Silvia Signorato*

STRENGTHENING INVESTIGATIVE COOPERATION BETWEEN STATES AS A TOOL TO MORE EFFECTIVELY COMBAT CYBERCRIME AGAINST CHILDREN AND THE ELDERLY.

The number of cybercrimes committed against Children and the elderly is constantly increasing. However, the fight against these crimes is characterized by significant problems. This is not only because many victims do not report these crimes, but also because there are various aporias affecting the investigations. Investigations for the fight against cybercrime often require the collection of evidence in another State. However, this requires investigators experienced in digital evidence and requires cooperation instruments between States which, often enough, imply periods of wait time incompatible with investigative needs. Furthermore, if the principle of double criminality is not satisfied, States do not cooperate. All this highlights the need to rethink the very concept of investigation. It is necessary to be aware that, just as the head is part of the human body, so national investigations are part of a larger investigative body. Hence, the need to reach criminal law and criminal procedures that are the same in all States is urgent. Even if this objective may appear utopian, it is not impossible to achieve and it is necessary to work towards its realization in order to reach a more effective fight against crimes.

Keywords: *Investigations against cybercrime; Children and the elderly as victims of crime; Reporting crime; Investigative cooperation between States.*

* Silvia Signorato, PhD, Associate Professor in Criminal Procedure, University of Padua (Italy), silvia.signorato@unipd.it

1. Introduction: Children and the elderly as victims of crime.

From the point of view of the spread of crime, the Internet has allowed new ways of committing crimes as well as the possibility of perpetrating new kinds of crime. Statistics show that the number of cybercrimes is constantly increasing, year after year. Consequently, the fight against cybercrime needs to be stepped up.

Anyone can be the victim of a cybercrime and this is because it is a particularly insidious type of crime. In particular, children and elderly people are undoubtedly very easy targets of this type of crime because they are among the most vulnerable potential victims. As regards children specifically, extremely serious crimes are perpetrated, such as offences related to child sexual abuse material. Indeed, "as a result of the rapid development of information and communication technology, there has been a significant increase in the number of cases of child pornography" (Pavlović, Paunović 2019: 181). In general, crimes against children are committed using new technologies as much as possible. Consider, for example, that the use of the Internet and new technologies are used as tools to commit the offences of the sale and sexual exploitation of children, online grooming activities on social media, and online gambling platforms (Europol, Internet Organised Crime Threat Assessment (IOCTA), 2021: 10). "Children, all around the world, suffer sexual abuse and exploitation since individuals who seek them out realized that digital technology provides the ability for making profit from their's exploitation" (Pavlović, Paunović, 2020: 318).

As regards elderly people, it should be noted that a significant number of them are not able to use computer systems. However, some services are now available online only. In various States this is the case; for example, for certain banking services, health services[1], and tax data. Moreover, it is possible to communicate with institutions and administrations only by email. Having the possibility of using certain online services is certainly an advantage. However, if online mode is the only way to access services, this becomes a factor of discrimination between those who are able to use computer systems and those who are unable to use them, as in the case of many elderly people. This appears to be of particular concern due to its important consequences.

An elderly person who is unable to use the internet is forced to appoint another person to create his/her IT credentials to access the services. Therefore, such a third person will use these credentials. Or else, the elderly person will have to delegate other people to carry

[1] Examples are booking medical examinations, viewing reports, simply requesting information, etc.

out the IT services on his/her behalf. These behaviours increase the risk of fraud, identity theft and various other cybercrimes committed by people whom the elderly trust (Kratcoski, 2018: 101-123).

Even the elderly who know how to use computer systems are significantly exposed to the risk of being victims of crime. Statistical data show how significant the number of elderly victims of online fraud is. For example, they are victims of Romance Scams[2] conducted by people they meet on social network. Among the pains that such a crime can cause to the victims there is a serious psychological harm (Sorell, Whitty, 2019: 342-361). Phishing is another example of cybercrime in which the elderly person is often the victim.

The risk of ageism is real[3], not only because elderly people are an easy target of crime, but also because, in many States, the action to combat crimes against the elderly is weaker than that against other crimes.

2. Reporting crime.

The number of crimes committed online against the elderly and children is very high. However, it is impossible to provide a reasonable estimate of these crimes because many times they are not reported.

There are many reasons why crimes are not reported. Sometimes, victims are unaware that they suffered a crime, as can happen in the case of unauthorized access to a computer system. It should also be noted that in various States there are victims who do not trust the law enforcements authorities, public prosecutors, judges and institutions because they believe the level of corruption is high and they think they will not get justice. Unfortunately, there are also victims who do not report because they are unable to bear the economic costs of the process. Moreover, since in many States trials may last many years, the elderly often does not report because they have a short life expectancy. In addition, older people often fear reputational damage, i.e., they feel strong shame and guilt for having been the victims of scams or other crimes. What is more, due to age (very young or very old), people may not have the psychological and physical strength to face a criminal trial.

[2] "Romance scams occur when a criminal adopts a fake online identity to gain a victim's affection and trust". See, Federal Bureau of Investigation (FBI), official website: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/romance-scams.

[3] In general, discrimination against older people appears to exist (Sargeant, 2011: 1-15).

The fact that many victims do not report crimes leads to a high number of crimes that the institutions are not aware of, with the consequence that the victims remain unknown. However, it may happen that, regardless of whether or not a complaint exists, in the context of investigations involving other subjects, the investigators discover that there are also victims who have not filed a complaint. This often happens in the context of investigations aimed at contrasting the sexual exploitation of children, since there are cases in which law enforcement agents find images depicting children victims of crimes but whose name and surname, nationality and current age are unknown. Moreover, the photos may have been taken many years ago. In order to identify the victims, various States have provided a/the Victim Identification Taskforce, to identify and offer help to the victims.

It should not be forgotten that victims of crime are often also injured in their hearts and souls. No court will ever heal such a wound. Indeed, the fact of having to face a criminal trial often means additional pain for the victims. At the European level, Directive[4] 2012/29 / EU of the European Parliament and of the Council of 25 October 2012 sets minimum standards on the rights, support and protection of victims of crime. This directive specifies that: «Crime is a wrong against society as well as a violation of the individual rights of victims. As such, victims of crime should be recognised and treated in a respectful, sensitive and professional manner without discrimination of any kind based on any ground such as race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age, gender, gender expression, gender identity, sexual orientation, residence status or health. In all contacts with a competent authority operating within the context of criminal proceedings, and any service coming into contact with victims, such as victim support or restorative justice services, the personal situation and immediate needs, age, gender, possible disability and maturity of victims of crime should be taken into account while fully respecting their physical, mental and moral integrity. Victims of crime should be protected from secondary and repeat victimisation, from intimidation and from retaliation, should receive appropriate support to facilitate their recovery and should be provided with sufficient access to justice».

[4] "Directives have different characteristics. Pursuant to Art. 288 TFEU, they are binding upon Member States only as to the results to be achieved, leaving them free to choose the form and methods to achieve such results. Therefore, directives, like regulations, cannot be applied selectively or partially, but, unlike regulations, they are not directly applicable and become effective in the national legal order only indirectly, that is, by means of the specific measures through which the State must implement them" (R.E. Kostoris, 2018: 25).

For this reason, States should put in place measures aimed at helping people who intend to file a complaint as victims of a crime.

3. The fight against cybercrime regarding children and the elderly.

Effective protection of the victims presupposes that the investigations allow the perpetrator to be identified quickly. However, this is not always the case, due to technical and legal obstacles.

Cybercrime investigations are technical investigations, which require specific digital forensics skills of investigators. However, many investigators lack the necessary technical skills. In this regard, there is a twofold risk. First of all, there is the risk that investigations will be carried out by investigators who are not experts in digital forensics who, involuntarily, commit technical errors that, in certain cases, can affect the admissibility of evidence in a criminal trial. On the contrary, there is a risk that investigators who actually have the technical skills are delegated to carry out an excessive and disproportionate number of investigations, with the consequence that they are forced to select which crimes to prosecute and which to overlook, causing discrimination between the victims.

From a legal point of view, there are some issues.

Firstly, cybercrimes are often characterized by problems inherent to the *locus commissi delicti* or foreign elements. For example, the perpetrator may be foreign, or foreign servers may have been used. However, in cases where it is necessary to collect evidence abroad, there are often obstacles due to the fact that cooperation of other States is usually necessary. It is necessary to point out that a foreign State cooperates only if the investigations concern a fact that the foreign State itself considers a crime (the so-called principle of double criminality). Otherwise, it refuses cooperation. This is what happens in the case of requests for cooperation addressed to the United States in the context of investigations concerning online defamation. In fact, unlike many other states, the United States considers freedom of speech and freedom of the press to prevail over the protection of reputation that the crime of defamation aims to protect. For this reason, Meta Platforms, Inc. (the Facebook company) refuses to cooperate in investigations concerning defamation.

Secondly, "one of the main obstacles is the difficulty in the collection of IP addresses[5], which are very important evidences" (Signorato, 2019: 481). Each State has its own legislation, and there is no uniform law about the retention period of IP addresses.

Thirdly, the States collaborate on the basis of the agreements in place with the State requesting the cooperation. Usually, the collection of evidence required by a European state from another European state is faster and easier than the collection of evidence required by a European / non-European state from a non-European state. This is because almost all European states apply a common discipline, namely Directive 2014/41 / EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (EIO). The latter is a judicial decision issued in or validated by the judicial authority in one EU country to have investigative measures to gather or use evidence in another EU country.

Outside the European states, cooperation takes place on the basis of multilateral or bilateral agreements, which often provide for letters rogatory[6]. However, often the letter rogatory takes a very long time, which contrasts with the need for investigative speed. Indeed, it may happen that the letters rogatory are so slow that often they operate when the evidence has already been canceled.

In summary, although many steps forward have been made globally, the fight against cybercrime still does not seem to be fully satisfactory. The number of experienced digital forensics investigators available at global level is less than what would be needed ideally. Furthermore, the collection of evidence in other States often slows down investigations, sometimes undermining their effectiveness.

4. Conclusions: If the world is interconnected, investigations are also interconnected.

The British mathematician Alan Turing, who was one of the main founders of information technology, wrote that "The displacement of a single electron by a billionth of a centimetre at one moment might make the difference between a man being killed by an avalanche a year later, or escaping" (Turing, 1950: 433–460). Moreover, the American mathematician and meteorologist Edward Lorenz, in a very famous lecture he gave on

[5] IP states for Internet Protocol.

[6] The letter rogatory is based on the "principle of mutual assistance. It consists in a request for evidence collection from one State to another, which is subject to a whole series of controls" (Daniele 2018: 360).

December 1972 at a session of the annual meeting of the AAAS (American Association for the advancement of Science), wondered "A butterfly flapping its wings in Brazil can produce a tornado in Texas?"

From a mathematical and physical point of view, the world is interconnected. The COVID-19 pandemic was and is characterized by a global interconnectedness. Similarly, interconnectedness also exists in investigative matters. Cybercrime is increasingly characterized by elements of extraneousness between victims and criminals and, in addition, by the fact that the corresponding evidence if often found abroad. For example, Romance Scams are often committed by Africans to the detriment of Europeans, using American social networks such as Facebook and having the money credited by the scammed persons on bank accounts located in non-European countries.

In such a scenario, cyber investigations are no longer just national. Rather, they require the acquisition of evidence abroad. However, this entails the need to rethink the same concept of investigation in a global key, in which the whole world is conceived as a single investigative body. In such a view, each state retains its individuality, but as part of a whole. Just like in the human body, the head or arms are parts of the human body. Without a global vision of the repression of crime, the fight against crime, in particular the fight against cybercrime, remains weak. From a practical point of view, it is necessary and urgent to reach a global criminal code and criminal procedure valid in all States. It could be argued that such a solution is utopian and unattainable.

However, various historical cases have shown that actions or measures that appeared to be impossible to implement or to propose at a certain time turned out to be possible later.

Bibliography

Daniele, M. (2018), Letter Rogatory, Ed. Kostoris, R., *Handbook of European Criminal Procedure*, Cham: Springer, p. 360.

Europol, *Internet Organised Crime Threat Assessment (IOCTA*) (2021), Luxembourg: Publications Office of the European Union, p. 10.

Federal Bureau of Investigation (FBI), official website: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/romance-scams

Kostoris, R. (2018), Sources of Law. Ed. Kostoris, R., *Handbook of European Criminal Procedure*, Cham: Springer, p. 25.

Kratcoski, P.C. (2018), The Victim-Offender Relationship in the Criminal Victimization of the Elderly. Kratcoski, P.C., Edelbacher, M. Ed.: Peter C. Kratcoski, Maximilian Edelbacher, *Perspectives on Elderly Crime and Victimization,* Berlin: Springer, pp. 101-123.

Pavlović, Z., Paunović, N., (2019). Criminal Law Protection of Children from Offences related to pornography. Republic of Serbia Autonomous Province of Vojvodina Provincial Protector of Citizens – Ombudsman, Institute of Criminological and Sociological Research, *Yearbook Human rights protection of the right's of the child "30 years after the adoption of the convention on the rights of the child*" (number 2), Novi Sad: Vojvodina Provincial authorities Common Affairs Department, p. 181.

Pavlović, Z., Paunović, N. (2020), Protection of children from sexual abuse and exploitation in International, European and National Legal Framework. Ed.: Republic of Serbia Autonomous Province of Vojvodina Provincial Protector of Citizens – Ombudsman, Institute of Criminological and Sociological Research, *Yearbook Human Rights Protection the Right to Human Dignity* (number 3), Novi Sad: Vojvodina Provincial authorities Common Affairs Department, p. 318.

Sargeant, M. (2011), Age Discrimination and Diversity Multiple Discrimination from an Age Perspective, Cambridge: Cambridge University Press, pp. 1-15.

Signorato, S. (2018), *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino: Giappichelli, pp. 152-180.

Signorato, S. (2019), Ip Address and the fight against child sexual offender after thirty years since the adoption of the Convention on the rights of the child: the need for EU regulation. Republic of Serbia Autonomous Province of Vojvodina Provincial Protector of Citizens – Ombudsman, Institute of Criminological and Sociological Research, *Yearbook human rights protection of the right's of the child "30 years after the adoption of the convention on the rights of the child*" (number 2), Novi Sad: Vojvodina Provincial authorities Common Affairs Department, pp. 481-492.

Sorell, T., Whitty, M. (2019), Online romance scams and victimhood. *Secur J 32*, pp. 342–361.

Turing, A.M. (1950), Computing machinery and intelligence, *Mind,* LIX (236), pp. 433–460.