization effect both in matters of substantive and procedural criminal law. Moreover, the Convention

[16] L. ZELTSER, "The Use of Pastebin for Sharing Stolen Data", 2015, available at https://zeltser.com/pastebin-used-for-sharing-stolen-data.

[17] Tor, an acronym for The Onion Router, makes it possible for users to hide their locations while offering various kinds of services, such as web publishing or an instant messaging server. Using Tor "rendezvouspoints", other Tor users can connect to these hidden services, each without knowing the other's network identity. Hidden services are extremely popular for the trade and distribution of illegal or objectionable materials.

[18] Existing payment types, like prepaid debit cards, can be of great use for micro laundering. Some online platforms (wallets) allow clients to open an online virtual account and link pre-paid debit cards to that account. Because of the international nature of these online services and absence of identification of the account holder, it is quite easy to use a fake or stolen identity where it is impossible for an organization to fully identify the user. See A. ARINK, "Trends in Payment Fraud", 2014, available at http://blog.equens.com/eu/2014/06/trends-in-payment-fraud/.

[19] Bitcoin was created in 2009 by an unknown person or entity using the name Satoshi Nakamato. See "Bitcoin: A Peer-to-Peer Electronic Cash System", available at https://bitcoin.org/bitcoin.pdf Europol has taken a keen interest in Bitcoins. In 2015 Europol produced a report warning of "a virtual and global criminal underground made up of individual criminal entrepreneurs, arguing that VCs increasingly enable individuals to act as freelance criminal entrepreneurs operating on a crime-as-a-service business model without the need for a sophisticated criminal infrastructure to receive and launder money". See Europol, "Massive Changes in the Criminal Landscape", 2015, available at www.europol.europa.eu/sites/default/files/Europol_Org CrimeReport_web-final.pdf.

[20] The Convention is available on the website of the Council of Europe at www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[21] Outside of Europe, Australia, Canada, the Dominican Republic, Japan, Mauritius, Panama, Sri Lanka and the United States are listed as non-Member States that ratified the Convention.





serves as a guideline for any country developing comprehensive national legislation against cybercrime.

Basically, this Convention imposes State Parties:

- to incriminate into their national substantive criminal law a series of cybercrime offences *against* and *by means* of computers.[22] Payment fraud does not have to be expressly incriminated by State Parties, but is covered by the mandatory criminalization of computer-related forgery and fraud. In addition, the Convention focuses on offences against computer data and systems, that is, the so-called offences against the "confidentiality, integrity and availability" of computer systems (illegal access, illegal interception, data interference, system interference and misuse of devices) being often perpetrated when committing payment fraud;
- to provide criminal justice authorities with effective means for investigations through procedural law tools such as the expedited preservation of stored data, the expedited preservation and partial disclosure of traffic data, the search and seizure of computer data, the real-time collection of traffic data, and the interception of content data. The Convention also mandates States to grant law LEAs the power to compel Internet Service Providers (ISPs) to retain data about their customers for law enforcement purposes ("data preservation")[23] and to monitor an individual's online activities in real time. It also contains provisions on cross-border access to data sought by investigating agencies in another country. It is important to note that these investigative means are to apply to the evidence on computer systems related to any criminal offence and not only for offences against and by means of computers. This gives the Convention a very broad scope. Finally, article 15 requires Parties to establish conditions and safeguards to limit and prevent abuse of law enforcement powers and to protect human rights. In this context, it is noteworthy to recall that the European Convention on Human Rights (ECHR), and in particular its article 8, impose State Parties'

[22] Traditionally, two kinds of cyber-offences are distinguished: (1) when a computer is the target of the crime and when (2) a computer is used as a tool to commit a crime. For more information about the classification of cybercrime offences, see D.L. CARTER, "Computer Crime Categories: How techno-criminals Operate?", *FBI Law enforcement Bulletin*, 1995, available at www.ncjrs.gov/pdffiles1/Digitization/156176NCJRS.pdf.

[23] It is noteworthy to mention that the Budapest Convention imposes State Parties to include data preservation as an investigative tool for LEAs but not data retention. Data preservation and data retention are two different criminal investigation mechanisms. Data preservation, also known as "quick freeze", is applied only from the moment a suspicion arises and a preservation order is issued with respect to a particular person. Data retention, on the other hand, is key to conducting investigations into events that took place prior to the moment a criminal suspicion arose. It guarantees the availability of historical data linked to the case under investigation. With this regard, the Budapest Convention imposes State Parties to include data preservation as an investigative tool for LEAs but not data retention. As a reminder, in April 2014, the Grand Chamber of the European Court of Justice (ECJ) declared Directive 2006/24/EC (the Data Retention Directive) invalid on the ground that European Union legislators had exceeded the limits of proportionality in forging the Directive. In particular, the Court held that the Directive entailed serious interference with the rights to privacy and personal data protection of individuals guaranteed by the Charter of Fundamental Rights, and also failed to establish limits on access by competent national authorities, such as prior review by a judicial or an independent administrative authority.

procedural criminal laws to be proportionate as regards interferences with the right to privacy (and data protection) of citizens.

Although the Budapest Convention dates back to 2001, Belgium only ratified it in 2012.[24] Its own Law on Cybercrime[25] (LoC) on the other hand had already been adopted a year before, on 28 November 2000, and fully complies with the Budapest Convention.[26] This law added provisions in both the Belgian Criminal Code (CC) and the Criminal Procedure Code (CPC). For what concerns substantive criminal law, the LoC added cyber-offences to the Belgian CC, covering "computer-related forgery",[27] "computer-related fraud",[28] "external and internal hacking",[29] "data and system Interference",[30] as well as the "possession, production, selling, procurement for use, imports, distribution, dissemination or otherwise making available"[31] any malware, virus, Trojan, including computer data. All these provisions were already applied by courts to punish "skimming" and "carding" behaviors.[32] The LoC also amended the CPC and included procedural provisions related to "expedited preservation of stored

[24] The ratifying Act was published in the Belgian Bulletin of Acts on 21 November 2012.

[25] Belgian Cybercrime Law of 28 November 2000.

[26] By law of 15 May 2006 the LoC was made fully compliant with the Budapest Convention.

[27] Art. 210*bis* CC punishes whoever commits "forgery by inputting, altering or deleting any data that is stored, processed or transmitted by a computer system, or by changing by any other technological means the use of any data in a computer system, resulting in the modification of the legal effect of such data".

[28] Art. 504*quater* punishes whoever "aims to procure without right, with intent to defraud, an economic advantage for himself or for another by inputting, altering or deleting any data that is stored, processed or transmitted by a computer system, or by changing by any other technological means the normal use of data in a computer system".

[29] Art. 550*bis*, §1, CC incriminates "external hacking" while art. 550*bis*, §2, reprehends "internal hacking". "External hacking" is defined as the fact of "obtaining access to a computer system or maintaining access to a computer system, while knowing that he is not entitled thereto". As for "internal hacking", the illicit behavior consists for someone to "exceed his rights of access to a computer system with intent to defraud or with intent to cause damage".

[30] Art. 550*ter* CC punishes whoever "directly or indirectly introduces, alters, deletes or changes by any other technological means the normal use of any data in a computer system, whilst knowing that he is not entitled to do so".

[31] Art. 550*ter*, §4, CC.

[32] Some case-law examples incriminating "skimming" can be found in Corr. Brussels, 6 January 2004, *inédit*, Corr. Dendermonde, 7 June 2004, *inédit*; Corr. Bruges, 8 June 2004, *inédit*, *in* E. ROGER FRANCE, *Aspects juridiques du paiement électronique*, Kluwer, 2004, pp. 239 and 244; Corr. Dendermonde, 14 May 2007, *T. Strafr.*, 2007, liv. 6, p. 403, note E. BAEYENS. For overall case-law reviews related to cybercrime in Belgium, see F. DE VILLENFAGNE, "Chronique de jurisprudence – Criminalité informatique" (covers 2002-2008) *in Revue du droit des technologies de l'information*, No. 39, 2010; F. OMRANI and F. DUMORTIER, "Chronique de jurisprudence – Criminalité informatique" (covers 2009-2011), *Revue du droit des technologies de l'information*, No. 48-49, 2012; C. FORGET and F. DUMORTIER, "Chronique de jurisprudence – Criminalité informatique" (covers 2012-2014), to be published.





computer data/data seizure"[33] and "computer and network search".[34] Recently in this specific matter, controversies arose in Belgium about the respective competences of prosecutors and investigative judges in carrying out investigative means related to the reading of content in suspects' computer systems.[35] Furthermore, the LoC imposes duties to cooperate with LEAs to any person having "particular knowledge about the computer system that is the object of the warrant"[36] and to electronic service providers.[37] The interception of electronic correspondence is covered by articles 90*ter et seq.* of the CPC and, finally, it has to be mentioned that articles 47*sexies* and *octies* of the CPC provide the possibility to use "special research methods of investigation", such as systematic observation and infiltration, but their application in the online environment remains very unclear.[38]

At the European level, a Framework Decision on combating fraud and counterfeiting of non-cash means of payment[39] was adopted in 2001 and defines the fraudulent behaviors that EU States need to consider as punishable criminal offences. The framework decision deliberately avoids references to specific offences under the existing criminal law because they do not cover the same elements everywhere. Instead, the framework decision merely lists the various types of behavior that should be criminal offences throughout the Union. Different types of behavior are defined on the basis of whether they are directed at the payment instrument itself or the making of payment instruments, one or more payment transactions or the system itself for ordering, collecting, processing, clearing and settling payment transactions. Belgium considered that Belgian legislation did not require transposition measures of this framework decision given that general provisions, in line with the Budapest Convention, had already been adopted.[40] However, Belgium might adapt its legislation in the future given that,

[33] Art. 39*bis*, §2, CPC states that "when a public prosecutor [...] discovers data that are stored in a computer system that are useful for the same purposes as the seizure, but the seizure is not desirable, these data shall be copied on storage media belonging to the government, together with the data that are necessary to render these data intelligible. In case of urgency or due to technical reasons, use can be made of the storage media available to the persons entitled to use the computer system".

[34] Art. 88*ter*, §1, CPC states that "when an investigating judge orders a search in a computer system or in a part thereof, this search can be extended to a computer system or a part thereof that is located at another place other than the place where the search takes place [...]".

[35] C. FORGET, "La collecte des preuves informatiques en matière pénale" *in Pas de droit sans technologie*, CUP, No. 158, Brussels, Larcier, 2015, pp. 251 to 278.

[36] Art. 46*bis* and 88*quater* CPC.

[37] Art. 90*quater* CPC.

[38] C. FORGET, *op. cit.*

[39] Council Framework Decision 2001/413/JHA of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment.

[40] Report of the Commission based on article 14 of the Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, COM(2004) 346 final, available at http://ec.europa.eu/transparency/regdoc/rep/1/2004/EN/1-2004-346-EN-F1-1.Pdf.

in the European Cybersecurity Strategy,[41] the Commission declared that "the 2001 framework decision combating fraud and counterfeiting of non-cash means of payments no longer reflects today's realities and new challenges such as virtual currencies and mobile payment. The Commission will assess the level of implementation of the current legislation, consult relevant stakeholders and assess the need for further measures".[42]

In 2013, the European Union strengthened its legislative framework by adopting a Directive on attacks against information systems[43] that replaces and updates the 2005 Framework Decision of the same name and extends its scope to "botnet" attacks. This Directive requires Member States to strengthen national cyber-crime laws and introduce tougher criminal sanctions. However, with regards to criminalization, this Directive does not go beyond the Budapest Convention, which is still considered to be "the legal framework of reference for combating cybercrime, including attacks against information systems".[44] This being said, the 2013 Directive has the merit of reinforcing common rules on criminal liability, criminal sanctions, jurisdiction, the exchange of information between law enforcement authorities, and the establishment of 24/7 contact points to assist in cross-border investigations.[45]

Whilst the legislative activity of the EU aiming at harmonizing national substantive cybercriminal laws mainly built on the Budapest Convention, its input in the field of cooperation between LEAs is substantial and innovative. Firstly, in order to promote cross-border information for the purpose of criminal investigations, The Hague Programme introduced the principle of availability, according to which LEAs have to exchange information across the EU in the same way they would do nationally. Building on this objective, the Stockholm Programme shifted the focus from the prime goal of combating terrorism and organised crime to widespread cross-border crime that has a significant impact on the daily life of the citizens of the EU, *e.g.* also cybercrime. By consequence, and in order to ensure timely access to accurate and up-to-date data for law enforcement authorities, a considerable number of EU instruments and systems[46] have been put in place in recent years, which are also supplemented by international and bilateral arrangements.[47]

[41] European Commission (2013), Communication on a Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace, Brussels, JOIN(2013) 1 final, 7 April.

[42] *Ibid.*

[43] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

[44] *Ibid.*, recital 15.

[45] Note that the G8, CoE and EU have all mandated the establishment of national Cybercrime points of contact to deal with cross-border requests for police cooperation and mutual legal assistance.

[46] The key instruments for information exchange between law enforcement authorities across borders are the Swedish Framework Decision 2006/960 (SFD), the Prüm Decision 2008/615/JHA, the Schengen Information System (SIS (II)), and Council Decision establishing the European Police Office (Europol).

[47] For an overview of the existing EU regulation in this field, see http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/police-cooperation/general/index_en.htm.





In parallel, to be compliant with Human rights, the EU regulator has boundaries for public authorities' competences by stipulating that LEAs should respect citizens' rights to privacy and to data protection when exchanging data.[48] These rights being considered as fundamental, in 2008, the EU adopted a Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.[49] However, this framework decision has been subject to criticism as regard its effectiveness. The main criticism comes from the fact that this instrument has a limited scope of application, since it only applies to cross border data processing and not to processing activities by the police and judiciary authorities at purely national level. This is liable to create difficulties for police and other competent authorities since they are not always able to easily distinguish between purely domestic and cross-border processing or to foresee whether certain personal data may become the object of a cross-border exchange at a later stage. Moreover, because of its nature and content, the framework decision leaves a large room for manœuvre to Member States' national laws in implementing its provisions. Finally, this framework does not apply to instruments enacted at EU level that already have a tailor-made data protection approach in place. This creates a wide landscape of different data protection rules. As part of the review of the data protection framework, the Commission proposed a Directive on 28 January 2012 to enhance the data protection rules in this area.[50]

In December 2012, the Commission published a Communication on the European Information Exchange Model[51] (EIXM), which lays down recommendations on how to increase the efficiency of cross-border information exchanges while ensuring data protection.[52] The Communication concluded that "no new EU-level law enforcement databases or information exchange instruments were needed. However, the existing EU instruments could and should be better implemented, and the exchanges should be organised more consistently". According to a study following up the EIXM process,[53] which was published in January 2015, the need for more EU overall governance and guidance in the field should include better implementation of the Swedish Framework

[48] The main legal basis for privacy and data protection in the LEA area are to be found in article 8 ECHR, articles 7 and 8 EU Charter, Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, Recommendation No. R (87) 15 of the Committee of Ministers to Member States regulating the Use of Personal Data in the Police Sector.

[49] Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

[50] *Cf.* http://ec.europa.eu/dgs/home-affairs/doc_centre/police/docs/com_2012_10_en.pdf.

[51] Communication from the Commission to the European Parliament and the Council, *Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM)*, COM(2012) 735.

[52] The EIXM aims to include all the different EU databases relevant for ensuring security in the EU so that there can be interaction between them, as far as it is needed and permitted, for the purpose of providing effective information exchange across the whole of the EU and maximizing the opportunities presented by technologies for improving citizens' security within a clear framework that also protects their privacy.

[53] Study on the implementation of the European Information Exchange Model (EIXM) for strengthening law enforcement, available at http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/police-cooperation/general/docs/eixm_study_-_final_report_en.pdf.

Decision and of the Prüm Decision by the Member States, better awareness of these instruments among police corps, progress with and a common understanding of the Single Point of Contact (SPOC) concept and the clarification of the channel through which information exchange requests are communicated. With regard to the latter point, the study notes that only a very few Member States have started to promote the Europol channel as the main one for EU information exchange.

This being said, a major improvement to strengthen the EU law enforcement response to cybercrime was the establishment of the Europol Cybercrime Centre (EC3) in 2013, which is instructed to focus on cybercrimes committed by organized groups generating large criminal profits, such as payment fraud. To this end, EC3 is designed to serve as a central hub for criminal information and intelligence related to cybercrime, collecting data from the "widest array of public, private and open source actors; to support Member State operations and investigations, including by providing highly specialized technical and digital forensic support capabilities".[54] EC3's specialized Focal Points (FPs) assist EU Member States in tackling specific forms of cyber criminality. One of these FPs–Focal Point Terminal–specifically deals with payment fraud and provides operational and analytical support to LEAs in cross-border cybercrime investigations. In its first year report, EC3 highlights that Focal Point Terminal supported cross-border investigations in 29 major operations that resulted in the dismantling of three different international networks of credit card fraudsters.[55]

Since September 2014, in order to take into account the international dimension of cybercriminal activities, EC3 has formally hosted the Joint Cybercrime Action Taskforce (J-CAT), made up of cyber liaison officers from EU Member States (Austria, France, Germany, Italy, the Netherlands, Spain and the UK) and non-EU law enforcement partners (Australia, Canada, Colombia and the US). Europol described J-CAT's task as "pro-actively driving intelligence-led coordinated actions against key cybercrime threats and top targets"[56] and credits it, for example, with the success of June 2015's Operation Triangle, which led "to the dismantling of a group of cybercriminals active in Belgium, Italy, Poland, Spain, the United Kingdom, and Georgia, suspected of committing financial fraud involving email account intrusions worth EUR 6 million. A total of 49 suspects were arrested, 58 properties were searched and numerous pieces of evidence, credit cards and cash were seized".[57]

[54] European Commission (2012), Communication from the Commission to the Council and the European Parliament: Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre. Brussels, COM(2012) 140 final, 28 March 2012.

[55] Europol, "European Cybercrime Centre – one year on", 2014, available at www.europol.europa.eu/sites/default/files/publications/ec3_first_year_report.pdf. For more recent achievements of EC3 in this area, see https://www.europol.europa.eu/category/global-categories/Payment-Fraud.

[56] Europol, "Mandate of Joint Cybercrime Action Taskforce Extended after Successful First Six Months", press release, 24 June 2015, available at www.europol.europa.eu/latest_news/mandate-joint-cybercrime-action-taskforce-extended-after-successful-first-six-months.

[57] *Ibid.*





Another significant example illustrating the importance of close collaboration between LEAs around the globe was the success of Operation Onymous in November 2014.[58] The action aimed to stop the sale, distribution and promotion of illegal and harmful items, including weapons and drugs, which were being sold on online "dark" marketplaces. The operation, which was coordinated by EC3, the FBI, the US Immigration and Customs Enforcement's (ICE), Homeland Security Investigations (HSI) and Eurojust, resulted in 17 arrests of vendors and administrators running these online marketplaces and more than 410 hidden services being taken down. In addition, bitcoins worth approximately USD 1 million, EUR 180 000 euro in cash, drugs, gold and silver were seized. Former EC3 Director Troels Oerting emphasized that "today we have demonstrated that, together, we are able to efficiently remove vital criminal infrastructures that are supporting serious organized crime. And we are not 'just' removing these services from the open Internet; this time we have also hit services on the Darknet using Tor where, for a long time, criminals have considered themselves beyond reach. We can now show that they are neither invisible nor untouchable. The criminals can run but they can't hide. And our work continues...".[59]

## IV. Current Challenges of LEAs

Despite important results having been achieved in the fight against payment fraud, Europol officials underline the lack of cybercrime cooperation from particular parts of the world. Troels Oerting, for instance, expressed frustration at Russia's lack of cooperation with J-CAT: "Russia is going through some things that will probably not boost our cooperation", he says. "85 per cent of our cases are Russian-speaking organized cyber groups, so we need to cooperate with these colleagues... but that's right now a bit complicated".[60] Furthermore, the growing use of the Internet in certain parts of the world is often mentioned in cybercrime threat assessments: "Especially in South-east Asia, South America and Africa the number of [Internet] users are (sic) expected to grow fast. Since these are regions with which limited judicial cooperation exists, the EU law enforcement response against perpetrators from those territories will face an increased level of complexity and constraints".[61]

A second series of concerns are related to the effectiveness of judicial cooperation in the field. Police-to-police cooperation for the sharing of data related to cybercrime and e-evidence is much more frequent than mutual legal assistance (the ratio seems to range from 10:1 to 50:1).[62] As a reminder, police cooperation is aimed at exchanging

[58] Information about Operation Onymous is available at www.europol.europa.eu/content/global-action-against-dark-markets-tor-network.

[59] *Ibid.*

[60] "Trouble with Russia, Trouble with the Law: Inside Europe's Digital Crime Unit", *The Guardian*, 15 April 2015, available at www.theguardian.com/technology/2014/apr/15/european-cyber-crime-unit-russia.

[61] Europol, "European Cybercrime Centre – one year on", *op. cit.*, p. 26.

[62] Cybercrime convention committee (T-CY), "Assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime", 2014, available at www.coe.int/t/dghl/cooperation/economiccrime/source/cybercrime/tcy/2014/tcy(2013)17_assess_report_v50adopted.pdf.

intelligence that could lead to the commencement of criminal proceedings and by consequence, information obtained through police cooperation often cannot be used as evidence in criminal proceedings. In some countries, only material received via MLA can be used as evidence in court (for example, in Australia). Others refer to the principle of the free evaluation of evidence in court. In some countries, a further differentiation may be required between MLA during the investigative stage and the trial stage. At the trial stage, evidence may require cooperation through Ministries of Justice or court-to-court cooperation, while other solutions may be possible during the investigative phase.[63] According to Oerting, "Our mutual legal assistance process is not sufficient anymore. There is a big need for speeding up the judicial cooperation. One thing is that police cooperation needs speeding up, but also the judicial because [I cannot obtain evidence]".[64]

Furthermore, the issue of cybercrime law enforcement cooperation and information sharing is complicated by the reality of private sector ownership of digital infrastructure. In terms of information sharing, commentators have noted the private sector's increased reluctance to share data following the Snowden revelations.[65] The private sector seems to draw "a distinction between intelligence-gathering for national security purposes (tainted by the Snowden revelations) and approved criminal inquiries".[66] This issue of the private sector's role in cybercrime law enforcement is closely related to another challenge: the fact that the US and US-based corporations play leading roles in the functioning of the Internet. Thus US legal frameworks have a significant impact on cybercrime law enforcement and the handling of personal data around the world. As a reminder, a private company is subject to the national law of the countries in which it operates. Several cases have spotlighted the public-private information sharing landscape, such as the case in the Belgian courts of Yahoo!. The case concerned whether or not the company was obliged to provide data about its e-mail users to law enforcement. The case largely hinged upon jurisdictional questions over whether US-based Yahoo! was compelled to provide data directly to law enforcement agencies based on the Belgian Criminal Procedure Code.[67]

Finally, a major problem in the EU is the lack of proper regulations for reporting data breaches to police authorities. Law enforcement agencies, even if aware of a breach, have difficulties finding information on, and links to, the point of compromise, stolen data and illegal transactions. The lack of legal provisions on reporting data breaches is not the only problem. One of the key factors making industry reluctant to report incidents to LEAs is the lack of trust in investigative possibilities as well as the need

[63] *Ibid.*

[64] The Guardian, 2015, *op. cit.*

[65] "Has the NSA's Mass Spying Made Life Easier for Digital Criminals?", *The Guardian*, 7 March 2014, available at www.theguardian.com/technology/2014/mar/07/nsa-spying-harmed-digital-crime-fight.

[66] F. RAGAZZI and S. SIMON, *op. cit.*, p. 45.

[67] About this case, see K. DE SCHEPPER, "Medewerking in een virtuele context? Ya! Hoo echter afdwingen?" *A&M*, No. 2-3, 2012, pp. 238 to 243.





to maintain the reputations of the respective private entities. On the other hand, the lack of reporting leads to a small number of international investigations and a low level of prioritization of such cases within LEAs. According to EC3, "the problem ends up with the situation where, despite a dynamic increase in CNP fraud, it is not reflected in the statistics of cases reported and investigated by EU police forces. Consequently, since the problem is not reflected in police statistics, this phenomenon is not prioritized and it is difficult to initiate international cooperation (for example Joint Investigation Teams)".[68]

## V. Conclusion

As already highlighted in the introduction of this contribution, it seems that the main challenges faced by LEAs in their mission to fight against payment fraud are more related to cross-border cooperation and policy difficulties than to technological ones. However, if LEAs argue that territorial legal structures and criminal law procedures stand in the way of their operations because of the "borderless nature of cybercrime", it is important to remind that these challenges should not be an excuse for LEAs to disproportionately limit or affect the rights to privacy, data protection, freedom of expression, and the rights of suspected persons.[69]

The main aim of national criminal procedure laws is to strike the right "balance" between these fundamental right of citizens and the legitimate interests of LEAs to ensure their missions. Even though national criminal procedure laws can still not be fully harmonized at the EU level[70] and certainly not at the International one, this challenge in the fight against cybercrime does not take away the obligation of EU Member States to ensure the safeguarding of EU fundamental rights in any operating framework of internal or transnational cooperation in law enforcement and criminal justice.

A recent example of the necessity to respect fundamental rights while combatting crime is provided by the Court of Justice of the European Union (CJEU) ruling on the Digital Rights Ireland case.[71] Not only has this decision invalidated the EU Data Retention Directive, it is also critical in terms of its impact on limiting the collection and exchange of personal data and for the emphasis it places on the principle of

[68] Europol, "Situation report – Payment card fraud in the European Union: perspective of law enforcement agencies", 2012, *op. cit.*, p. 10.

[69] F. RAGAZZI and S. SIMON, *op. cit.*, p. 46.

[70] From a harmonizing perspective, even though the Lisbon Treaty has merged the three pillars that have been in existence since the Maastricht Treaty, national criminal procedure laws can still not be fully harmonized at the EU level. For an overview of the protection of personal data in the LEA sector before the adoption of the Lisbon Treaty, see Y. POULLET and F. DUMORTIER, "La protection des données à caractère personnel dans le contexte de la construction en piliers de l'Union européenne" *in Défis du droit à la protection à la vie privée*, Cahiers du CRID, Vol. 31, Brussels, Academia-Bruylant, 2008, pp. 447 to 478; J. JOURET, D. MOREAU, F. DUMORTIER, C. GAYREL and Y. POULLET, "La protection des données dans l'Espace européen de liberté, de sécurité et de justice" *Journal de droit européen*, No. 166, pp. 33 to 46.

[71] Judgment of the Court of Justice of the European Union in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, 8 April 2014.

proportionality. The Court's reasoning and findings are thus relevant for assessing the legality and proportionality of cybercrime law enforcement cooperation pertaining to data exchange and processing.

A recent Centre for European Policy Studies (CEPS) report, focusing on the trans-atlantic context and third-country access to data held by private companies for the purposes of law enforcement, maintains that existing legal models should be adhered to and can be made more effective "through a combined approach focused on bilateral case consultations, day-to-day contacts, stronger political commitments, more effective use of existing tools and sound financial, technological and human resources investments in their implementation".[72]

Finally, it should be noted that the right to data protection also covers data security. With this regard, facilitating investigations related to payment fraud at its initial stage–data breach–would be welcomed. As stated earlier, the majority of data breaches are not reported to LEAs, as industry mainly focuses on preventive measures rather than relying on the outcome of investigations. For this reason, the concretization of the proposal to introduce a general obligation for data controllers to notify personal data breaches to their national supervisory authority in article 31 of the GDPR[73] (the proposed General data Protection Regulation) would be of great benefit. In the same way, the adoption of the NIS proposal[74] (the Commission Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union) would be of great help.

[72] S. CARRERA, G. GONZÁLEZ FUSTER, E. GUILD and V. MITSILEGAS, "Access to Electronic Data by Third-Country Law Enforcement Authorities", available at www.ceps.eu/system/files/Access%20to%20Electronic%20Data%20%2B%20covers_0.pdf.

[73] Available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN.

[74] Available at http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1666.