2

The boundaries of legality in criminal prosecution against hacking in the information society

GREICE PATRÍCIA FULLER

Pós-Doutorado em Direito pela *Universidad de Navarra* (Espanha). Doutora e Mestra em Direito (PUC-SP). Professora do Programa de Mestrado em Direito da Sociedade da Informação da (FMU) e curso de Direito da (PUC-SP). Professora convidada da *Universidad de Navarra* (Espanha).

Artigo recebido em 9/5/2022 e aprovado em 15/12/2022.

CONTENTS:

ABSTRACT: The article analyzes the possibility of using legally authorized computer equipment for the purpose of criminal investigation into digital crimes. In order to fulfill this desideratum, an analytical approximation between Law and Art is made, aiming at the realization of the digression regarding possible dehacking instruments concerning domestic and foreign laws in the face of intimacy and privacy rights. The article adopts the legal-constitutional and criminal procedural methodological aspect that seeks to examine law not only as a phenomenon linked to the adjacent social reality, but as a science that must be dynamic in the context of new technological paradigms. The article was developed using the deductive method, with research based on bibliographic review, carried out under the reflective-critical view. It concludes on the subsumption of legalized surveillance to the model of criminal prosecution in face of information society.

KEYWORDS: Hacking • Legality • Criminal investigation • Information society

Las fronteras de la legalidad en la persecución penal ante el *hacking* en la sociedad de la información

CONTENIDO: *1 Introducción • 2 Las tecnologías de información y de comunicación: la realidad de un mundo ideado por George Orwell • 3 El hacking y su legalidad en la investigación criminal, en la sociedad de la información • 4 Conclusiones • 5 Referencias.*

RESUMEN: Este artículo analiza la posibilidad de utilizar equipos informáticos legalmente autorizados para la investigación penal de delitos digitales. Para ello, se realiza una aproximación analítica entre el Derecho y el Arte, con el fin de hacer una digresión sobre los posibles instrumentos de *hacking* ante la legislación brasileña y extranjera en materia de derechos de privacidad e intimidad. Se adopta la vertiente metodológica jurídico-constitucional y procesal, incluso comparada, que busca examinar el derecho no solamente como fenómeno de conexión a la realidad social adyacente, sino también como ciencia que debe ser dinámica ante los nuevos paradigmas tecnológicos. El trabajo se desarrolla utilizando el método deductivo con una búsqueda basada en la revisión bibliográfica realizada a través del criterio reflexivo-crítico. Se concluye la subsunción de la vigilancia legalizada al modelo de persecución penal frente a la sociedad de la información.

PALABRAS CLAVE: *Hacking* • Legalidad • Investigación penal • Sociedad de la información

As fronteiras da legalidade na persecução penal frente ao *hacking* na sociedade da informação

RESUMO: O artigo examina a possibilidade do uso de equipamentos informáticos legalmente autorizados para o fim de investigação criminal em delitos digitais. Para o cumprimento deste desiderato, faz-se uma aproximação analítica entre o Direito e a Arte, objetivando a digressão a respeito de possíveis instrumentos de *hacking* em face da legislação pátria e estrangeira, ante os direitos de privacidade e de intimidade. Adota a vertente metodológica jurídico-constitucional e processual penal que procura examinar o direito não apenas como fenômeno ligado à realidade social adjacente, mas como ciência que deve ser dinâmica ante os novos paradigmas tecnológicos. O trabalho é desenvolvido utilizando o método dedutivo, com uma pesquisa baseada em revisão bibliográfica realizada sob o crivo reflexivo-crítico. Conclui-se que a vigilância legalizada se subordina ao modelo de persecução penal, em meio à sociedade da informação.

PALAVRAS-CHAVE: *Hacking* • Legalidade • Investigação criminal • Sociedade da informação

http://dx.doi.org/10.20499/2236-3645.RJP2023v25e135-2830

1 Introduction

In order to study the theme, criminal prosecution in face of information society and digital crime must be analyzed, faced and questioned, taking as paradigmatic front the constitutional normativity in face of fundamental rights.

The present study initially analyzes the new information and communication technologies, establishing a comparative sequence between Criminal Procedural Law and Art, according to George Orwell's vision, bringing to light its intersection with aspects related to surveillance in face of the XXI century. Subsequently, the possibility of hacking within the limits of legality in relation to digital crimes is analyzed, based on the rights to privacy and intimacy and comparing its use in Brazil and Spain.

The development of this work uses a methodology consistent with the analytical technique, in which the systemic-constitutional aspects of the legal norms are evaluated, added to the dialectic and multidisciplinary approach.

2 Information and communication technologies: reality of a world thought of by George Orwell

Information and communication technologies have become part of post-industrial revolution's history, giving rise to the technological revolution that occurred in the mid-1990s and consequently to the so-called Information Society, whose defining feature is the capture and dissemination of information across borders, in real time, based on cost reduction and information elevated as a commodity and an element that generates the circulation of wealth.

According to Castells (2016, p. 214) "the so-called Information Society provides a new step in the relations between nations, influencing political and economic systems and the very sovereignty of each people".

Note that information exists to generate knowledge, but as Castells (2016, p. 88) emphasizes, this is what characterizes the era of technological revolution:

> [...] is not the centrality of knowledge and information, but the application of that knowledge and information to the generation of knowledge and information processing/communication devices, in a cumulative feedback loop between innovation and its use. An illustration can clarify this analysis. The uses of new telecommunications technologies in the past two decades have gone through three distinct stages: the automation of tasks, the experimentation of uses, and the reconfiguration of applications [...]

It is convenient, at this point, to differentiate the knowledge society from the information society, establishing that the information society can be considered as a previous stage to the knowledge society, the latter being a "social stage in which man would dominate more intensively the biological, informatic, neurotechnological and GNO (the neural sciences) fields" (BERNAL-MEZA *et al.*, 2007, p. 25).

Therefore, and in any case, it is easy to verify the universalization of technologies being used in diverse areas such as work, education, social and interpersonal relations, and in various parts of the world. New expressions have appeared in worldwide vocabulary (such as WhatsApp, e-mails, twitter, SMS, chat, blogs, megas, mp3, Facebook, Instagram, digital signature, big data, among others), as well as new customs that have been interchanged by the use of technological instruments (messages through computers, cell phones or social networks).

By taking into account such phenomenon, an incessant concern has arisen with regard to the ethical, legitimate and legal limits of the use of information through new technologies. This is especially true regarding new criminal modalities called digital crimes or computer crimes, which differ from traditional criminality in the face of a new modus operandi, affecting legal goods of constitutional nature, generally practiced through various active subjects. In the digital era context, one can notice the generation of new technological tools for criminal investigation and criminal procedure, aiming to obtain evidence in digital or traditional crimes.

In respect to the issue of new digital means for criminal prosecution and in

relation to traditional criminality, one can cite as examples of what was exposed the lessons of González-Cuéllar Serrano (2006, p. 889). He cites the hypotheses of a violent young man who does a video-recording, in his cell phone, of the beating he inflicts on a beggar; or the drug dealer who writes down the details of the transactions in an electronic document on his computer. In both cases, they end up creating digital data and evidence that inform the criminal fact.

Criminal investigation of digital crimes present certain characteristics of its own, due to the means by which they are committed (i.e.: the Internet), thus requiring the use of technological investigative tools. In many cases, they are considered, crimes at a distance, transposing their results transnationally and quickly (BRENNER, 2007, p. 379), which makes it difficult to determine the place where the conduct was committed, as well as its authorship.

In view of the above characteristics held by digital crimes, international organizations (GERCKE, 2012, p. 74) have taken the initiative to use international

http://dx.doi.org/10.20499/2236-3645.RJP2023v25e135-2830

cooperation instruments in the fight against investigation, in addition to international treaties and agreements, recommendations, resolutions, good practice measures, etc.)

The book entitled "1984" (ORWELL, 2009), written by Eric Blair, bearer of the pseudonym George Orwell, and published in 1949, was considered emblematic among the publications of the 20th century, for its narrative translated (in a premonitory way) a new reality battered by the totalitarian system, which maintained control of the population through continuous surveillance by technological instruments created for this purpose. The book presents a society whose informational flow is represented through the so-called *teletela,* radio and billboards, controlled and monitored by the government and directed to the *Big Brother*.

The narrative takes place in a state called Oceania, ruled by a party whose leader was called *Big Brother*, portrayed by an abstract entity that informed the population that he would watch over them, and whose mottos were: "War is peace; freedom is slavery, and ignorance is strength" (ORWELL, 2009). The scenario presented the total control of the State over people's lives, through the telescreens, which were uninterruptedly on, with the purpose of capturing the acts performed in people's privacy.

Among several aspects that can be analyzed in relation to the aforementioned film, such as the issue concerning the repression of emotions, family ties, and the extermination of the feeling of solidarity, in the present work we will observe the issue concerning the breach of privacy in face of the technological advance - that allows broad and unlimited monitoring of each individual in the described society. The fact is that due to the criminality that occurs in the middle of the 21st century and in an attempt to search for security, cameras are placed at entrances of buildings, public establishments, elevators, streets. Meanwhile, information regarding personal identity taken from social networks is stored in the buildings' lobby.

Data on income and consumption habits are controlled by official bodies' computers and by the informational network that manages the Big Data phenomenon, that is, companies called Data Brokers. These capture, organize and commodify information from data (EL PAÍS, 2017). The Big Data refers to "the technology capable of statistically processing and analyzing any type and volume of data - structured or not- such as texts, audios, videos, clicks, logs, images and others" (CUKIER *et al.*, 2012)

George Orwell engages the reader to inquire about the legitimate justification for the constant surveillance of citizens, using the inclusive utilitarian ethics propounded by Jeremy Bentham, especially in his 1780 work *Le Pyearptique*. The pyearpticon (WHITAKER, 1999, p. 46) was a type of prison architecture designed in the late 18th century, whose goal was to allow the jailer to observe all prisoners in individual cells, without them knowing they were being observed. Thus, the central idea was to give more power to the one who sees than to those who are seen (GARCIA-ALGARRA, 2002).

The modern pyearpticon is characterized by the new surveillance mechanisms of programmed conduct self-enforcement such as video cameras, *web*, facial recognition programs, proximity sensors, motion detectors, infrared cameras, drones, video sequencers, among other technological instruments. Besides this, data is constantly crossed through new technologies, presenting the potential framework of non-observance of the limits of the rights to privacy and intimacy, materializing George Orwell's futuristic society that observes us and synthesizes in moments the history of our daily steps.

In any case, despite the fact that in the 21st century we have reached the phenomenon of globalization and the so-called *post-modern* society, we certainly live in a cyclical movement of imitating the surveillance kept and imposed in George Orwell's plot. Thus, post-modernity is being forged from the transformation of values, customs, social habits, institutions, achievements, and also social changes - that is the transition (BITTAR, 2005).

Therefore, in this context, it is clear that the role of law is to impose limits based on axiological and constitutional aspects that justify the use of *hacking* in criminal prosecution, in order to avoid legally insecure procedural environments, based on personal, arbitrary aspects, full of common-sense elements and extra-official law.

3 *Hacking* and its legality in criminal investigation in information society

3.1 Rights to privacy and intimacy in the face of computer use

The Universal Declaration of Human Rights approved in 1948 established in its art. XII that: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor or reputation. Everyone has the right to the protection of the law against such interference and attacks"(UNICEF, 1948).

http://dx.doi.org/10.20499/2236-3645.RJP2023v25e135-2830

The inherent theme of privacy is also highlighted in art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (COUNCIL OF EUROPE, 2021); in the International Covenant on Civil and Political Rights (UNITED NATIONS, 1976) in its art. 17, § 1º and § 2º; and in art. 11 of the American Convention on Human Rights -Pact of San Jose da Costa Rica (ORGANIZATION OF AMERICAN STATES -OAS).

Regarding the constitutional level, it is observed that the right to privacy is foreseen in a generic way in Portugal, Hungary, Russia and Slovenia. Meanwhile, article 18 of the Spanish Constitution (CONSTITUCIÓN ESPAÑOLA, 1978) has broadened the meaning of the right to privacy, by guaranteeing the right to intimacy, private life, privacy of the home, privacy of communications; and by establishing limits on the use of computer means in order to protect the intimacy of others.

In Brazil, the regulation of the rights to privacy and intimacy is based on Article 5º, item X of the Federal Constitution (BRASIL, 1988), which prescribes that privacy, private life, honor, and image are inviolable, and that the right to compensation for material or moral damage resulting from their violation is assured.

The issue inherent to the sphere of private life was developed by the German doctrine of Heinrich Hubmann (1953) through the creation of the *theory of concentric circles,* establishing divisions in three circles defined in face of the degrees of their densities. These degrees are composed of a larger sphere that refers to privacy, a second one that concerns secrecy, and the central and nuclear one that manifests itself through intimacy. In 1957, based on the *theory of concentric circles of the sphere of private life* (COSTA JUNIOR, 1995, p. 36) also called *theory of the spheres of personality* (SAMPAIO, 1998, p.54) or *theory of three degrees* (SOUZA, 1995, p. 366), Heinrich Henkel defined that the right to private life may be analyzed under the viewpoint of three circles that aggregate (i.e.: add up in layers). However, he states that the core should be represented by secrecy, while intimacy is presented in the second circle (DI FIORE, 2012).

Within the perspective of concentric circles, there is a differentiated level of protection. Initially, in the first circle, representative of private life (privacy in the strict sense), there are the most superficial interpersonal relationships, which generally possess certain degree of restriction on public knowledge that, for reasons of public interest, may be mitigated (COSTA JUNIOR, 1995, p. 34).

Under the viewpoint of the three circles, the one located in the intermediate zone is intimacy, which has as its fundamental characteristic a set of information of greater restriction to the public, which could possibly be shared among friends and family.

Finally, the core can be characterized as a secret, carrying information that belongs only to the person involved. There is a low probability of sharing it (COSTA JUNIOR, 1995, p. 34).

Both privacy and intimacy in the context of information society are called informational privacy or informational self-determination[1], whose basic theme of study refers to the protection of information about a certain person (natural or legal), with respect to his or her most intimate sphere, but especially about those relating to personal data that can lead to the identification of a certain holder.

In this context, it is imperative to distinguish between private life and intimacy, and for this it is worth considering Sidney Guerra (2004, p. 55) lessons on the subject:

> Thus, for better clarification, it is verified that intimacy is something more than private life, that is, intimacy is characterized by that space, considered by the person as impenetrable, insurmountable, impassable and that, therefore, concerns only and exclusively the person, such as, for example, personal memories, diaries, etc. This space would be of such importance that the person would not want to share it with anyone. These are the secrets, the particularities, the expectations, in short, it would be what we will call the "sacred corner" that each person has. Private life, on the other hand, consists of those particularities that concern, for example, the family, problems involving close relatives, physical and mental health, etc. It would then be that intimate sphere of each person, forbidden to the intrusion of others.

Besides the concepts mentioned above, Marcelo Pereira (2004, p. 140) verifies that the "right to privacy would be (...) the power of people to control their personal information, which, even if it is not part of their private life, may reveal aspects of their personality".

Having made the above considerations about the rights to privacy and intimacy, we must now examine the ethical and legitimate limits of monitoring and surveillance in the information society and to that end the question of the possibility of legal *hacking* in the face of criminal investigation.

1 It should be noted that the concept of informational self-determination was thus recognized in a decision of the German Constitutional Court of 1983 (Bverge 65,1 - Volkszählungsurteil) which declared null and void the provisions relating to the comparison and transmission of data to public offices laid down in the Census Act of 1983. The decision recognised that this concept should be understood as the right of each individual to control and protect their own personal data.

3.2 Legal *hacking,* cybersecurity and surveillance legitimized by the information society phenomenon

Initially, it is important to state that the subject in question has a close connection with digital security (*Cyber Security or cybersecurity*), which aims to prevent and combat conducts carried out in the information society scenario.

The issue related to the theme started being concrete with the creation of NATO CCD COE (NORTH ATLANTIC TREATY ORGANIZATION COOPERATIVE CYBER DEFENSE CENTRE OF EXCELLENCE, 2018), constituted by an intergovernmental military alliance based on the North Atlantic Treaty, formed by 28 member states after the cyber-attack in Estonia. *Cyberdefense* in Brazil still needs to be created in a more structured way. Since 2012, the country has the Cyber Defense Center, which is an organ of the national army. Regarding national *cybersecurity,* although a Public Cyber Security Agency does not exist, it is verified that the legal framework for its creation already exists: art. 91 of the Federal Constitution of Brasil (BRASIL, 1988).

It should be noted that legal *hacking* and, therefore, measures inherent to state surveillance for the purpose of promoting public safety should be analyzed, especially in light of the fulfillment of constitutional precepts and especially against crimes such as *cyberterrorism*, drugs trafficking, attacks on public websites, pertaining to banks and hospitals, for example. According to digital sociologist Pete Fussey (2016, p. 31), a study on the production of theories about the human being in digital security discourses and practices must be carried out to identify that there is a need for training and experience of those who use digital tools (e.g.: radio frequency identification ticket, drones, digital magazine, among others), besides the need for technological monitoring.

As previously discussed in this article, on one hand, there is the undeniable anguish for the guarantee of rights that cannot return to the *status quo* after violation - such as intimacy, privacy, honor and image. On the other hand, there is a flaming agony for searching the cessation of conducts related to diffuse criminality (e.g.: cybercrime), which would result in the rescue of public security.

However, this generation undeniably engenders an absolutely ambivalent relationship in many cases, as Zygmunt Bauman (2013, p. 73) writes:

http://dx.doi.org/10.20499/2236-3645.RJP2023v25e135-2830

> This is the paradox of our world saturated with surveillance devices, whatever their purported purposes: on the one hand we are more protected from insecurity than any previous generation; on the other hand, however, no previous, pre-electronic generation experienced feelings of insecurity as an everyday (and every night) experience.

Therefore, the theme is rooted in the question of the binomial right to privacy versus the right to public security - as a diffuse right with constitutional stature. Does surveillance give way to freedom, which becomes the legitimating instrument of security and of the search for real truth in criminal proceedings? Are there conditioning or limiting elements for this question?

Today, the network society lives in relationships with quantitatively exponential ties that are sources of information and generate surveillance in personal relationships and conduct, even before that established by the State, as Foucault predicted:

> Foucault highlights with a new type of power, which he calls 'disciplinary power', that unfolds throughout the nineteenth century, reaching its maximum development at the beginning of the present century. Disciplinary power is concerned firstly with the regulation, surveillance and government of the human species, or of whole populations, and secondly with the individual and the body. Its sites are those new institutions that developed over the course of the nineteenth century and that 'police' and discipline modern populations [...]. (HALL, 2011, p. 43).

When analyzing digital public security and consequently the possibility of legal hacking, one must observe the constitutional limits of the established guarantees and the limits of police power, in the exact terms of legality. Thus, the *hacking* used by state prosecution agencies must strictly comply with the constitutional and infra-constitutional dictates alluded to in the Brazilian legal system, under penalty of becoming an instrument of arbitrariness and offense against the democratic rule of law.

Therefore, the digital criminal prosecution must pay attention to the fundamental triduum based on the validity and constitutionality of the evidence; on the constitutional principles and rights, notably, the principle of human dignity and public security.

In the search for evidence and the real truth, the law operator cannot be equal to the violator of the criminal rule, and if there is an urgent need for the State to protect security (a right of all citizens), this is so because of the principle of human dignity: Article 1, item III of the Federal Constitution (BRASIL, 1988) (that raises man to an end and not a means- under the kantian viewpoint.

3.3 Legal *hacking* in Brazil and Spain: specific considerations on casuistry

Currently, digital evidence is being used in criminal prosecution and can be defined as "all information with evidential value stored or transmitted digitally" or information of probative value stored or transmitted in digital form (original). It is a definition given by the Scientific Working Group on Electronic Evidence (SWGDE - Scientific Working Group on Digital Evidence) created in collaboration with the International Organization of Computer Evidence (IOCE) and FBI - in charge of drafting cross-sectional guidelines, best practices and standards for the recovery, preservation and study of digital evidence (SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE, 2018). The evidence used in this way is essential to the investigation of cybercrime, which is practiced precisely in the digital environment and with the use of technological instruments.

When talking about digital evidence, until now, some obstacles could not be overcome, such as the need for specific knowledge required from those who have the expertise to analyze it; the imperative creation of standards, practices and protocols that guarantee the integrity of the digital data obtained; the rapid technological innovation and the necessary infrastructure to perform digital forensics.

In all cases, today we have intelligence services and electronic instruments capable of intercepting and recording in real time the traffic or data location used as a means of gathering evidence in electronic criminal investigations, especially in digital crimes.

In respect to cell phones' electronic surveillance, several issues are being discussed, such as the access to personal data directly by the police, either through monitoring via *chip* implantation (cloning of the phone number) or by listening to the phone traffic, through the installation of software that downloads files related to the functions of the investigated cell phone, for example.

The cell phone is no longer just a device for telephone conversations. It is a true computer with multiple functions, highlighted by its various applications (social networks, sending e-mails, text messages, videos, voicemail, photography, work and banking records, history of itineraries, as well as use of browsers to search for specific sites, etc.), embodying the profile and personal identity of its user.

http://dx.doi.org/10.20499/2236-3645.RJP2023v25e135-2830

Therefore, it is easy to see that the cell phone carries information and digital traces inherent to the rights to intimacy, privacy, image, freedom of expression, among others considered of constitutional stature.

In this sense, Greice Patricia Fuller (2017) points out that the new information technologies, such as those of the modern mobile phone, have initiated a change of structural nature in social organization, especially with regard to work, administration, leisure, economics and interpersonal relations, characterizing the so-called information society.

In Brazil, a normative gap is perceived concerning police agents' access of personal data. The issue faces the analysis of legal goods and constitutional principles such as privacy, intimacy, public security, prohibition of evidence obtained by unlawful means, real truth, due legal process and the right to no self-incrimination (as a corollary of the ample defense principle).

Regarding telephone interception, Law n. 9296/96 (BRASIL, 1996) is advocated, although it does not cover the hypothesis of police agents' access to personal data from cell phones. Nor did Law n. 13.709/2018 (BRASIL, 2018) (which regulated the right to the protection of personal data in Brazil) establish specific regulations on the subject.

Undeniably, there are conflicting jurisprudential positions about this subject. The Federal Supreme Court in HC 91.867/PA (SUPREMO TRIBUNAL FEDERAL, 2012), whose rapporteur is Minister Gilmar Mendes, understood that one must not confuse the concepts of telephone communication and mere telephone records, thus the possibility of access to personal data is a lawful practice, without any constitutional obstacle, according to art. 5, item XII. Meanwhile, the Superior Court of Justice in RHC /RO 51.531 (SUPERIOR TRIBUNAL DE JUSTIÇA, 2016), reported by Minister Nefi Cordeiro, advocated that the direct access by police agents to data such as programs, Whatsapp and telephone data (agendas) characterize illicit evidence for requiring a previous judicial order and constitute unauthorized interception of communications.

Regarding the Spanish legislation, the police's obtention of personal data has been admitted by the jurisprudence of the Supreme Court in its STS 2/2018, 9 de Enero de 2018 (TRIBUNAL SUPREMO, 2018) and STS 39/2004 (TRIBUNAL SUPREMO, 2004) with for prior authorization, as it considers the information contained in cell phones as personal data, according to art. 18.4 of the Spanish Constitution. Thus, Spain applies the legal regime that regulates such data's obtention for criminal investigation purposes (art. 22 of L.O. 15/1999) (AGENCIA ESTATAL BOLETÍN OFICIAL

DEL ESTADO, 1999a) and not Law n. 25/2007 (AGENCIA ESTATAL BOLETÍN OFICIAL DEL ESTADO, 2007) which regulates the conservation of data related to electronic communications and public communications networks).

At any rate, it is interesting to note that since 1991, in the European Union the group of Ministers of Justice and Home Affairs of the European Union Member States (Trevi[2]) already warned of the need to study the legal, technical and commercial effects on the telecommunications sector, especially in the matter of communications' interception.

Then, on 17 January 1995, the Council of the European Union established a list of requirements, in the Council Resolution on lawful interception of telecommunications (OFFICIAL JOURNAL OF THE EUROPEAN COMMUNITIES, 1995), to be met by authorities of the member states, network operators or service providers.

On September 11th, 1995, the Committee of Ministers introduced an appendix Recommendation R (95) 13 (COUNCIL OF EUROPE, 1995), noting the Member States' laws insufficiency in relation to criminal procedural legislation, particularly with respect to search and seizure of computer equipment and the need to regulate specific investigative measures relating to the computer system, such as the registration of computer equipment (*searching computer systems*, *seizing data stored therein* or yet, the intervention on transmitted data - which means: *intercepting data in the course of transmission).*

On November 23rd, 2001 the Convention on Cybercrime (CONSELHO EUROPEU, 2001) was held. It represents the main document and instrument of international cooperation in the fight against digital crimes. Brazil approved the accession to the Convention in 2021 (BRASIL, 2021).

Later, on April 20, 2005, through Recommendation R 10 of the Committee of Ministers to member states on "special investigation techniques" in relation to serious crimes including acts of terrorism (COUNCIL OF EUROPE, 2005) on investigation measures associated to serious crimes, including terrorism, of the Council of Europe's Committee of Ministers, the use of technology was approved for measures such as private sector collaboration, judicial or police cooperation agreements, and international cooperation on information exchange in cross-border operations.

---

2 *Ad hoc* group composed of Ministers of Justice and Internal States - members of the European Union. Its first meeting was held in the city of Trevi and its main objective is to build a forum for debates on cooperation in the fight against illegal immigration, drugs, terrorism and international violence.

http://dx.doi.org/10.20499/2236-3645.RJP2023v25e135-2830

Besides these instruments, it is also worth mentioning the Communication *Hacia una política general de lucha contra la ciberdelincuencia*[3] (COMISSÃO DAS COMUNIDADES EUROPEIAS, 2015), for the adoption of concrete measures to encourage Member States and third countries to ratify the Cybercrime Convention, as well as investigation tools such as the use of joint investigation equipment and registry or the cooperation and exchange of information between law enforcement authorities and the private sector. The Communication *Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos*[4] (COMISSÃO DAS COMUNIDADES EUROPEIAS, 2009a) indicated jurisdictional competence standards, legal framework applicable to cyberspace, and the creation of a specialized network that groups responsible people at an internal level for the development of common investigation techniques.

On either occasion, the European Commission published the "Green Paper on obtaining evidence in criminal matters in earther member state and guaranteeing its admissibility" (COMISSÃO DAS COMUNIDADES EUROPEIAS, 2009b) with the aim of increasing the use of electronic evidence.

Finally, the Annex to the Stockholm Program - *una Europa abierta y segura que sirva y proteja al ciudadano*[5] (CONSELHO EUROPEU, 2010*)* is worth mentioning. It established legislative proposals on attacks against information systems, the creation of a Europe-wide warning platform for cybercrime, the development of an European model agreement on public-private partnerships, and proposals for jurisdictional rules on digital crimes committed on an European and international scale.

One must examine the casuistry on the subject of legal *hacking* through the infiltration of agents in the digital environment. The practice of this persecutory tool, besides requiring judicial authorization to obtain evidence, needs to preserve the rights and guarantees of the investigated person. This rule exists so that the evidence is not tainted by the vice of illegality, and so that the intimacy and privacy of victims and third parties is preserved, especially when the crime is committed against the sexual dignity of a child or adolescent (FULLER et al., 2018, p. 181)

3 “Towards a general policy on the fight against cybercrime” (free translation by author)

4 “An area of freedom, security and justice serving the citizen” (free translation by author)

5 “An open and secure Europe serving and protecting citizens” (free translation by author)

http://dx.doi.org/10.20499/2236-3645.RJP2023v25e135-2830

In Brazil, infiltration of police agents in the digital environment is possible, according to some regulations, namely: art. 53 of Law n. 11343/2006 (established the National System of Public Drug Policy - SISNAD) (BRASIL, 2006); articles 10 to 14 of Law n. 12.850/2013 (Criminal Organization) (BRASIL, 2013) and Law n. 13.441/2017 (provides for the infiltration of police agents on the Internet in order to investigate crimes against the sexual dignity of children and adolescents) (BRASIL, 2017). It is true that this last legal diploma raises some doubts, such as on the lifting of the thesis of *in prepared flagrant*, on the limits of the undercover agent and on the list of criminal types that authorize the infiltration of police officers in the digital environment. However, the mentioned law establishes in a peremptory way the need for prior circumstantial and reasoned judicial authorization, so that there is no violation of constitutionally listed rights and guarantees.

In Spain, the infiltration of police officers in digital media was authorized by Organic Law n. 13/2015 (AGENCIA ESTATAL BOLETIN OFICIAL DEL ESTADO, 2015), which inserted legal provisions in Organic Law n. 5/1999 (new paragraphs to art. 282 bis) (AGENCIA ESTATAL BOLETIN OFICIAL DEL ESTADO, 1999b) and determined authorization by the investigating judge for judicial police officers to act under identity preservation, in closed channels' virtual communications. This has the purpose of producing evidence in criminal organizations' cases. It is interesting to note that undercover agents have specific authorization for cases at hand and may be authorized by the competent judge to obtain images or recordings of the conversations held between the agent and those investigated.

4 Conclusion

The present article begins by operationalizing the link between Law, especially Criminal Procedural Law and Art. It offers some considerations between the theme surveillance in information society and the book entitled "1984" by George Orwell, making it clear that there is an undeniable paradox between freedom and security - legal goods proportionally inversely related. If the first rises, the second decreases, and vice versa.

When one bears in mind the concerns above, and observes the new reality of information society, it is clear that in the face of new technologies, the rights to privacy and intimacy must be protected. Therefore, there must be a prohibition on monitoring and surveillance - when fraudulently based on constitutionally determined principles. Therefore, *hacking* in criminal prosecution must be used according to the legal limits established by the rights to intimacy, privacy, legality and ethics, under penalty of becoming a legitimizing instrument for attacks on the Brazilian democratic rule of law.

5 References

BAUMAN, Zygmunt. **Vigilância líquida:** diálogos com David Lyon. Trad. Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BERNAL-MEZA, Raúl; MASERA, Gustavo Alberto. América Latina e a sociedade da informação. **Política externa.** v. 15, n. 4, p. 23-41, mar./abr./maio 2007.

BITTAR, Eduardo C.B. **O direito na pós-modernidade**. Rio de Janeiro: Forense Universidade, 2005.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988.

BRASIL. **Lei nº 9296, de 24 de julho de 1996.** Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Available at: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Accessed on: 3 May 2022.

BRASIL. **Lei nº 11.343, de 23 de agosto de 2006.** Available at: https://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Lei/L11343.htm. Accessed on: 14 May 2021

BRASIL. **Lei nº 12.850, de 2 de agosto de 2013**. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Accessed on: 5 July 2021

BRASIL. **Lei nº 13.441, de 8 de maio de 2017**. Available at: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13441.htm. Accessed on: 5 July 2021

BRASIL. Ministério da Justiça e Segurança Pública. **Portaria nº 1.185, de 20 de dezembro de 2017**. Available at: http://www.justica.gov.br/Acesso/institucional/sumario/regimento/senasp/regimento-senasp-portaria-1185-2017.pdf. Accessed on: 9 Feb. 2018.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Accessed on: 2 May 2022.

BRASIL. Ministério da Justiça e Segurança Pública. **Aprovada adesão do Brasil à Convenção de Budapeste sobre o Crime Cibernético.** Available at: https://www.gov.br/mj/pt-br/assuntos/noticias/aprovada-adesao-do-brasil-a-convencao-de-budapeste-sobre-o-crime-cibernetico. 2021. Accessed on: 2 May 2022.

BRENNER, Susan. At light speed: attribution and response to Cybercrime/Terrorism/ Warfare. **Journal of Criminal Law & Criminology**, 2007, n. 97.

CASTELLS, Manuel. **A sociedade em rede.** A era da informação: economia, sociedade e cultura, v.1. Trad. Roneide Venancio Majer. São Paulo: Paz e Terra, 2016.

CONSELHO EUROPEU. **Convenio sobre la ciberdelincuencia.** 2001. Available at: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf. Accessed on: 12 Jun. 2018.

CONSELHO EUROPEU. **Programa de Estocolmo** — una Europa abierta y segura que sirva y proteja al ciudadano. 2010**.** Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:ES:PDF. Accessed on: 7 Jun. 2018.

COSTA JUNIOR, Paulo José. **O direito de estar só:** tutela penal da intimidade. São Paulo: Revista dos Tribunais, 1995.

COUNCIL OF EUROPE. **Recommendation R10** of the Committee of Ministers to member states on "special investigation techniques" i**n relation to serious crimes including acts of terrorism.** Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805da6f6. Accessed on: 12 Jun 2021.

COUNCIL OF EUROPE. **Convention for the protection of human rights and fundamental freedoms**, 2021. Available at: https://rm.coe.int/1680a363d2 Accessed on: 01 May 2021.

COUNCIL OF EUROPE. **Recommendation No. R (95) 131995.** 1995. Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76. Accessed on: 06 Apr 2020.

CUKIER, Kenneth; MAYER-SCHÖNBERGER, Viktor. **Big Data** – como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. Rio de Janeiro: Campus, 2012.

DI FIORE, Bruno Henrique. **Teoria dos círculos concêntricos da vida privada e suas repercussões na praxe jurídica.** 2012. Available at: www.flaviotartuce.adv.br. Acessed on: 14 Dec 2017.

EL PAÍS. **Seus dados são vendidos por 7,5 centavos de dólar.** Disponível em: https://brasil.elpais.com/brasil/2017/05/03/tecnologia/1493835469_309268.html Acesso n 13 Jan 2018.

ESPANHA. **Constitución Española,** 1978. Available at: http://www.lamoncloa.gob.es/documents/constitucion_es1.pdf. Accessed on: 02 Sept. 2018.

ESPANHA. **Agencia Estatal Boletín Oficial del Estado.** Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Available at: https://boe.es/buscar/act.php?id=BOE-A-2007-18243. Accessed on: 9 Apr. 2019.

ESPANHA. **Agencia Estatal Boletín Oficial del Estado.** Ley orgánica 13/2015, de 5 de octubre (modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica), 2015. Available at: https://www.boe.es/eli/es/lo/2015/10/05/13. Accessed on: 09 Apr 2019.

ESPANHA. **Agencia Estatal Boletín Oficial del Estado**. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Persona., 1999a. Available at: https://boe.es/buscar/doc.php?id=BOE-A-1999-23750. Accessed on: 8 Apr. 2019.

ESPANHA. **Agencia Estatal Boletín Oficial del Estado.** Ley Orgánica 5/1999, de 13 de enero, de modificación de la Ley de Enjuiciamiento Criminal en materia de perfeccionamiento de la acción investigadora relacionada con el tráfico ilegal de drogas y otras actividades ilícitas graves, 1999b. Available at: https://www.boe.es/buscar/doc.php?id=BOE-A-1999-846. Accessed on: 9 Apr. 2019.

ESPANHA. TRIBUNAL SUPREMO. **STS 2/2018,** 9 de Enero de 2018. Available at: <https://vlex.es/vid/706334405>. Accessed on: 3 Apr. 2020.

ESPANHA. TRIBUNAL SUPREMO. **STS 39/2004,** 22 de Marzo de 2004. Available at: https://www.burovoz.es/sentencia-delito-la-interceptacion-comunicaciones/. Accessed on: 4 Apr. 2021.

FULLER, Greice Patrícia. A responsabilidade social e ambiental das entidades financeiras em face do Direito Ambiental como direito humano e da sociedade da informação. **Revista da Faculdade de Direito Universidade Federal de Minas Gerais**, n. 71, 2017.

FULLER, Greice Patricia; GALLINARO, Fábio. A infiltração de agentes em meio virtual sob a égide da dignidade da pessoa humana: uma análise da Lei 13.441/2017. **Revista dos Tribunais.** São Paulo, v. 995, year 107, 2018.

FUSSEY, Pete; MAGUIRE, Mark. **Sensing evil:** Counterterrorism, techno-science, and the cultural reproduction of security. Journal Focaal. 2016.

GARCIA-ALGARRA, Javier. **La reforma carcelaria en el pensamiento ilustrado y su plasmación en modelos arquitectónicos.** 2002. Available at: https://www.researchgate.net/publication/304157195_La_reforma_carcelaria_en_el_pensamiento_ilustrado_y_su_plasmacion_en_modelos_arquitectonicos. Accessed on:13 Jun. 2021.

http://dx.doi.org/10.20499/2236-3645.RJP2023v25e135-2830

GERCKE, Marco. **Understanding cybercrime:** phenoma, challenges and legal response. 2012. Available at: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf. Accessed on: 22 Aug. 2018.

GUERRA, Sidney. **O direito à privacidade na internet:** uma discussão da esfera privada no mundo globalizado. Rio de Janeiro: América Jurídica, 2004.

HALL, Stuart. **A identidade cultural na pós-modernidade**. Rio de Janeiro: DP&A Editora, 2011.

HUBMANN, Heinrich. **Das persönlichkeitsrecht.** Münster:Böhlau-Verlag, 1953.

NATO. **North Atlantic Treaty Organization cyber defence centre of excellence.** Available at: https://ccdcoe.org/. Accessed on: 12 Oct. 2018.

OFFICIAL JOURNAL OF THE EUROPEAN COMMUNITIES. COUNCIL OF EUROPE. **Council Resolution on the lawful interception of telecommunications**, 1995. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31996G1104. Accessed on: 7 May 2021.

ORGANIZATION OF AMERICAN STATES (OAS). **American convention on human rights**. Pact of San Jose da Costa Rica. Available at: https://www.cidh.oas.org/basicos/english/basic3.american%20convention.htm. Accessed on: 2 Apr. 2018.

ORWELL, George. **1984.** São Paulo: Companhia das Letras, 2009.

PEREIRA, Marcelo Cardoso. **Direito à intimidade na internet**. Curitiba: Juruá Editora, 2004.

SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada:** uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte. Belo Horizonte: Del Rey, 1998.

SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE. **SWGDE Best Practices for Computer Forensic Examination.** 2018. Available at: https://drive.google.com/file/d/12z6Vrtmts6oxg9HHORFkHrwUPa7cGAck/view. Accessed on: 2 May 2018.

SERRANO, Nicolás González-Cuéllar. Garantías constitucionales en la persecución penal en el entorno digital. *In:* VV.AA., **Derecho y justicia penal en el siglo XXI:** liber amicorum en homenaje al Profesor Antonio González-Cuéllar Garcia. Madrid: Colex, 2006.

SOUZA, Rabindranath.Capelo de. **O direito geral de personalidade**. Coimbra: Coimbra, 1995.

http://dx.doi.org/10.20499/2236-3645.RJP2023v25e135-2830

SUPREMO TRIBUNAL FEDERAL. **HC 91.867/PA.** Órgão julgador: Segunda Turma Relator(a): Min. Gilmar Mendes. Julgamento: 24/04/2012. Available at: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=2792328. Acessed on: 3 May 2021.

SUPERIOR TRIBUNAL DE JUSTIÇA. **RHC 51.531 -** RO (2014/0232367-7). Órgão julgador: Sexta Turma. Relator: Min. Nefi Cordeiro. Julgamento: 10/04/2016. Available at: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201700958225&dt_publicacao=03/09/2018. Accessed on: 10 Oct. 2021.

UNICEF. **Declaração Universal dos Direitos do Homem.** Resolução n. 217A (III) da Assembleia Geral das Nações Unidas. 10 de dezembro de 1948. Available at: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Accessed on: 1 Apr. 2018.

UNITED NATIONS. **International Covenant on Civil and Political Rights,** 1976. Available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights. Accessed on: 1 Apr.2018

WHITAKER, Reg. **El fin de la privacidad: cómo la vigilancia total se está convirtiendo en realidade**. Barcelona: Paidós, 1999.

http://dx.doi.org/10.20499/2236-3645.RJP2023v25e135-2830