Contents

A New Right in Criminal Procedure Implied by Human Dignity: The right to Non-Automated Judicial Decision-Making

Silvia Signorato*

Abstract

The right to respect for human dignity is a fundamental right that gives substance to all other rights. Human dignity is inviolable. It prevents any reification of man and postulates respect for the Kantian categorical imperative, which states that «Act in such a way that you treat humanity, whether in your own person or in the person of any other, never merely as a means to an end, but always at the same time as an end».

However, information technology poses new challenges regarding human dignity. This article analyses this issue in relation to the possibility of criminal judgements being issued by machines. In some cases, this kind of judgement is considered acceptable by Article 11 of directive (EU) 2016/680. However, a question must be asked: Does such automated judicial decision-making respect human dignity or not?

The article shows the incompatibility of robotic decisions with the right to respect for human dignity. Consequently, Article 11 of Directive (EU) 2016/680, in that part in which it admits that such judgments can be issued if authorized by Union or Member State law, should be regarded as unlawful.

Keywords: *human dignity, robotic decision, right to non-automated judicial decision-making in criminal matters, Article 11 of Directive (EU) 2016/680, algorithm, machine learning.*

I. Human dignity: An introduction

Human dignity is a multifaceted concept. Such a term comes from the Latin *dignus*. In the legal field, as has happened in other fields, the meaning of the term *dignity* has evolved over time. Initially, its meaning was close to that of *merit* and was associated with a high status in some languages. For example, this is one of the reasons why in the US Declaration of Independence, adopted on 4 July 1776, the term *dignity* is not used.

Therefore, the meaning of the term *human dignity* changes over time. The significant historical evolution of the concept of *human dignity* is reflected in legal semantics. What happened during the Second World War, with unimaginable atrocities against civilian populations, thinking in particular of the Holocaust, brought this concept to the center of the legal debate[1].

* PhD, Assistant Professor in Criminal Procedure, University of Padua (Italy), Lecturer in Criminal Procedure, University of Innsbruck (Austria). Contact: silvia.signorato@unipd.it.

[1] A. Barak, *Human dignity as a value and as a right in international documents*. In *Human Dignity: The Constitutional Value and the Constitutional Right*, Cambridge, Cambridge University Press, 2015, pp. 34-48, doi:10.1017/CB09781316106327.005.

There is a need for the protection of human dignity both in times of peace and in times of war[2], and in any situation, including criminal trials.

For this reason, treaties and international documents began to speak explicitly of human dignity. This was an epochal transition.

This happened first with the Preamble of the Charter of the United Nations, signed on 26 June 1945, where faith in the word "dignity" was reaffirmed.

Afterwards, the Universal Declaration of Human Rights proclaimed by the United Nations General Assembly in Paris on 10 December 1948 explicitly mentioned human dignity in the preamble[3] as well as in some articles[4]. In particular, Article 1 provides that «All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood».

At the European Level, the Convention for the Protection of Fundamental Rights and Fundamental Freedoms (better known as the European Convention on Human Rights), which opened for signature in Rome on 4 November 1950 and came into force in 1953, did not mention human dignity. Nevertheless, this fundamental right is frequently recalled in judgements of the European Court of Human Rights (ECHR).

Instead, human dignity is claimed by the Charter of Fundamental Rights of the European Union (Charter), proclaimed on 7 December 2000. The Charter provides for the inviolability of this right. In particular, Article 1 states: «Human dignity is inviolable. It must be respected and protected».

Human dignity is a fundamental right. It gives substance to the rights laid down in the Charter. As early as 2001 the Court of Justice of the European Union (CJEU)[5] made

---

[2] I.C. Paşca, *Drept penal international*, Bucureşti, Universul Juridic, 2020, p. 116.

[3] The Preamble first specifies that the *"recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world, has evolved over the years"*. This Preamble also claims that *"the peoples of the United Nations have in the Charter reaffirmed their faith in fundamental human rights, in the dignity and worth of the human person and in the equal rights of men and women and have determined to promote social progress and better standards of life in larger freedom".*

[4] See Articles 1, 22, and 23.3. Article 22 provides that *"Everyone, as a member of society, has the right to social security and is entitled to realization, through national effort and international cooperation and in accordance with the organization and resources of each State, of the economic, social and cultural rights indispensable for his dignity and the free development of his personality".* Moreover, Article 23.3 provides that *"Everyone who works has the right to just and favourable remuneration ensuring for himself and his family an existence worthy of human dignity, and supplemented, if necessary, by other means of social protection".* The human dignity is also mentioned by: *UN Declaration on the Elimination of All Forms of Racial Discrimination* (20 November 1963), *International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights* (16 December 1966); *Final Act of the Helsinki Conference on Security and Cooperation in Europe* (1 August 1975); *Convention on the Elimination of All Forms of Discrimination against Women* (18 December 1979); *African Charter on Human and Peoples' Rights* (27 June 1981); *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment* (10 December 1984); *Convention on the Rights of the Child* (20 November 1989); Protocol No. 13 to *European Convention on Human Rights concerning the abolition of the death penalty in all circumstances* (3 May 2002); *International Convention for the Protection of All Persons from Enforced Disappearance* (20 December 2006); *Convention on the Rights of Persons with Disabilities* (13 December 2006); *Second Optional Protocol to the International Covenant on Civil and Political Rights on the abolition of the death penalty* (15 December 1989); *Optional Protocol to the Convention on the Elimination of All Forms of Discrimination against Women* (6 October 1999); *Council of Europe Convention on Action against Trafficking in Human Beings* (16 May 2005); *Optional Protocol to the Convention on the Rights of the Child on a communications procedure* (19 December 2011); *Optional Protocol to the International Covenant on Economic, Social and Cultural Rights* (10 December 2008).

[5] See CJEU, 9 October 2001, Netherlands vs. Parliament and Council, Case C-377/98, at grounds 70-77.

clear that the right of human dignity is part of Union law. However, the problem remained that the Charter did not have a binding force, being only a source of "soft law"[6].

The Treaty of Lisbon, which was signed on 13 December 2007 and came into force on 1 December 2009, provided that the Charter is a primary law of the Union, therefore assigning to the Charter the same legal status of the Treaties (6.1 TEU). Regarding this fact, Kostoris[7] highlighted: *"this is a crucial step that brought about significant consequences for the general framework of the multilevel protection of fundamental rights. Indeed, the Charter, enjoying now the status of primary EU law, is binding on both secondary EU law and Member States law. In addition, it must be stressed that the Charter not only has codified the fundamental rights that had been recognized exclusively by the case law of the Court of Justice but also includes a list of new rights, such as 'human dignity' (Art. 1 of the Charter)".*

Two consequences arise from the inviolability of human dignity: first of all, no right recognized by the Charter can prejudice the dignity of another person. Furthermore, human dignity cannot be balanced with other rights, because it must always be protected and cannot be limited by other rights.

II. The Kantian categorical imperative as the kernel of human dignity

Human dignity is a fundamental right that guides the interpretation of other rights. This is testified by judgments issued by many national and supranational judges, even if the meaning of dignity varies significantly from jurisdiction to jurisdiction[8].

Nevertheless, some examples can be mentioned.

The United States Supreme Court stated that *"the primary principle is that a punishment must not be so severe as to be degrading to the dignity of human beings"*[9].

The ECHR has established on several occasions that the detention regime must be such as to not violate human dignity[10]. Moreover, this Court ruled that human dignity and human freedom are the "very essence" of the Convention[11].

The CJEU also stated that human dignity imposes certain standards for the reception of applicants for international protection, in particular with regard to material conditions involving housing, food or clothing. The Court specified that a Member State cannot withdraw these standards even temporarily, not even in those cases where the person committed serious breaches of the rules of the accommodation centers or is characterized by seriously violent behavior[12].

These judgements are just a few examples involving the subject of human dignity, but they are more than enough to demonstrate how human dignity is a fundamental right underlying every other right. The fil rouge that connects these judgments seems to be the need to affirm that man can never be considered or treated as a thing.

---

[6] R.E. Kostoris, *The Protection of Fundamental Rights*. In Kostoris R.E. (Ed.) *Handbook of European Criminal Procedure,* Cham, Springer, 2018, p. 72.

[7] *Idem*, p. 73.

[8] C. McCrudden, *Human Dignity and Judicial Interpretation of Human Rights*, in *European Journal of International Law*, Volume 19, Issue 4, September 2008, pp. 655–724, https://doi.org/10.1093/ejil/chn043.

[9] Furman v. Georgia (1972), No. 69-5003.

[10] ECHR, Yaroslav Belousov v. Russia, No 2653/13 and 60980/14, 6 March 2017.

[11] ECHR, Christine Goodwin v. the The United Kingdom, No 28957/95, 11 July 2002.

[12] CJEU, Grand Chamber, 12 November 2019, Zubair Haqbin v. Federaal Agentschap voor de opvang van asielzoekers, Case C-233/18.

After all, any legal system should apply the Kantian categorical imperative, which states that "Handle so, daß du die Menschheit sowohl in deiner Person, als in der Person eines jeden andern jederzeit zugleich als Zweck, niemals bloß als Mittel brauchest" (Act in such a way that you treat humanity, whether in your own person or in the person of any other, never merely as a means to an end, but always at the same time as an end)[13].

III. Information technology and new challenges to human dignity: The case of judicial decision-making

The growing use of information technology (IT) poses new important challenges in terms of respect for fundamental rights and also for human dignity[14].

Technological development made possible the processing of a huge amount of personal data. However, there is the risk that the person is reified and considered a mere set of personal data to be marketed and exploited for the most varied purposes.

As a consequence, the protection of natural persons in relation to the processing of personal data is a fundamental right strictly connected to human dignity.

From a technological point of view, the processing of personal data is based on specific algorithms. In general, an algorithm is a set of instructions for carrying out a procedure or for solving a problem in a finite number of steps[15]. It is important to underline that some artificial intelligence (AI) techniques, in particular *Deep learning,* which is currently undergoing great development, require that the machine learn from data. Therefore, there are some elements of the algorithm actually used in the processing whose values have not been chosen by a programmer, but which are instead the result of automatic learning by the machine (machine learning)[16].

In the legal field, the use of AI algorithms poses significant problems[17]. For this reason, the European Commission for the efficiency of Justice (CEPEJ) tried to provide guidelines by adopting the European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment (Strasbourg, 3-4 December 2018).

AI applied to criminal proceedings and criminal procedures is already a reality in the most diverse fields. For example, there are algorithms that perform profiling of potential offenders or predict where a crime is likely to be committed. From this point of view, it has been noted that the use of algorithms can lead to an increase in proactive investigations[18].

---

[13] I. Kant, *Critik der practischen Vernunft,* 1788, AA IV, 429.

[14] See Z. Bauman, and D. Lyon, *Liquid surveillance: A conversation*. Melden: Polity Press, 2013, VIII – 152, and S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,* New York: PublicAffairs, 2019, pp. 1-691.

[15] See e.g. https://www.merriam-webster.com/dictionary/algorithm.

[16] See M. Kubat, *An introduction to machine learning*, Switzerland, Springer, 2017, pp. 1-339.

[17] See J. Nieva Fenoll, *Inteligencia artificial y proceso judicial*, Madrid, Marcial Pons 2018, pp. 1-168; A. Garapon, J. Lassègue, *Justice digitale. Révolution graphique et rupture anthropologique*, Paris, Puf 2018, pp. 1-368; S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for A European Legal Discussion*, Cham Springer, 2020, pp. 1-247; and L.M. Stănilă, *Inteligența artificială și sistemul de justiție penală – Instrumentele de evaluare a riscului penal*, București, Universul Juridic, 2020, pp. 1- 336.

[18] A.G. Ferguson, Predictive Prosecution, *Wake Forest Law Review*, Symposium 2016, Volume 51, May 2016 pp. 705-744, available at SSRN: https://ssrn.com/abstract=2777611, K. Ligeti, Artificial Intelligence and Criminal Justice, *Concepts paper for XX AIDP-IAPL International Congress of Penal Law*, Rome, 13-16 November 2019, p. 9, available at: http://www.penal.org/sites/default/files/Concept%20Paper_AI%20and%20Criminal%20Justice_Ligeti.pdf.

Moreover, other algorithms evaluate the reliability of a witness in a criminal trial. The use of algorithms aimed at assessing potential recidivism risk is currently widespread[19].

There are also algorithms that allow lawyers to reasonably predict what the judgment will be.

The use of algorithms can go even further. A machine can come to serve as a judge by issuing judgments. Robot judges are, for example, being tested in Estonia where they operate only in matters other than Criminal matters and for cases of low value. However, they decide.

At the European level, the use of such algorithms is only apparently prohibited by Directive (EU) 2016/680 (directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data), as well as by Regulation (EU) 2016/679 (regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data; cd. General Data Protection Regulation – GDPR).

Regarding the criminal trial, Article 11 of Directive (EU) 2016/680 provides that *"Member States shall provide for a decision based solely on automated data processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited".* Therefore, any robotic decision would appear to be prohibited.

However, the same article establishes a relevant exception. In fact, it provides that the robotic decision is prohibited unless it is authorized by Union or Member State law to which the controller is the subject and which provides appropriate safeguards for the rights and freedoms of the data subject. In particular, at least the right to obtain human intervention on the part of the controller must be safeguarded in all cases.

However, it is necessary to ask ourselves what *"the right to obtain human intervention on the part of the controller"* consists of. The risk to be avoided is that the Judge becomes a mere ratifier of what the algorithm decides, on the basis of the alleged aura of infallibility that connotes IT.

In fact, IT is a human product and, therefore, it is fallible. Both programming and algorithm operating errors may occur. For example, recently two planes and more than 300 lives were lost due to a programming error which, combined with a sensor malfunction, caused the on-board computer to shut down the pilots' commands[20]. Furthermore, the learning process of a machine can lead to errors. It is important to underline that the goal of machine learning is not to obtain a machine that responds exactly in all cases, but a machine that responds correctly almost always based on reasonable requirements, taking into account the fact that a 100% accuracy rate is not achievable.

IV. The difficult relationship between the decision made by a machine and respect for human dignity

At the European level, both Directive (EU) 2016/680 and the GDPR allow exceptions to the prohibition of decision-making based solely on automated data processing,

[19] See e.g. Supreme Court of Wisconsin, State of Wisconsin v. Eric L. Loomis, Case No. 2015AP157-CR, 5 April – 13 July 2016.

[20] R.L. Sumwalt, J. Homendy, B. Landsberg, *Safety Recommendation Report 59582*, National Transportation Safety Bord, Washington, DC 2019, pp. 1-13.

including profiling. However, it is necessary to ask whether, in criminal matters, the exceptions to the prohibition of decision-making based solely on automated data processing are or are not compatible with respect for human dignity.

The problem to be faced is different from that of establishing whether an algorithm (or a set of algorithms) is capable of issuing a reliable judgment or not. This different problem, which was mentioned in § 3, is extremely important, but it is relevant from the point of view of the Right to a fair trial instead.

This question is faced here: Is human dignity violated or not by the fact that it is a machine and not a man who issues the judgement?

It is true that at the European level it is provided that "the right to obtain human intervention on the part of the controller" is respected. However, this does not solve the problem. This can be illustrated by means of an example. Suppose a person is undergoing inhuman or degrading treatment. There would be a clear violation of both the prohibition of torture and human dignity. If that person at a later stage is treated in full compliance of all the rules and rights, the previous violation of the prohibition of torture and of human dignity would not disappear.

Similarly, if the robotic decision involved a violation of human dignity, this violation would not be remedied by any subsequent human intervention.

It is therefore essential to understand whether, in criminal matters, a robotic decision causes a violation of human dignity or not. In my opinion the answer is affirmative.

A machine that issues a judgement on a person actually decides on the basis of current and past digital information. In essence, man is reduced to a set of data, that is, to a thing.

One could object to this reasoning saying that, even in an ordinary trial, the judge decides on the basis of a set of information. However, there is a difference. In the case of the robot judge, the person is reduced to information itself. In the case of the human judge, this is not the case. Even in the case of judgments in absentia, the person is something more than the information available to the judge.

If the robotic decision reduces man to a set of information, it follows that man is treated as a thing. Human dignity instead requires that man must always be considered and treated as a person and never as a thing. For this reason, the robotic decision violates human dignity.

Ultimately, human dignity seems to dictate that every man must be judged by another man. A machine could possibly assist a judge, a prosecutor or an investigator and could pick up on elements that would be difficult for a man to detect, especially in the case where a large amount of data needs to be processed, but any decision in a criminal trial must be made only by a man or a panel of men.

V. Conclusions

Human dignity is inviolable. Its kernel meaning dictates that man can never be reified. A robotic decision, on the other hand, reduces humans to a mere set of data and, therefore, to one thing. For this reason, such a type of decision seems to conflict with human dignity.

It follows that it is possible to doubt the legitimacy of Article 11 of Directive (EU) 2016/680, in the part in which it provides that the robotic decision can be authorized by Union or Member State law.

It is also possible to dispel the unfounded myth of the perfection of algorithms. An algorithm is not perfect, nor can it be. Furthermore, the algorithm does not consider the uniqueness of every human being but brings every man back into standard types. It would be interesting to wonder what the algorithm would decide if a person not attributable to typified categories, such as Beethoven, Einstein, Michelangelo, Leonardo da Vinci, were imputed.

It may also be mentioned that, as part of the update and enhancement of Israel's armored forces, a new tank is planned in which the two crew members are joined by an additional virtual member. This virtual member integrates all current and previous information provided by sensors and maps, as well as historical information that may not be available to the human crew, analyses the situation and, using AI techniques, shows to the crew possible solutions to the tactical problem. The decision to engage the target is only up to the human crew, i.e. the system is of the "man in the loop" type[21]. Anyway, AI in warfare, if not tempered by a "man in the loop" system, is believed to violate several principles, including the principle of human dignity[22].

If the concept of "man in the loop" is so important in war, where the decision time can be very short, is it not possible that it is at least as important in criminal procedure, where the decision time is not as short? AI can be useful to help the Judge reach a decision[23], but the decision must be only up to one or more human beings.

In conclusion, it seems necessary to recognize a new right: the right to non-automated judicial decision-making[24].

References

1. Barak, A., *Human dignity as a value and as a right in international documents,* in *Human Dignity: The Constitutional Value and the Constitutional Right,* Cambridge: Cambridge University Press, 2015, pp. 34-48, doi:10.1017/CB09781316106327.005.

2. Bauman, Z., Lyon D, *Liquid surveillance: A conversation*. Melden: Polity Press, 2013 VIII – 152.

3. Eshel, T., *Israel's Carmel Programme. Charting Future Concepts for Mounted Combat*, European Security & Defense, Volume 2020, Issue 1, February 2020, pp. 90-92.

4. European Commission for the efficiency of Justice (CEPEJ) *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*. Strasbourg, 3-4 December 2018.

5. European Parliament, *The ethics of artificial intelligence: Issues and initiatives*. Brussels: European Union, 2020, p. 64, doi: 10.2861/6644.

6. Ferguson, A.G., Predictive Prosecution. *Wake Forest Law Review, Symposium 2016*, Volume 51, May 2016, pp. 705-744, Available at SSRN: https://ssrn.com/abstract=2777611.

[21] T. Eshel, *Israel's Carmel Programme. Charting Future Concepts for Mounted Combat*, European Security & Defense, Volume February 2020, Issue 1, pp. 90-92.

[22] European Parliament, *The ethics of artificial intelligence: Issues and initiatives*, Brussels, European Union 2020, p. 64, doi: 10.2861/6644.

[23] The case of Beijing Internet Court is particularly interesting. Founded on 9 September 2018, Beijing Internet Court mainly deals with the first-instance of specific types of Internet cases within the jurisdiction of Beijing. The use of algorithms is aimed at giving support to the judge in relation only to the formal and procedural aspects. Consequently, the purpose of robots is not to replace humans or to arrive at algorithmic decisions, but to help the judge.

[24] S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, Giappichelli, 2018 pp. 99-103.

7. Garapon, A. - Lassègue, J. *Justice digitale. Révolution graphique et rupture anthropologique*. Paris: Puf, 2018, pp.1-368.

8. Kant, I., *Critik der practischen Vernunft*, 1788, AA IV, 429.

9. Kostoris, R.E., *The Protection of Fundamental Rights*, in Kostoris R.E. (Ed.) *Handbook of European Criminal Procedure.* Cham: Springer, 2018, pp. 72-73.

10. Kubat, M., *An introduction to machine learning*. Switzerland: Springer, 2017, pp. 1-339.

11. Ligeti, K., *Artificial Intelligence and Criminal Justice*, *Concepts paper for XX AIDP-IAPL International Congress of Penal Law,* Rome, 13-16 November 2019*,* p. 9. Available at: http://www.penal.org/sites/default/files/Concept%20Paper_AI%20and%20Criminal%20Justice_Ligeti.pdf.

12. McCrudden, C., *Human Dignity and Judicial Interpretation of Human Rights*, European Journal of International Law, Volume 19, Issue 4, September 2008, pp. 655–724, https://doi.org/10.1093/ejil/chn043.

13. Nieva Fenoll, J., *Inteligencia artificial y proceso judicial*. Madrid: Marcial Pons, 2018, pp. 1-168.

14. Paşca, I.C., *Drept penal international.* Bucureşti: Universul Juridic, 2020, p. 116.

15. Quattrocolo, S., *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for A European Legal Discussion,* Cham: Springer, 2020, pp. 1-247.

16. Signorato, S., *Le indagini digitali. Profili strutturali di una metamorfosi investigative*, Torino: Giappichelli, 2018, pp. 99-103.

17. Stănilă L.M., *Inteligența artificială și sistemul de justiție penală – Instrumentele de evaluare a riscului penal.* București: Universul Juridic, 2020, pp. 1- 336.

18. Sumwalt R.L., Homendy J., Landsberg B., *Safety Recommendation Report 59582, National Transportation Safety Board*. Washington, DC, 2019, pp. 1-13.

19. Zuboff, S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,* New York: PublicAffairs, 2019, pp. 1-691.

New Species of Criminal Phenomena: Organized Cybercrime

Laura Stanila*

Abstract

ICT (Information and Communication Technology) has spread to all dimensions of social life, including criminal phenomenon. Organized crime, as a rising type of crime, has gained new forms of manifestation since the members of criminal groups use ICT tools to commit crimes or moved to virtual space as this space offers them the ideal "work-field" providing anonymity, a large number of victims, and huge sources of profit.

In fact, the organized cybercriminal groups have become one of the most ascending criminal groups, very difficult to discover and combat.

In the present study, the author offers a presentation of cybercrime in its organized form, presents the cybercriminal groups, their types and characteristics and the types of cybercrimes that are to be committed by an organized criminal group online and offline.

Keywords: *cybercrime, organized crime, organized criminal group, organized cybercrime, cybercriminal group*

I. The Newest Challenge for the Criminal Investigators. Social context

In the recent years everyone may notice an increasing addiction of the society to technology, especially to ICT (Information and Communication Technology). This addiction turned dramatic as it has extended in the "criminal" area with criminals becoming specialized in committing online crimes and in using AI (artificial intelligence) as an important tool to achieve illegal goals. Organized crime was itself a devastating plague of the contemporary society, very difficult to discover, investigate and combat, but the new social realities seem to make it even more dangerous and even more difficult to fight with. Digital networks seem the perfect playground for criminals taking advantage of their features and advantages: privacy, secrecy, velocity, the possibility for dissimulation. Due to these features, the criminal goal is easier to achieve, while *modus operandi* is changed and adapted to the digitalization of the society. The result of this tendency is a sad one: a new type of organized crime – organized cybercrime.

As general Director of the FBI had stated *"transnational crime groups, sexual predators, fraudsters, and terrorists are all transforming the way they do business as technology evolves. Huge swaths of these crimes have a digital component or occur almost entirely online. And new technical trends are making the investigative environment a lot more complex"*[1].

* PhD, Associate Professor, West University of Timişoara (Romania). Contact: laura.stanila@e-uvt.ro.

[1] C. Wray, Director of Federal Bureau of Investigation (FBI), *Digital Transformation: Using Innovation to Combat the Cyber Threat*, Speech at the Boston College/FBI – Boston Conference on Cyber Security, March 7, 2018, https://www.fbi.gov/news/speeches/digital-transformation-using-innovation-to-combat-the-cyber-threat, accessed on 2.11.2020.

II. What is cybercrime? What is organized cybercrime? Distinctions

Cybercrime has evolved in parallel with society's use of digital networks, reacting to every development in legal sector with new approaches to committing offenses[2]. Scholars have noticed that, in the past decade, cybercrime has transformed itself from fragmented acts committed by individuals to increasingly sophisticated and highly professionalized activity[3].

It is obvious we are facing a new type of organized criminal groups operating solely in the cyberspace, tending to expand their activity at a global level.

From the very beginning one should notice that nowadays several terms and expressions are used in relation with the notion of crime in cyberspace and the notion of organization of crime. For example, would it be accurate to refer to organized cybercrime as organized crime in cyberspace? Or do these notions differ?

The answer key to this question is the cyberspace.

a) If we consider cyberspace as a medium for "traditional organized crime", a space where organized crime carries out its activity, then organized cybercrime is in fact a subdivision, a special type of organized crime.

In this case, the structure, purpose and operations of organized crime are the same in the case of organized cybercrime, while the area of carrying out criminal operations, the IT specializations of the members of the organized criminal group and a specific modus operandi implying specific techniques and methods (e.g. phishing, botnet trade) are features characterizing organized crime in cyberspace.

b) If we consider cyberspace as an enabler for organized crime, then organized cybercrime becomes a new distinct type of crime, which shares few features with traditional organized crime.

The debate on this distinction is not new. Actually, in the early 2000s, there were scholars affirming organized crime and cybercrime could not be one and the same because organized crime would be operated offline while most cybercrimes would be committed by individuals rather than organized groups[4]. Williams even identified five possible trends in the evolution of organized crime in the era of digitalization:

1. the use of the Internet for major fraud and theft activities by the organized crime groups;

2. the increased opportunities for profit stemming from the growth of electronic banking and electronic commerce for organized crime.

3.the growth of cyberextortion using complex extortion schemes, conducted anonymously and incurring modest risks, very efficient in money outputs.

4. the use of "nuisance tools", such as computer viruses, for more openly criminal activities.

5. jurisdictional arbitrage – cybercrimes will be committed by organized criminal groups in jurisdictions with poor legal framework and little capacity to enforce laws against cybercrime.

---

[2] T. Tropina, *The evolving structure of online criminality. How cybercrime is getting organized*, Eucrim, The European Criminal Law Associations' Forum, issue 4/2012, p. 158.

[3] *Idem*.

[4] P. Williams, *Organized Crime and Cybercrime: Synergies, Trends, and Responses*, Global Issues, Volume: 6, Issue: 2, August 2001, pp. 22-26, https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=191389, accessed on 2.11.2020.

6. the increased use of the Internet for money laundering, as being a medium through which international trade takes place. Online auctions and online gambling offer similar opportunities to launder money through apparently legitimate purchases, and then lose the "clean" money through offshore financial centers. In addition, *"as e-money and electronic banking become more widespread, the opportunities to conceal the movement of the proceeds of crime in an increasing pool of illegal transactions are also likely to grow"*[5].

7. growing network connections between hackers or small-time criminals and organized crime. Network connections between the two kinds of groups are likely to deepen and widen.

Referring to all trends, it is worth to mention organized crime groups use the Internet for communications (usually encrypted) and for other purposes. Organized crime is proving as flexible and adaptable in its exploitation of cyber-opportunities as it is in any other opportunities for illegal activity.

These thoughts were expressed 18 years before and they appear accurate in the contemporary context.

In 2017 a study was conducted to investigate to what extent cybercriminals operating in phishing and malware attacks can be conceptualized as organized criminal groups. To answer this question, the authors analyzed 40 criminal networks investigated in four countries (Netherlands, UK, USA and Germany) and analyzed them through an organized crime analytical framework. The empirical analysis indicates that even if the criminal networks considered display the minimum set of characteristics to consider them as organized crime, if someone looks only at their structure and composition, they mostly fail to meet the existing definitions of organized crime when it comes to the characteristics of criminal activities carried out and social functions of these networks[6].

As a result of the study, the authors identified 39 networks and classified them into four types:

1. Completely through offline social contacts;
2. Offline social contacts as a base and online forums to recruit specialists;
3. Online forums as a base and offline social contacts to recruit local criminals;
4. Completely through online forums.

The analysis revealed specific features of traditional organized crime, such as use of Violence and Corruption and connections with the Legal Economy. Still, it was very difficult to declare cybercriminals operating in phishing and malware attacks, which were indeed acting in networks, as organized criminal groups.

Tropina distinguishes between two different phenomena, namely, migration of traditional organized crime in cyberspace and organized groups focused on committing cybercrimes[7]:

a) migration of traditional organized crime in cyberspace

The Internet has become a tool for facilitating all types of offline organized criminality (child abuse, drug trafficking, trafficking in human beings for sexual exploitation, illegal migration, different types of fraud, and counterfeiting) due to increased anonymity, money laundering schemes and possibilities of advertising.

---

[5] *Idem*.

[6] E.R. Leukfeldt, A. Lavorgna, E.R. Kleemans, *Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime, European Journal of Criminal Policy Res* 23, 2017, pp. 287–300, https://doi.org/10.1007/s10610-016-9332-z, accessed on 2.11.2020.

[7] T. Tropina, *cited,* p. 159.