International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime

Filippo Spiezia

Accepted: 21 March 2022 / Published online: 4 April 2022
© @ ERA 2022

Abstract
The topic of the victims of cybercrime is addressed here in the context of a fundamental analysis of modern forms of cross-border crime. In the framework as outlined, international judicial cooperation remains, once again, a key concept in implementing effective and successful strategies, also with a view to ensuring better protection of those who fall victim to these forms of crimes. A powerful stimulus could be provided by the implementation of the new Protocol—adopted in 2021—to the 2001 Budapest Convention, the innovative regulatory framework of which could also positively influence the functioning of the European Agencies long involved in the sector, such as Eurojust and Europol, in their activities in supporting national authorities.

Keywords Victims of cybercrimes · II Protocol to Budapest Convention on Cybercrime · Eurojust · International judicial cooperation

1 Victims in cyberspace

Anyone observing current manifestations of crime cannot fail to notice some of its peculiar features, such as its indisputably global nature, its unprecedented level of growth and the constant and rapid technological advances associated with it. Limiting our gaze to the European dimension, we can affirm that, due to the variety, pervasiveness and danger of the criminal phenomena that today threaten our security, we are witnessing a clear discontinuity with respect to earlier paradigms of the threat,
because of the different intensity and quality.\footnote{For a recent, complete and original analysis of the crimes affecting the EU security, see by the same author “Criminal Threats and EU Response—An Atlas of crime to understand the threats, the responses and the perspectives”, Laurus Robuffo, editor, May 2021.} We seem to have reached a point of no return: we live and operate in a new dimension, in ‘another world’, of which we do not yet know the geography, inhabitants, rules or characteristics. Like Dorothy in the film “The Wizard of Oz”, we can say that “we are definitely not in Kansas anymore”.

This is even more evident with respect to cybercrime. If we look at this phenomenon from the point of view of the attackers, we realise that we are no longer dealing with isolated ‘hackers’, or merely ephemeral groups (more or less dangerous) of cybercrime ‘artisans’: there are now hundreds of transnational organised criminal groups that bill billions of euros. There are multinational crime syndicates on the scene operating with unlimited means, every day, engaged in a fight without barriers. They have infrastructures, weapons and targets, networks, servers, clients, mobile devices, social and instant messaging, on a global scale, 365 days a year, 24 hours a day. The situation appears to be one of unprecedented gravity, putting everyone at risk.

Regarding the victims of cybercrime, the overall number of these is difficult to estimate: what is striking is that in the concrete dynamics of crime, the relationship between victims and perpetrators is becoming increasingly distant, and all too often the perpetrators remain unknown. For some time now,\footnote{See in this regard, A. Apruzzese, “Autori e vittime nella criminalità informatica” in Rivista di Criminologia, Vittimologia e Sicurezza Vol. III, N. 3 Vol IV, N. 1 September 2009—April 2010.} therefore, there has been a need for renewed reflection, not only on the criminological profiles of perpetrators, but above all on the victims of such crimes.

Already in 2015, the United Nations Office on Drugs and Crime estimated that there were approximately 431 million people worldwide who were victims of cybercrime (corresponding to fourteen adults per second). Data published in 2017 by the Norton Cyber Security Insights Report was even more alarming: according to this source, 978 million consumers from 20 different countries worldwide were affected by cyber attacks (including about 16 million in Italy alone).\footnote{The Norton Cyber Security Insights Report is the result of online research conducted on a sample of 21,549 individuals ranging in age from 18 years and older in 20 markets, commissioned by Symantec and conducted by the research firm Reputation Leaders. The margin of error for the overall sample is +/-7%. The report is available at: https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf.} The phenomenon increased in subsequent years: according to data reported in the latest Clusit report for 2021, cyber attacks increased by 12% globally. While the number of victims in the US remained largely unchanged in the first half of 2021 (rising from 45% to 46%), attacks against victims operating in Europe grew significantly (from 15% to 25%), while those against Asian organisations remained unchanged in percentage terms.

Another emerging feature is that states and public organisations are also becoming actual or potential victims of these forms of crime. According to the latest report of the Italian Postal Police on Cyber Security, published on 4 January 2022, there were 5434 attacks on strategic structures in 2021. The data offered by the law enforcement community appears to be approximate by default, because it must be taken into account that thousands of cyber crimes are not reported by the victims, who are often unaware of them. Thus, if 2020 was the worst year ever in terms of the
evolution of cyber threats and their impacts, confirming a persistent trend, this negative trend—confirming a persistent pattern—increased in 2021. And the pandemic situation brought about by COVID-19 played its part: pandemic containment measures forced many people into long periods of lockdown. There was then an increase in cases of domestic violence, child sexual abuse and cybercrime, including various forms of racism and xenophobia.

Despite the uncertainty about the precise extent of the phenomenon, in terms of the actual number of victims affected (individuals and organisations) and how cybercrime attacks the different categories, there is sufficient consensus that it has some distinctive features compared to traditional crime: above all, high levels of access to victims (i.e. perpetrators can reach a significant number of victims) and anonymity, resulting in limited detectability of the action (sometimes victims are not even aware that they have been victimised). The truth is that the more connected we are, the more vulnerable we become, according to the shared message of the then EU counter-terrorism coordinator, Gilles De Kerchove. The latter, on the occasion of the Justice and Home Affairs (JHA) Council meeting on 6 and 7 June 2019, warned EU interior ministers about the risks associated with the future of technology, observing that “the vulnerability of citizens, economies and governments increases proportionally to their connectivity and interdependence and could be triggered with the arrival of 5G and interconnected devices.”

The observation of these dynamics confirms the conviction that a real epochal change in global cyber-security levels has now taken place, caused by the very rapid evolution of the threat actors, of the modalities, of the pervasiveness and effectiveness of the attacks, which has not been matched by a sufficient increase in the countermeasures adopted by the ‘defenders’. It is foreseeable that the exposure of victims will remain very high in the coming years.

2 The fundamental need for international judicial cooperation

The above-mentioned features reflect on the effectiveness of prevention and law enforcement action: in the face of the speed with which so much personal data is illegally acquired and shared among offenders, there is continuing difficulty in accessing digital evidence and information. More and more frequently, in order to reconstruct criminally relevant conduct, judicial and police authorities must acquire and/or preserve and/or document information in digital format, available in jurisdictions other than the domestic ones, ensuring its conformity with the original and its immutability. This information can be found in digital devices, including computers, CDs, hard disks, USB memories, mobile phones, iPods, iPads, digital cameras and video cameras, which are capable of storing and preserving an infinite series of data, information and representations of facts that concern a significant part of the life, relationships and activities of a huge number of people. It is also clear that electronic data that can be used as evidence is often transnational in nature, as it is not linked to the territory where the crime has been committed or the investigation is taking place.

Three aspects, in particular, determine the transnational nature of electronic evidence: its peculiar location and storage; the private sources (Internet Service
Providers) from which it frequently originates, often located in jurisdictions far away from the places where the crime is committed; and the cross-border nature of the criminal groups to which cybercrime conduct can be attributed. Digital data is often stored on servers or computers located in countries other than the one in which the investigation is conducted or the need for investigation exists. This means that police and judicial authorities are confronted with the need to obtain digital evidence from private parties who are bound by a different set of rules than those of the country where they are based. Moreover, in the case of investigations into transnational forms of crime, the fact that the criminal conduct is carried out in several countries makes it even more difficult to identify, collect, store and use electronic data that can be used as criminal evidence. It should therefore be clear why it is increasingly crucial to strengthen the international legal framework, in particular, as regards the provision of effective instruments of judicial cooperation and supranational coordination. Its consolidation is crucial with a view to offering support and protection to so many victims of crime and to ensuring greater resilience in crisis situations, such as the one we would like to leave behind.

The framework described just now led to high expectations for the adoption by the Council of Europe of the Second Protocol to the Budapest Convention of 2001, adopted in November 2021. This, in fact, places at the centre of a new legal framework, the strengthening of the mechanisms of judicial cooperation, whose paradigm is definitely extended to the direct relationship with the providers of digital services (cf. Art. Chap II–Sec. II of the Protocol). Its adoption enhances the role and centrality of the Budapest Convention of 2001, the first international agreement that dealt with crimes committed via the internet. With it, for the first time, emphasis was placed not only on the problems of substantive and procedural law connected to information technology and its growing development, but above all on international judicial cooperation and the necessary coordination of investigations between signatory states. The Budapest Convention was for a long time the only instrument that European states used to implement action against cybercrime and to strengthen judicial cooperation. Its new Additional Protocol will end up relaunching also the applicative sphere of the basic Convention, confirming its centrality in the procedures of international cooperation in the investigation of crimes committed through the Internet and as regards any other form of crime in relation to which the acquisition of digital evidence is necessary. If the Protocol reinforces some of the positive aspects that had already emerged in the parent Convention—such as that of the relationships of suppliers of digital services, whose framework of relations with the requesting authority is definitively clarified—the overall regulatory framework is improved, placing the cooperative dimension at the centre. The tools made available to national judicial authorities have clearly been enriched. One thinks of the new provisions on video-conferencing and joint investigation teams, for which Articles 11 and 12 of the new Protocol establish the regulatory framework, which will be applicable in the absence of other specific provisions between the operating authorities.

Ultimately, it is the entire new legal framework—as highlighted in the preamble of the instrument—that moves along the common thread of ensuring greater justice

---

4This Convention was ratified by Italy on 27 February 2008.
for victims, while ensuring that the risk of accountability for their acts is significantly greater for perpetrators.

The impact of this Protocol could be considerable also by reason of the influence that it could exert on EU regulatory processes to regulate better access to digital evidence on the part of EU member countries. As is well known, in the last decade, the EU has adopted important legislative acts in matters of crime. In fact, with the entry into force of the Lisbon Treaty in 2009, cybercrime was included in Article 83 TFEU as one of the serious and transnational criminal phenomena over which the EU has criminal jurisdiction. It was on the basis of this article, that Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography and Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems, for example, were adopted. However, the particular problems posed by cybercrime and, above all, the obstacles encountered in the collection and exchange of digital evidence, have not been adequately addressed at EU level for a long time. There is still no legal framework governing the collection, preservation and exchange of electronic evidence across the EU Member States, although considerable progress has been made in recent years.

Discussion on an effective reform of the digital evidence system attracted the attention of the European legislator during the thorough French investigations relating to the 2015 Bataclan terrorist attack. This led the European institutions to look for a way to simplify mutual legal assistance and mutual recognition procedures. The need for a legal framework for access to electronic evidence with respect to online service providers operating in the context of the European Union led, as is well known, to the proposal of a legislative initiative by the European Commission presented in April 2018. This is the proposal for a Directive of the European Parliament and of the Council for the introduction of harmonised rules on the appointment of legal representatives by service providers for the purposes of obtaining evidence in criminal proceedings and on a proposal for a Regulation of the European Parliament and of the Council on European orders for the production and preservation of electronic evidence in criminal matters. The aim, in proposing the Directive, is to introduce an obligation for any Internet Service Provider offering services in the EU to appoint a representative in one of the Member States, so as to clearly identify to whom the competent authorities of the Member States may address their orders for obtaining evidence in criminal proceedings and thus facilitate cooperation by internet service providers. A time limit of ten days for providing a response and six hours in case of emergency is also foreseen. The presentation of the proposal by the European Commission

5COM (2018) 226 final.
6COM (2018) 225 final.
7The proposal for a Regulation, currently in the trilogue phase of the institutional dialogue between the European Parliament, the Council and the Commission, allows judicial authorities to issue European orders for the production and preservation of electronic evidence directly against ISPs offering services in the EU. The EU has therefore decided to focus on direct cooperation between public entities and ISPs and on making Internet service providers more responsible: in particular, the latter, which until now cooperated with judicial authorities on a voluntary basis, will be obliged to cooperate and provide the requested data, if the request meets the requirements, as from the adoption of the Regulation.
8The text of the proposed Regulation is available online at this location: https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0005.02/DOC_1&format=PDF.
mission led to an intense debate both within and outside the European institutions. The Council proposed several changes to the Commission’s text and the European Parliament in turn proposed a far greater number of amendments than the Council, focusing in particular on the legal basis used to support the proposal for a regulation.9

It is to be hoped that the adoption of the Second Protocol to the Budapest Convention will also act at this point as a driving force for the completion of the regulatory process under way in the EU, filling a gap that seems obvious to all.

3 The role of Eurojust and the development of virtuous models

Fighting cybercrime is one of Eurojust’s competences. The increase in the number of (computer) frauds and other forms of crime typical of cybercrime is a constant fact in Eurojust’s operations and makes this type of threat, which has become widespread and pervasive, particularly alarming. Analysis of the procedures carried out by the Agency confirms the investigative difficulty in organising a structured and timely response, capable of tracing a chain of criminal activity and going beyond the identification of individual subjects involved in the final phase of a criminal scheme. In this sense, the use of joint investigation teams has proved itself the collaboration instrument par excellence, as it is particularly effective in dealing with the different phases and articulations through which this form of crime develops and the Agency’s activities will be able to benefit from the new Protocol to the Budapest Convention, especially as regards relations with third countries.

Eurojust’s work in the field of cybercrime has intensified in recent years: in 2021, 188 cases of crime in the strict sense of the word and 1453 cases of fraud (often of a cyber nature) were registered with the Agency. Just as many coordination meetings have been organised. The Agency’s coordination and assistance to Member States has resulted in the opening of a dialogue between the different parties that play a role in ensuring the rule of law in cyberspace and, on many occasions, in the achievement of excellent investigative results. Eurojust has often promoted the establishment of joint investigation teams in order to foster the emergence of investigative interests in countries where digital evidence ought to be collected and shared within a team.

Eurojust plays a key role in resolving actual or potential conflicts between states on the identification of the competent state to judge, which, as has already been made

9Specifically, it was pointed out that the invoked provision, Article 82(1) TFEU requires that cooperation take place between authorities performing a judicial function, a description which cannot be attributed to a service provider company such as an internet service provider. In addition, criticism was also levelled at the proposed regulation’s devolution to the service provider of the assessment of compliance the requirements of legality and of respect for the fundamental rights of the European Union. Further elements of criticism related to the lack of provision for the principle of speciality, which it is suggested should be adopted in a broad sense, and the need to introduce an obligation to notify the judicial authority of the service provider’s home state of any request from the issuing authority.

The European Parliament’s position also differed with regard to the use of a directive to introduce an obligation for service providers to establish a registered office in the European Union and appoint legal representatives in order to speed up the acquisition of electronic evidence in criminal proceedings. Parliament believed that this provision should have been included in the text of the regulation to be enacted. Meetings between the institutions were instituted so that, under the legislative procedure, an agreement on the text could be reached rapidly by the European Parliament and the Council of the European Union, with the mediation of the European Commission.
clear, is one of the sore points of cybercrime investigations. Through the involvement of Eurojust in the early stages of the proceedings, state authorities have received specific recommendations that allow them to overcome uncertainties regarding the identification of the competent authority to take the necessary procedural measures and thus to coordinate their efforts more efficiently.

However, it is also worth mentioning how Eurojust is also fostering the formation of cybercrime and virtuous models. Worth referring to, first of all, is the management of the “European Judicial Network on Cybercrime”, which has been operating since 2016, and which consists of a network of contact points and serves as a specialised support centre for prosecutors and judges dealing with cybercrime and with investigations in cyberspace. Cooperation with Europol is also crucial. Most of today’s criminal investigations include a transnational request for access to electronic evidence such as emails, text messages or messaging apps. In a fast-changing online environment, investigators and prosecutors need support in developing knowledge about electronic data recovery. The SIRIUS project, jointly implemented by Eurojust and Europol, addresses this growing need for cross-border access to electronic evidence. The usefulness of the platform is reflected in an annual increase of 18% in 2021 of judicial authorities who are members (bringing the total number to 380 judicial representatives). Together with Europol and the European Judicial Network, SIRIUS published its third annual EU Digital Evidence Situation Report in November 2021. For the first time, the report’s survey results show that SIRIUS is the number one source of information for law enforcement practitioners seeking assistance on data requests, making it the leading reference centre in the field of electronic evidence. The report shows that the volume of cross-border requests made by EU authorities to foreign-based online service providers (OSPs) increased by 27% in 2020 compared to the previous year, and there was a significant (112%) increase in the disclosure of emergency information requested in 2020, compared to 2019.

Europol and Eurojust have championed the need to find adequate tools to solve the problems posed by cybercrime, providing constant specialised support to speed up assistance and reduce the difficulties arising from the lack of uniformity between the laws of the Member States. But in the activities of these agencies, major practical difficulties still stand in the way of effective international cooperation. In particular, the EU still lacks a legal framework that uniformly regulates both the processing and exchange of e-evidence and the storage of electronic data.

Finally, it merits mention that further upstream, there is still a major issue in the area of data retention, i.e., creating a legal regime capable of ensuring the preservation of digital data. In this respect, it should be noted that there is still legal uncertainty due to the lack of an adequate EU regime concerning data retention by private data managers, which authorities can subsequently access. As is well known, the present configuration is a consequence of the pronouncements of the Court of Justice of the

---

10 For a thorough analysis of the role played by Eurojust in this crime area, see “The Final frontier; crime travels on the web”, at p. 166 thereof and chapter 5 of “Criminal Threats and EU response, an Atlas of crime to understand the threats, the responses and the perspectives”, Laurus Robuffo, May 2021.

11 In 2007, Europol and Eurojust published a joint report outlining the persistent challenges identified in practice in combating cybercrime. This can be found at https://www.europol.europa.eu/publications-documents/common-challenges-in-combating-cybercrime.
EU, whereby certain provisions of the European rules concerning retention of the data of telephonic and telematic traffic (in particular, the so-called “Frattini” Directive 2006/24/EC) were annulled, because they were held to be in conflict with certain fundamental rights of the individual (in particular, the right to privacy). The existence of such uncertainty fuels the difficulties encountered by investigating authorities and may lead to limitations in the cooperation and exchange of information between competent authorities in cross-border cases. This must be remedied by providing uniform rules on data retention that respect the fundamental rights of those involved, avoid mass acquisitions and respect the principle of proportionality.

Finally, emerging new technologies, such as the development of 5G networks and the spread of commonly-used devices connected to the internet, require the creation of a new security paradigm and the development of still-young scientific disciplines, such as digital forensics. The professionalisation of this field remains in the EU an open question, and an achievement which must happen if we are to see the birth of a criminal justice system that sees in technology a valuable ally and not merely the weapon of an enemy which must be neutralised.

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

12European Court of Justice, judgement of 21 December 2016, Tele2 and Watson, Joined Cases C-203/15 and C-698/15.

13Digital forensics is concerned with studying, adapting or proposing to improve the results that can be obtained and at the same time better protect the integrity of digital evidence.

14See on this point M.A. Biasiotti, M. Epifani, F. Turchi, Opportunities and challenges for electronic evidence in Informatica e diritto, Vol. XXIV, 2015, no. 1-2, p. 19.