Citizens' right to privacy in data protection during criminal investigations in Brazil

Zoran Jordanoski
Senior Academic Fellow at the United Nations University, Operating Unit for Policy-Driven Electronic Governance. PhD in International Law (2011-2018), Master in International Law and International Relations (LL.M) (2008-2011), both from the University of Ss Cyril and Methodius in Skopje, North Macedonia.

Abstract: Law enforcement authorities focus on preventing crimes and conducting effective criminal investigations. In doing so, they collect information and data that might be relevant for a specific case. On the other hand, fundamental rights to privacy and data protection require minimum standards and safeguards for individuals. During criminal procedures, everyone must enjoy full respect for their privacy and data protection. Given the specific nature of the work and mandate of law enforcement authorities and formal criminal procedures, this study aims to analyse the current legal framework in Brazil that sets the legal basis for law enforcement authorities to collect and process personal data to detect, prevent, and investigate criminal offences and analyse whether this framework provides adequate and efficient safeguards to individuals. Our findings suggest that, although Brazil has no legal vacuum, it needs to adopt new legislation to regulate data protection issues during criminal investigations and proceedings. Practice shows that, if properly designed, this new legislation will avoid endangering the ability of law enforcement authorities to execute their powers in crime prevention and investigation.

Keywords: Data protection. Law enforcement. Criminal investigation. Crime prevention.

Submission: 23/09/2022
Accept: 28/09/2022

Introduction

Law enforcement authorities and citizens' right to privacy and data protection. Wherever we use both in the same context, it comes with an inevitable tension between the powers and mandates of law enforcement authorities and human rights (CARUANA, 2019), including individuals' fundamental right to protect their privacy and data (BRASIL, 1988; EU, 2012; KOKOTT; SOBOTTA, 2013; RODOTÀ, 2009; SEYYAR; GERADTS, 2020). Although not absolute (SEYYAR; GERADTS, 2020), the right to privacy and data protection must apply to all individuals regardless of their nationality, residence or status (especially in criminal procedures). Applicable to both public and private sector entities, data protection principles and rules aim to establish consistent and high protection of individuals' personal data and to designate efficient mechanisms to protect such rights. However, over the years, the practice showed that some areas require special rules for regulating data protection. That is the case with the rules aimed to protect data from individuals subject to criminal investigations or prosecutions. The specific nature of law enforcement[1] and judicial authorities[2] activities gave rise to the need for a *lex specialis* to protect personal data (CARUANA, 2019; HUDOBNIK, 2020). These rules must be carefully designated to ensure an appropriate balance between the need for efficient

[1] For our purposes, the term 'law enforcement authorities' will encompass the police and all other public authorities mandated to exercise public authority and powers to prevent, investigate, and detect criminal offences.

[2] For our purposes, the term 'judicial authorities' will encompass the courts and public prosecution offices established by law.

criminal investigations, prosecutions, and court proceedings and individuals' data protection rights (FUNTA; ONDRIA, 2021).

Digital technologies transformed the way governments and the public sector operates (BANNISTER FRANK, 2011; CORDELLA; BONINA, 2012), enabling them to increase their efficiency and effectiveness (LEITNER, 2003; MILLARD, 2010; NIELSEN; JORDANOSKI, 2020; SAVOLDELLI; CODAGNONE; MISURACA, 2014). By utilising information and communications technology, the judiciary system managed to increase its efficiency and effectiveness in general, improve access to justice (BAKAIANOVA; POLIANSKYI; SVYDA, 2020), and change how law enforcement authorities, public prosecutors, and courts communicate and exchange data. Law enforcement authorities benefited from new technologies, which improved their capacities to transform how they conduct criminal intelligence and investigations (JASSERAND, 2018). The criminal intelligence phase focuses more on collecting and processing data to detect and prevent criminal offences before they occur (such as terrorist activities, robberies, kidnappings, drug smuggling, financial crimes, etc.), whereas criminal investigations are formal procedures, usually regulated by criminal procedural laws in which one or more law enforcement or judicial authorities are authorised to conduct an official investigation to identify facts and collect evidence and circumstances regarding specific criminal acts (EU, 2016a). In both cases, the primary objective of law enforcement

authorities is to collect and process all the necessary information to be more effective and efficient in performing their tasks.

Data and information have always been essential for law enforcement authorities. Even in the past, law enforcement authorities had, by law or judge authorisation, access to most public and private databases, the ability to use surveillance, fingerprints (HOOD, 2020), DNA profiling (WILLIAMS; JOHNSON, 2013), and other tools to identify people during criminal investigations. All these data represent valuable information for law enforcement authorities to prevent crimes or conduct investigations. New technologies only improve data collection and criminal investigations (BALOGUN; ZHU, 2013; SHEETZ, 2007). Various public surveillance opportunities emerged (HILL; O'CONNOR; SLANE, 2022). Nowadays, law enforcement authorities may collect and use data from surveillance (e.g., CCTV) (DESSIMOZ; CHAMPOD, 2016) and body-worn cameras (BOWLING; IYER, 2019; RINGROSE, 2019), devices to electronically monitor defendants (KLÁTIK; VAŠKO, 2020), drones (BRADFORD *et al*., 2020), GPS tracking (e.g., from smartphones or vehicles) (SLOBOGIN, 2019), and many other technologies used during the criminal intelligence and investigation phases (JASSERAND, 2018; FUNTA; ONDRIA, 2021). Digital forensics (STOYKOVA *et al*., 2022), reverse engineering (STOYKOVA *et al*., 2022), government hacking (CAVIGLIONE; WENDZEL; MAZURCZYK, 2017; GUTHEIL *et al*., 2017; HERPIG, 2018), and other tools enabled

law enforcement authorities to extract data from digital sources to secure digital evidence for investigations and trials at a later date, if necessary. Combining these technologies with the use of artificial intelligence (BRAYNE, 2017; FERGUSON, 2017; YADAV *et al*., 2022), facial recognition technology (HILL; O'CONNOR; SLANE, 2022) or big data predictive policing technologies (BRAYNE, 2017; FERGUSON, 2017; JOH, 2016) significantly increased the opportunities and capacities of the law enforcement agencies.

However, all these opportunities come with a risk, especially regarding privacy and data protection (HILL; O'CONNOR; SLANE, 2022; MEROLA; LUM, 2012). Law enforcement authorities have grown an appetite for data (JASSERAND, 2018) and often collect all they can rather than what they need. Since the scale of data law enforcement authorities collect and process has significantly increased, these brought new challenges to ensuring the right to data protection as a fundamental right. Even if we are discussing this issue in the context of the data law enforcement authorities process to prevent, investigate, detect, or prosecute criminal offences, we must face the fact that law enforcement authorities collect all the data they can in the process. For example, the facial recognition software employed at airports collects data about all the passengers travelling to and from that airport. The same takes place with the transfer of passenger names to police authorities. Also, serious consequences for individuals' privacy can emerge from the absence of a clear legal framework and standards

regarding digital forensics, reverse engineering (STOYKOVA *et al*., 2022), and the lack of standards to extract information from mobile phones, computers, and other communication devices (GARFINKEL, 2010), including government hacking which is legally allowed in some countries.

This raises questions about the legal basis that allows law enforcement authorities to collect and process such a massive amount of data, whether we find any legal safeguards to prevent the misuse of such data, and what citizens' rights are. How these data is collected, what was the legal basis for their collection and processing, how and where it is stored, for how long they will be stored, what security measures are implemented to prevent these data from being misused or to avoid security breaches, and whether citizens have legal rights concerning this processing and how they can execute them are just some of the questions which must be properly regulated. This brings us to the utmost importance of regulating personal data protection for all individuals whose data law enforcement authorities process to detect, prevent, and investigate criminal offences.

The debate on how to ensure a proper balance between the interests of individuals in protecting their data and the mandate of law enforcement authorities to protect the interests of society and fight crime (FUNTA; ONDRIA, 2021) is ongoing (SEYYAR; GERADTS, 2020). In the meantime, we are seeing the adoption of various international and domestic legal instruments to achieve such balance. Convention 108+ (COUNCIL OF EUROPE, 2018)

of the Council of Europe regulates all areas regarding personal data processing at the European level, including the activities of law enforcement and judicial authorities (FUNTA; ONDRIA, 2021). Resembling the European Union (EU) General Data Protection Regulation (EU, 2016c), the EU has adopted Directive 2016/680 (EU, 2016b), which defines, in its Article 1, that it:

> […] lays down the rules relating to 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, including the safeguarding against and the prevention of threats to public security. (EU, 2016b, p. 105).

Directive (EU) 2016/680 also specifies data protection principles, controllers' (law enforcement and judicial authorities) obligations, subjects' data rights, data protection design and by default principles, the obligation to appoint a Data Protection Officer (DPO), data breach notifications, and others (CARUANA, 2019; EU, 2016b; FUNTA; ONDRIA, 2021; HUDOBNIK, 2020; JASSERAND, 2018; LYNSKEY, 2019; SEYYAR; GERADTS, 2020). Note that all 27 EU Member States must adopt national legislation to transpose the rules and minimum standards imposed via the Directive (EU) 2016/680. Other countries (non-EU Member States) followed this example and adopted domestic legislation.

Following these global trends and practices, this study aims to analyse the current legal framework in Brazil to regulate the rules and procedures which enable law enforcement authorities to

collect and process personal data to detect, prevent, and investigate criminal offences. If existing, does this legal framework provide adequate and efficient safeguards to subjects and ensure the balance between effective and efficient criminal investigation and data protection in Brazil?

I have organised the remainder of this study as follows: we show our research methodology in section 1; analyse the current legal framework for data protection and criminal procedure in Brazil in section 2; assess the impact of the new legislation on criminal procedures in Brazil in section 3; and lastly, delineate the importance of our findings for policymakers and indicates the future scope of the current research in our conclusion.

1 Methodology

This study addresses two key questions. First, does Brazil have a legal framework that sets the legal basis for law enforcement authorities to collect and process personal data to detect, prevent, and investigate criminal offences? Second, does this legal framework provide adequate and efficient safeguards to data subjects and does it ensure the balance between effective and efficient criminal investigations and data protection in Brazil? Lastly, how will this new data protection legislation to detect, prevent, and investigate criminal offences in Brazil impact the ability of law enforcement authorities to prevent crimes or conduct effective criminal investigations?

To answer these research questions, the method of analysis (BHAT, 2020) was applied to examine the current state of data protection regulation so law enforcement can detect, prevent, and investigate criminal offences. A synthesis method (COOPER, 2021; LLEWELLYN, 2012) combined all information and abstract patterns to create a single unit. Lastly, the comparative method helped us to analyse the problem from different angles and compare the Brazilian solutions with the EU or other solutions globally (FUNTA; ONDRIA, 2021).

Primary sources include relevant national policy documents and legislation, such as the Federal Constitution, the General Data Protection Act (LGPD), the Penal Code, the Criminal Procedure Code, and other relevant legislation in Brazil. Internationally, the primary sources included the EU General Data Protection Regulation (GDPR), the EU Directive 2016/680, and other relevant international and regional acts and regulations.

2 Identifying the relevant legal framework

This section aims to identify the relevant legal framework to protect individuals' data to prevent, detect, and investigate criminal offences in Brazil.

The Brazilian Federal Constitution (BRASIL, 1988) recognised privacy and data protection in Brazil as a fundamental right. Article 5 X contains a general provision on the right to privacy, defining that "the privacy, private life, honour and image of persons are inviolable, and the right to compensation for property or moral

damages resulting from their violation is ensured." Furthermore, Article 5 XII defines that the "secrecy of correspondence and of telegraphic, data and telephone communications is inviolable." However, this right is not absolute and, as defined in the second part of the same provision, it is subject to restrictions in case of "by court order, in the cases and in the manner prescribed by law for the purposes of a criminal investigation or criminal procedural finding of facts." The recent Constitutional changes in 2022 further specified the right to privacy and data protection in Article 5 LXXIX, indicating that "under the terms of the law, the right to protection of personal data is ensured, including in digital media." Although a fundamental right, it is not absolute, as the Constitution provides that exceptions can be made under the terms specified in a particular law.

Currently, the most important law which regulates the collection and use of personal data in Brazil is its General Data Protection Law (BRASIL, 2018). Adopted in September 2018, the law entered into force in August 2020, whereas the provisions on penalties became enforceable on August 1, 2021. Influenced by the EU GDPR, the LGPD defines the basic principles to process data (Article 6), the legal basis to process personal data (Articles 7-16), subjects' data rights (Articles 17-22), the processing of personal data by public authorities (Articles 23-32), the international transfer of data (Articles 33-36), personal data processing agents (Articles 37-45), monitoring and sanctions (Article 52-54), and others.

The LGPD represents a general legal framework which regulates the collection and use of personal data in Brazil, aimed at unifying the existing laws which contain provisions for processing personal data. Regarding applicability, the LGPD adopts the extraterritoriality principle, which is common for privacy laws nowadays. Article 3 of the LGPD states that it applies to "any processing operation carried out by a natural person or a legal entity of either public or private law, irrespective of the means, the country in which its headquarter is located or the country where the data are located." The only conditions for applying the LGPD are that the procession operation is carried out in Brazil. The processing activity aims at offering or providing goods or services or at processing data of individuals located on the Brazilian territory or personal data collected within the national territory.

The LGPD also authorises the National Data Protection Authority (*Autoridade Nacional de Proteção de Dados*) (ANPD) to be the main body of the federal public administration with technical and decision-making autonomy and the responsibility to ensure the protection of personal data and for guiding, regulating, and monitoring compliance with legislation. Although it was created in 2018, the ANPD effectively began functioning after the appointment of its first Chief Executive Officer on November 5, 2020. The main tasks of the ANPD, among others, are to ensure the protection of personal data under the terms and conditions defined in the legislation, oversee the implementation of the law and the data processing by public and private sector entities, perform

inspections, impose administrative sanctions, develop guidelines to protect national data and establish privacy policies, and raise awareness among the population.

However, following the global practices and the EU GDPR model, Article 4 of the law defines the exemptions to which the LGPD fails to apply. Among other exemptions, Article 4 (III) provides that LGPD fails to apply to processing personal data performed solely for public safety, national defence, state security, or investigation and prosecution of criminal offences. This exemption excludes the application of the LGPD and its safeguards for all data processing operations undertaken by law enforcement authorities, public prosecutors, and Brazilian courts. For comparison, the EU GDPR also makes exemptions. Recital 19 defines that the processing of personal data to prevent, investigate, detect or prosecute criminal offences or execute criminal penalties is exempted from the application of the GDPR. Such processing is regulated by the Directive (EU) 2016/680, the so-called 'Police Directive' (EDPS, 2022; VOGIATZOGLOU; FANTIN, 2019) or 'Law Enforcement Directive' (HUDOBNIK, 2020; LEISER; CUSTERS, 2019).

We find provisions related to the protection of privacy and data protection in both the Brazilian Penal Code (BRASIL, 1940) and the Criminal Procedure Code (BRASIL, 1941). The Penal Code contains general provisions in Article 153, which address crimes relating to the inviolability of correspondence and the invasion of information technology devices. On the other hand, the Criminal Procedure Code also contains explicit provisions in

its article 201 §6, obliging judges to take all necessary measures to preserve defendants' privacy, private life, honour, and image. If found necessary, judges may establish justice secrecy concerning the data, testimonies, and other information contained in the records concerning defendants to avoid their exposure to the public and the media.

Regarding criminal procedure and evidence collection, the general rule is that any interference with suspects' privacy requires a warrant. Warrants, as regulated in Article 3-A XI of the Criminal Procedure Code, are mandatory to search for residents and companies, authorise wiretapping or electronic surveillance, collect data protected by constitutional secrecy (telephone and electronic communications, call logs, bank records, fiscal data, and other correspondence), access confidential information, or any other means to obtain evidence which may restrict investigated persons' fundamental rights. Failing to comply with this obligation can result in evidence inadmissibility in court proceedings, as provided in Article 5, LVI of the Brazilian Constitution. To complement the Criminal Procedure Code, the country has adopted the Interception of Telephone Communication Law (BRASIL, 1996), aimed to define the procedure which authorises the interception of communications or wiretapping of information technology devices in the context of a criminal investigation.

The Brazilian Civil Code (BRASIL, 2002) also distinguishes the right to privacy and private life as a personality right which cannot be waived or subject to voluntary limitations. Among

others, article 21 defines that "the private life of the natural person is inviolable, and the judge, the application of the person concerned, shall adopt the necessary arrangements to prevent or otherwise cease to act contrary to this norm." Significantly, the Civil Code confirms the regimes of pseudonymised data as personal data. Namely, its article 19 defines that "the pseudonym adopted for lawful activities enjoys the protection that one gives to the name," which falls under the LGPD data protection regime.

Provisions related to privacy and data protection can be found in other laws and regulations in Brazil. For example, the Civil Rights Framework for the Internet (BRASIL, 2014) "settles principles, guarantees, rights and duties for the users of the web in Brazil" (CIVIL…, 2014). The law imposed requirements regarding the processing of personal data of Internet users, obligations for service providers, and the rights of Internet users. Further, the Brazilian Consumer Protection Code (BRASIL, 1990) contains rules regarding the collection, storage, and use of consumer data. It defines "consumer" as any individual or legal entity that acquires goods or services as an end-user. Also, the Information Access Law (BRASIL, 2011b), which regulates the terms and conditions for access to information held by public entities and agencies in Brazil, provides a legal definition of what is considered "personal information" for the purpose of the law. Namely, article 4 IV defines personal information as any information "related to the identified or identifiable natural person." Provisions can also be found in its complementary law (BRASIL, 2001), which established rules

regarding bank secrecy for financial institutions, and the Good Payer's Registry Law (BRASIL, 2011a), which regulates the establishment of credit and purchase history databases.

The Criminal Procedure Code regulates criminal procedures and investigations as part of them. Its articles 4 to 23 control the powers and mandate of law enforcement authorities and the procedural steps to conduct the investigations. It clearly defines who can initiate investigations, what are the roles and responsibilities of the law enforcement authorities regarding investigating, collecting, documenting facts and evidence, and taking all necessary steps to discover potential offenders and help victims (if any). In doing so, law enforcement authorities can collect data from other public or private entities or citizens. During investigations, according to article 3-B XI of the Criminal Procedure Code, if found necessary, law enforcement authorities can request, from courts, a warrant to intercept telephones, the flow of communications in computer and telematics systems or other forms of communication; remove fiscal, banking, data, and telephone secrecy; search and seize homes; access confidential information; and other means of obtaining evidence which restricts investigated persons' fundamental rights. Such provision established the legal guarantee of individuals' right to privacy from unlawful actions from law enforcement authorities. Judges must approve every interference with suspects or investigated persons' privacy.

Regarding the powers and authorisations of law enforcement authorities, the Constitution regulates some of them, whereas specific laws, others. Article 144 defines the key law enforcement authorities and their mandates. For criminal intelligence and investigation, the key law enforcement agencies mandated to investigate criminal activities are the federal and civil police. According to article 144 §1 of the Constitution, the Federal Police is mandated to:

> I – Investigate criminal offences against the political and the social order or to the detriment of property, services and interests of the Union or of its autonomous government entities and public companies, as well as other offences whose practice has interstate or international effects and requiring uniform repression, as the law shall establish; II – to prevent and repress illegal traffic of narcotics and like drugs, as well as smuggling and embezzlement, without prejudice to action by the treasury and other government agencies in their respective areas of competence; III – Exercise the functions of maritime, airport and border police […]. (BRASIL, 1988).

Some of these offences are further specified in special laws which mandate the federal police the power to investigate specific crimes (e.g., cybercrimes, prevent and combat terrorism, organised crime, etc.).

Article 144 §4 of the Constitution also defines the mandate of the civil police, which is mandated to "except for the competence of the Union, to exercise the functions of criminal police and to investigate criminal offences, with the exception of the military ones." Currently, each state (and the Federal District) has its own police department (a total of 27), aimed to conduct all criminal

investigations which fail to fall under the mandate of the federal or military police.

Apart from the federal and civil police, we find other government agencies which, within their mandate, may conduct criminal investigations in their focus area. These agencies include IBAMA – the Brazilian Institute of Environment and Renewable Natural Resources (environmental offences), the Federal Revenue of Brazil (offences related to revenue and federal tax frauds), the Central Bank of Brazil (financial crimes), the Securities and Exchange Commission (offences in the securities market), and COAF – the Council for Financial Activities Control (anti-money laundering and countering the financing of terrorist activities).

By analysing the Brazilian domestic legislation and comparing it to the EU standards imposed by Directive 2016/680 leads us to answer our first two research questions. Namely, Brazil has no legal vacuum in Brazil regarding the protection of individuals' data to detect, prevent, and investigate. The fundamental right to data protection, as provided by the Constitution, applies to all citizens and legal residents in Brazil, including those subjected to investigation. The Brazilian Constitution and the Criminal Procedure Code guarantee respect for individuals' privacy or private life. The involvement of judges in investigations, as those who must authorise actions against individuals' privacy, represents a significant safeguard over the possibility of law enforcement authorities misusing their power and authorisations. Lastly, article 20 of the Criminal Procedure

Code provides a general obligation for law enforcement authorities to "ensure in the investigation the secrecy necessary to elucidate the fact or required by the interests of society." This provision can be understood in light of the need for law enforcement authorities to use technical and organisational measures to ensure the secrecy of investigations and the integrity of the collected data.

However, the answer to our second research question is obvious if we compare these standards to EU Directive 2016/680 and the current legal framework applicable in Brazil. Findings show that the discussed and analysed legal framework in Brazil fails to provide adequate and efficient legal safeguards for subjects' data and ensure the balance between effective and efficient criminal investigation and data protection in Brazil. The LGPD fails to apply to detection, prevention, and investigation of criminal offences, and neither the Criminal Procedure Code nor other laws define principles to process data, the obligations of law enforcement authorities regarding technical and organisational measures, and most importantly, fails to regulate citizens' rights and the procedures to enforce them. This results in the absence of legal mechanisms to operationalise the fundamental constitutional right to data protection for individuals subjected to criminal investigations or prosecutions.

3 The need for new legislation to protect data in criminal investigations

Following our conclusion that Brazil needs to adopt new legislation to operationalise citizens' constitutional right to data protection in detecting, preventing, and investigating criminal offences, this section aims to continue to discuss it's the adoption of new legislation (COSTA; REIS, 2021; OLIVEIRA, 2022a, 2022b), rather than providing its content. Rather, we aim to answer our third research question and provide an overview of how the new legislation (working title: Penal LGPD) will impact criminal investigations.

The new legislation should follow the same concept and approach as the LGPD and use the EU Directive 2016/680 standards as its guide. These principles should be tailored to ensure the balance between the safeguards to protect data subjects' rights and freedoms concerning the processing of personal data by law enforcement agencies and the need for effective and efficient criminal investigation.

3.1 Data protection principles

Following domestic and international best practices, we recommend that the new legislation include the following principles:

Lawfulness[3], *Purpose limitation*[4], *Adequacy*[5], *Necessity*[6], *Quality of data*[7], *Security*[8], *Prevention*[9], *Time limits for storage and review*[10], *Non-discrimination*[11], and *Accountability*[12]. The new legislation should also make a clear distinction between different categories of data subjects, such as persons in situations in which we find serious grounds for believing they have committed or are about to commit a criminal offence, persons convicted of criminal offences, victims or potential ones, and other parties (e.g., witnesses).

3 Legally processed only by a competent authority necessary for the performance of a task (adapted from EU, 2016b, Article 8).

4 Processed for specific and explicit purposes with no possibility of subsequent processing that is incompatible with these purposes (adopted from BRASIL, 2018, Article 6, I).

5 Compatibility between processing and purposes, in accordance with its context (BRASIL, 2018, Article 6, II).

6 Limitation of processing to the minimum necessary to achieve its purposes, covering data which are relevant, proportional, and non-excessive regarding its purposes (BRASIL, 2018, Article 6, III).

7 Guarantee to data subjects of the accuracy, clarity, relevancy, and updating of the data, in accordance with needs and to achieve the purpose of processing (BRASIL, 2018, Article 6, V).

8 Use of technical and administrative measures which are able to protect personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, alteration, communication, or dissemination (BRASIL, 2018, Article 6, VII).

9 Adoption of measures to prevent the occurrence of damages due to the processing of personal data (BRASIL, 2018, Article 6, VIII).

10 Appropriate time limits to be established to erase personal data or a periodic review of the need to storage personal data (adopted from EU, 2016b, Article 5).

11 Impossibility of processing for unlawful or abusive discriminatory purposes (BRASIL, 2018, Article 6, IX).

12 Demonstration, by the data processing agent, of the adoption of measures which are efficient and capable of proving compliance with the rules of personal data protection, including the efficacy of such measures (BRASIL, 2018, Article 6, X).

In practice, these principles will avoid jeopardising the ability of law enforcement authorities to prevent, detect or investigate criminal activities. Brazilian law enforcement agencies already implement and respect most principles *de facto*, but the practice varies. Their adoption will increase the harmonisation across the country and improve the quality of criminal investigations. It will provide guidance on what data can be collected and processed, how to securely store it, time limitations, how investigations can use it, how to share and disclose them to other relevant authorities, and how to perform international transfers (e.g., INTERPOL).

3.2 New obligations for law enforcement authorities

This new legislation will inevitably impose new obligations on law enforcement authorities. Yet, we should refrain from considering these new obligations as obligations which will hinder or jeopardise criminal investigations. All these obligations will improve the quality of law enforcement agencies' work and of criminal investigations regarding evidence collection, processing, storing, and sharing with other agencies and public prosecutors, and use during the court procedure.

In general, law enforcement authorities will have to adopt and implement appropriate *technical and organisational (administrative) measures to ensure data security and secrecy via* appropriate *data protection policies*. This will practically mean that considering the nature, scope, context, and purposes of processing, as well as the risks of varying likelihood and severity

for natural persons' rights and freedoms, each law enforcement agency will need to develop its internal data protection policies and standards which will be mandatory for its officials during all phases of investigations. To ensure that these policies and procedures are aligned with the law, the supervisory authority should review and approve them. This aligns with the obligation of the law enforcement authorities to *cooperate with the supervisory authority*. This obligation will in no way endanger criminal investigations. Rather, it will provide clear and harmonised internal rules that will standardise the practice inside each law enforcement agency.

Considering the scope of data security and secrecy, as provided for in Chapter VII of the LGPD, we expect the new legislation to adopt the same requirements and standards as a minimum for criminal investigation. This will practically mean that, as with article 46 of the LGPD, law enforcement authorities will have to "adopt security, technical and administrative measures able to protect personal data from unauthorised accesses and accidental or unlawful situations of destruction, loss, alteration, communication or any type of improper or unlawful processing." Following this practice with the EU Directive 2016/680, these provisions will require law enforcement agencies to ensure equipment access control[13], data media control[14], storage control[15],

[13] Deny unauthorised persons access to processing equipment (EU, 2016b, Article 29, 2a).

[14] Prevent the unauthorised reading, copying, modification, or removal of data media (EU, 2016b, Article 29, 2b).

[15] Prevent the unauthorised input of personal data and the unauthorised inspection, modification, or deletion of stored personal data (EU, 2016b, Article 29, 2c).

user control[16], data access control[17], communication control[18], input control[19], transport control[20], recovery[21], and integrity[22].

The new legislation will also impose the obligation for law enforcement agencies to designate a data protection officer (DPO). Courts and other independent judicial authorities (such as the public prosecutor's office) may avoid this obligation when acting in their judicial capacity from that obligation. In practice, this will fail to constitute a novelty since all public authorities are already obliged to designate a DPO according to articles 23 (III) and 41 of the LGPD. Following this, law enforcement authorities will need to either authorise the existing DPOs to act as DPOs in accordance with the new legislation or appoint new DPOs in parallel with the existing ones. We are unable to recommend

16 Prevent the use of automated processing systems by unauthorised persons using data communication equipment (EU, 2016b, Article 29, 2d).

17 Ensure that persons authorised to use an automated processing system have access only to the personal data covered by their authorisation (EU, 2016b, Article 29, 2e).

18 Ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment (EU, 2016b, Article 29, 2f).

19 Ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom personal data were input (EU, 2016b, Article 29, 2g).

20 Prevent the unauthorised reading, copying, modification, or deletion of personal data during transfers of personal data or during transportation of data media (EU, 2016b, Article 29, 2h).

21 Ensure that installed systems may, in case of interruption, be restored (EU, 2016b, Article 29, 2i).

22 Ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability'), and that stored personal data are unable to be corrupted by a malfunctioning of the system (EU, 2016b, Article 29, 2j).

the latter (although it is possible) as it can create a dualism in the functioning of the authority. In any case, the DPO will have the power to inform and advise the authority and the employees who process their obligations according to the new legislation, monitor compliance with the new legislation, and cooperate with the supervisory authority.

The aim of all these obligations for law enforcement authorities is, rather than slowing down or jeopardising criminal investigations, to increase the security and handling of the data collected in the investigations, which will most likely be used in the later stages of court proceedings.

3.3 Rights of individuals

Subjects' data rights should be the cornerstone of the new legislation. It must operationalise the fundamental constitutional right to data protection and carefully define the subjects' data rights and the mechanisms for their enforcement in line with the principle of an effective and efficient criminal investigation. Following global practices but also the specific nature of criminal investigations, the new legislation should define the right to information, access, and to rectification or erasure of personal data and restriction of processing as subjects' minimum rights.

The *right to information* is essential. It will provide a general obligation to all law enforcement authorities to provide basic information on their websites about the controller's name, legal grounds for processing data, the purpose of processing,

DPO contact details, and citizens' rights. The law enforcement authority will be, by law, obliged to provide information to subjects regarding the legal basis for processing, the period for which personal data will be stored and processed, and the recipients of those data (e.g. third countries or international organisations). However, having the specific nature of criminal investigations in mind, law enforcement authorities can decide to delay, restrict or omit the provision of information to data subjects as long as such a measure constitutes a necessary and proportionate measure to avoid obstructing official or legal inquiries, investigations or procedures, protect the public and national security or ensure the rights and freedoms of others.

The *right to access* is also essential for individuals. Every individual will have the right to obtain information from law enforcement authorities on whether or not their personal data are being processed, for what purpose, which categories of data are being processed, who are the recipients of the personal data (e.g. third countries or international organisations), and the predicted period for which the personal data will be stored. Apart from providing all this information, law enforcement authorities should also inform data subjects about their rights to request rectification or erasure of personal data, the right to request the restriction of personal data processing, and the right to complain to the supervisory authority. Nevertheless, this right is not absolute, and law enforcement authorities can decide to delay, restrict, or omit the provision of information to data subjects as long as such

a measure constitutes a necessary and proportionate measure to avoid obstructing official or legal inquiries, investigations, or procedures, protect the public and national security or ensure the rights and freedoms of others. Any refusal or restriction to access must be in writing, and explain the reasons for the refusal or restriction. Again, this information can be omitted when law enforcement authorities find that disclosing this information can jeopardise criminal investigations.

The *right to rectification or erasure of personal data and restriction of processing* is also important for data subjects and criminal investigations. The country shall guarantee the right of data subjects to obtain from the controller (without undue delay) the rectification of inaccurate personal data relating to them. Also, data subjects should have the right to require the controller to erase their data if processing infringes basic data protection principles (as defined in the new legislation) or if data were unlawfully processed (as decided by the supervisory authority or the court). However, instead of erasure, the controller can restrict the processing if the accuracy of personal data cannot be ascertained or if it must maintain the data for evidence. Similar to the previous rights, law enforcement authorities can delay, restrict, or omit the provision of information to data subjects as long as such a measure constitutes a necessary and proportionate measure to avoid obstructing official or legal inquiries, investigations, or procedures, protect the public and national security, or protect the rights and freedoms of others. Law enforcement authorities must explain any refusal of rectification,

erasure of personal data, or processing restriction. Again, this information can be omitted when the controller assesses that it can jeopardise the criminal investigation.

However, to avoid the exception becoming a rule and law enforcement authorities always refusing or remaining silent to data subjects' requests, the new legislation should provide a legal procedure for data subjects to exercise their right via the supervisory authority. The latter should guarantee that any refusals made by the controller are justified and in line with the balance between efficient criminal investigations and data protection. Each controller processing personal data under the new legislation should make this information available on their websites. Lastly, the new legislation should establish a judicial remedy if data subjects are unsatisfied with the supervisory authority's decision.

4 Conclusion

This research found that the recent constitutional changes in Brazil recognised the right to personal data protection as a fundamental right. Inspired and influenced by the EU GDPR, Brazil has already adopted and implemented the LGPD to regulate the collection and use of personal data in Brazil. Following the GDPR exemption of the competent authorities to process personal data for law enforcement purposes (Article 2 (1)(d)), the LGPD also excludes its application to process personal data in activities of investigation and prosecution of criminal offences (Article 4(III)(d)). Thus, Brazil followed the EU data protection model and

excluded the application of LGPD to process personal data in activities of investigation and prosecution of criminal offences. However, Brazil failed to adopt an additional instrument to regulate these issues and avoid legal uncertainties and protect individuals' personal data during criminal investigations or proceedings.

The analysis of the current Brazilian legal framework regarding individuals' data in detecting, preventing, and investigating crimes showed that its Constitution and the Criminal Procedure Code guarantee respect for individuals' privacy and data protection regarding any interference with their privacy or private life. Judges' involvement in investigations as one who must authorise actions against the privacy of individuals represents a significant safeguard over the possibility of power misuse and authorisation law enforcement authorities enjoy. Article 20 of the Criminal Procedure Code can also be interpreted as imposing obligations to law enforcement authorities to use technical and organisational measures to ensure the secrecy of investigations and the integrity of the collected data.

However, comparing the imposed standards with EU Directive 2016/680 and the current legal framework applicable in Brazil, we conclude that the existing legal framework in Brazil fails to provide adequate and efficient safeguards to subjects' data and ensure the balance between effective and efficient criminal investigation and data protection in Brazil. This resulted from the country missing the legislation to operationalise the fundamental constitutional right to data protection for individuals subjected to

criminal investigation or prosecution and failing to define principles for data processing, the obligations of law enforcement authorities regarding technical and organisational measures, and most importantly, failing to regulate citizens' rights and the procedure to enforce them. As a result, adopting new legislation to protect individuals' rights and establish the balance between efficient criminal investigations and the legal safeguards of citizens' right to privacy and data protection is of utmost importance.

Concerning our third research question, on how the new data protection legislation to detect, prevent, and investigate crimes in Brazil will impact the ability of its law enforcement authorities to prevent crimes or conduct effective criminal investigations, the practice of EU Member States shows that respecting individuals' data protection rights of imposed with the Directive (EU) 2016/680 during criminal investigations will neither endanger the ability of law enforcement authorities to prevent and investigate crimes nor conduct efficient criminal investigations. Rather, such legislation will harmonise Brazilian rules and improve its criminal investigations. It will guide them on what data can be collected and processed, how to securely store them, their time limitations, how to use them during investigations, how to share and disclose to other relevant authorities, and international transfers. The obligation to designate a DPO, conduct data protection impact assessments, and implement data protection policies and technical and organisational (administrative) measures will increase the level of security of handling the data collected during the

investigation. Lastly, individuals' rights and legal mechanisms for their enforcement should never be seen as a threat to the work of law enforcement or judicial authorities in democratic societies. All these facts favour the Brazilian need to adopt new legislation regulating individuals' right to data protection for detecting, preventing, and investigating crimes.

To further explore our findings, future research should focus on the use of new emerging technologies by Brazilian law enforcement authorities to prevent and investigate crimes, how it uses these technologies in the absence of special legislation to protect data, their efficiency, what security measures are implemented, and how the new legislation will impact its use.

Acknowledgment

This document is a result of the project "INOV.EGOV-Digital Governance Innovation for Inclusive, Resilient and Sustainable Societies / NORTE-01-0145-FEDER-000087", supported by Norte Portugal Regional Operational Programme (NORTE 2020), under the PORTUGAL 2020 Partnership Agreement, through the European Regional Development Fund (EFDR).

Título: O direito do cidadão à privacidade na proteção de dados durante investigações criminais no Brasil

Resumo: As autoridades policiais focam na prevenção de crimes e na condução efetiva de investigações criminais. Para tanto, elas colhem informações e dados que possam ser relevantes para um caso específico. Entretanto, os direitos fundamentais à privacidade e à proteção de dados exigem padrões e garantias mínimos aos indivíduos. No curso do inquérito policial, todos devem gozar do

direito à total privacidade e à integral proteção de dados. Considerando as naturezas específicas do trabalho e das atribuições das autoridades policiais e, também, do inquérito, este estudo procura analisar o atual arcabouço jurídico pátrio que ampara legalmente a coleta e processamento de dados pelas autoridades de polícia para detectar, prevenir e investigar delitos. Ademais, o trabalho busca examinar se o arcabouço assegura aos indivíduos um resguardo adequado e eficiente. Nossos achados sugerem que, embora o Brasil não padeça de um vácuo legal, é preciso aprovar uma nova legislação que disponha sobre questões de proteção de dados durante investigações na fase inquisitorial. A prática demonstra que, se adequadamente delineada, a nova legislação evitará prejuízos à capacidade das autoridades policiais de executar as suas atribuições de prevenção e investigação de crimes.

Palavras-chave: Proteção de dados. Polícia. Investigação criminal. Prevenção de crimes.

References

BAKAIANOVA, Nana; POLIANSKYI, Yurii; SVYDA, Oleksii. Information technology in the litigation due to the pandemic COVID-19. *Cuestiones Políticas*, Maracaibo, v. 38, n. 67, p. 485-499, 2020.

BALOGUN, Adedayo M.; ZHU, Shao Ying. Privacy impacts of data encryption on the efficiency of digital forensics technology. *International Journal of Advanced Computer Science and Applications*, Cleckheaton, v. 4, n. 5, p. 36-40, 2013.

BANNISTER, Frank; CONNOLLY, Regina. Transformation and public sector values. *In*: IFIP WG 8.5 INTERNATIONAL CONFERENCE, 3.; EPART 2011, 2011, Delft. Proceedings […]. New York: Springer, 2011. p. 231-239.

BHAT, P. Ishwara. Analytical legal research for expounding the legal wor(l)d'. *In*: BHAT, P. Ishwara. *Idea and methods of legal research*. Oxford: Oxford University Press, 2020. p. 169-197.

BOWLING, Ben; IYER, Shruti. Automated policing: the case of body-worn video. *International Journal of Law in Context*, Cambridge, v. 15, n. 2, p. 140-161, 2019.

BRADFORD, B. *et al.* Live facial recognition: trust and legitimacy as predictors of public support for police use of new technology. *The British Journal of Criminology*, Oxford, v. 60, n. 6, p. 1502-1522, 2020.

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil de* 1988. Brasília, DF: Senado Federal, 1988. Available at: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Accessed on: 29 Sep. 2022.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. *Diário Oficial da União*, Rio de Janeiro, 31 dez. 1940. Available at: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Accessed on: 29 Sep. 2022.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. *Diário Oficial da União*, Rio de Janeiro, 13 out. 1941. Available at: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Accessed on: 29 Sep. 2022.

BRASIL. Lei Complementar nº 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. *Diário Oficial Eletrônico*, Brasília, DF, 11 jan. 2001. Available at: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm. Accessed on: 29 Sep. 2022.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*, Brasília, DF, 12 set. 1990. Accessed on: 29 Sep. 2022.

BRASIL. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. *Diário Oficial da União*, Brasília, DF, 25 jul. 1996. Available at: http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm. Accessed on: 29 Sep. 2022.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. *Diário Oficial da União*, Brasília, DF, 11 jan. 2002. Available at: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Accessed on: 29 Sep. 2022.

BRASIL. Lei nº 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. *Diário Oficial da União*, Brasília, DF, 10 jun. 2011a. Available at: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm. Accessed on: 29 Sep. 2022.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal […]. *Diário Oficial da União*, Brasília, DF, 18 nov. 2011b. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Accessed on: 29 Sep. 2022.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*, Brasília, DF, 24 abr. 2014. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Accessed on: 29 Sep. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). *Diário Oficial da União*, Brasília, DF, 15 ago. 2018. Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Accessed on: 29 Sep. 2022.

BRAYNE, Sarah. Big data surveillance: the case of policing. *American Sociological Review*, Thousando Oaks, v. 82, n. 5, p. 977-1008, 2017.

CARUANA, Mireille M. The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement. *International Review of Law, Computers & Technology*, Abingdon, v. 33, n. 3, p. 249-270, 2019.

CAVIGLIONE, Luca; WENDZEL, Steffen; MAZURCZYK, Wojciech. The future of digital forensics: challenges and the road ahead. *IEEE Security & Privacy*, Piscataway, v. 15, n. 6, p. 12-17, 2017.

CIVIL rights framework for the internet in Brazil: What is it? *Pensando o Direito*, 2014. Available at: http://pensando.mj.gov.br/marcocivil/civil-rights-framework-for-the-internet-in-brazil/. Accessed on: 29 Sep. 2022.

COOPER, Jennifer M. The science of legal synthesis. *St. John's Law Review*, New York, v. 95, n. 2, p. 285-318, 2022.

CORDELLA, Antonio; BONINA, Carla M. A public value perspective for ICT enabled public sector reforms: A theoretical reflection. *Government Information Quarterly*, Amsterdam, v. 29, n. 4, p. 512-520, 2012.

COSTA, Eduarda; REIS, Carolina. Histórico da LGPD penal: o que foi feito até aqui e quais são os próximos passos? *Lapin*, Brasília, DF, 16 abr. 2021. Available at: https://lapin.org.br/2021/04/16/lgpd-penal-o-que-foi-feito-ate-aqui-e-quais-sao-os-proximos-passos/. Accessed on: 22 Sep. 2022.

COUNCIL OF EUROPE. *Modernised convention for the protection of individuals with regard to the processing of personal data*. Strasbourg: Council of Europe, 2018.

DESSIMOZ, Damien; CHAMPOD, Christophe. A dedicated framework for weak biometrics in forensic science for investigation and intelligence purposes: The case of facial information. *Security Journal*, New York, v. 29, n. 4, p. 603-617, 2016.

EUROPEAN DATA PROTECTION SUPERVISOR (EDPS). *Police directive*. Brussels: EDPS, 2022. Available at: https://edps.europa.eu/data-protection/our-work/subjects/police-directive_en. Accessed on: 29 Sep. 2022.

EUROPEAN UNION (EU). Charter of fundamental rights of the European Union. *Official Journal of the European Union*, Luxembourg, 26 Oct. 2012. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN. Accessed on: 29 Sep. 2022.

EUROPEAN UNION (EU). Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union. *Official Journal of the European Union*, Luxembourg, 29 Dec. 2016a. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006F0960&from=en. Accessed on: 29 Sep. 2022.

EUROPEAN UNION (EU). Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data […]. *Official Journal of the European Union*, Luxembourg, 4 May 2016b. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN. Accessed on: 29 Sep. 2022.

EUROPEAN UNION (EU). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, Luxembourg, 4 may 2016c. European Union. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Accessed on: 29 Sep. 2022.

FERGUSON, Andrew Guthrie. *The rise of big data policing: Surveillance, race, and the future of law enforcement*. New York: NYU Press, 2017.

FUNTA, Rastislav; ONDRIA, Peter. Data protection in law enforcement and judicial cooperation in criminal matters. *TalTech Journal of European Studies*, Tallinn, v. 11, n. 2, p. 148-166, 2021.

GARFINKEL, Simson L. Digital forensics research: The next 10 years. *Digital Investigation*, Amsterdam, v. 7, p. S64-S73, 2010. Supplement.

GUTHEIL, Mirja *et al*. *Legal frameworks for hacking by law enforcement: Identification, evaluation and comparison of practices*. Brussels: European Parliament, 2017. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf. Accessed on: 29 Sep. 2022.

HERPIG, Sven. *A framework for government hacking in criminal investigations*. Berlin: Stiftung Neue Verantwortung, 2018. Available at: https://www.stiftung-nv.de/sites/default/files/framework_for_government_hacking_in_criminal_investigations.pdf. Accessed on: 29 Sep. 2022.

HILL, Dallas; O'CONNOR, Christopher D.; SLANE, Andrea. Police use of facial recognition technology: The potential for engaging the public through co-constructed policy-making. *International Journal of Police Science & Management*, Thousando Oaks, v. 24, n. 3, p. 325-335, 2022.

HOOD, Jacob. Making the body electric: The politics of body-worn cameras and facial recognition in the United States. *Surveillance & Society*, Chapel Hill, v. 18, n. 2, p. 157-169, 2020.

HUDOBNIK, Matthias M. Data protection and the law enforcement directive: A procrustean bed across Europe? *ERA Forum*, New York, v. 21, n. 3, p. 485-500, 2020.

JASSERAND, Catherine. Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680? *Computer Law & Security Review*, Amsterdam, v. 34, n. 1, p. 154-165, 2018.

JOH, Elizabeth E. The new surveillance discretion: Automated suspicion, big data, and policing. *Harvard Law & Policy Review*, Cambridge, v. 10, n. 1, p. 15-42, 2016.

KLÁTIK, Jaroslav; VAŠKO, Adrián. Using e-services in Slovak criminal proceedings. *Journal of Advanced Research in Law and Economics*, Craiova, v. 11, n. 3, p. 885-896, 2020.

KOKOTT, Juliane; SOBOTTA, Christoph. The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, Oxford, v. 3, n. 4, p. 222-228, 2013.

LEISER, Mark; CUSTERS, Bart. The Law Enforcement Directive: Conceptual challenges of EU Directive 2016/680. *European Data Protection Law Review*, Berlin, v. 5, n. 3, p. 367-378, 2019.

LEITNER, Christine (ed.). *eGovernment in Europe*: The state of affairs. Maastricht: European Institute of Public Administration, 2003.

LLEWELLYN, Karl N. *The bramble bush*: On our law and its study. Louisiana: Quid Pro, 2012. (Legal legends series). Available at: https://books.google.pt/books?id=ozEULgEACAAJ. Accessed on: 29 Sep. 2022.

LYNSKEY, Orla. Criminal justice profiling and EU data protection law: Precarious protection from predictive policing. *International Journal of Law in Context*, Cambridge, v. 15, n. 2, p. 162-176, 2019.

MEROLA, Linda M.; LUM, Cynthia. Emerging surveillance technologies: Privacy and the case of license plate recognition (LPR) technology. *Judicature*, Chicago, v. 96, n. 3, p. 119-126, 2012.

MILLARD, Jeremy. Government 1.5: Is the bottle half full or half empty. *European Journal of ePractice*, Brussels, v. 9, n. 1, p. 35-50, 2010.

NIELSEN, Morten Meyerhoff; JORDANOSKI, Zoran. Digital transformation, governance and coordination models: A comparative study of Australia, Denmark and the Republic of Korea. *In*: ANNUAL INTERNATIONAL CONFERENCE ON DIGITAL GOVERNMENT RESEARCH, 21., 2020, Seoul. *Proceedings* […]. New York: ACM, 2020. p. 285-293.

OLIVEIRA, Marcela. Desdobramentos da LGPD Penal. *LGPD Brasil*, São Paulo, 10 mar. 2022a. Available at: https://www.lgpdbrasil.com.br/desdobramentos-da-lgpd-penal/. Accessed on: 22 Sep. 2022.

OLIVEIRA, Marcela. LGPD penal e o que se sabe até agora. *Privacy Tech*, [*s. l.*], 3 mar. 2022b. Available at: https://privacytech.com.br/lgpd/lgpd-penal-e-o-que-se-sabe-ate-agora,411325.jhtml. Accessed on: 22 Sep. 2022.

RINGROSE, Katelyn. Law enforcement's pairing of facial recognition technology with body-worn cameras escalates privacy concerns. *Virginia Law Review Online*, Charlottesville, v. 105, p. 57-66, 2019.

RODOTÀ, Stefano. Data protection as a fundamental right. *In*: Gutwirth, Serge *et al*. (ed.). *Reinventing data protection?* Dordrecht: Springer Netherlands, 2009. p. 77-82.

SAVOLDELLI, Alberto; CODAGNONE, Cristiano; MISURACA, Gianluca. Understanding the e-government paradox: Learning from literature and practice on barriers to adoption. *Government Information Quarterly*, Amsterdam, v. 31, p. S63-S71, 2014. Supplemtent.

SEYYAR, M. Bas; GERADTS, Zeno J. M. H. Privacy impact assessment in large-scale digital forensic investigations. *Forensic Science International*: digital investigation, Amsterdam, v. 33, 200906, 2020.

SHEETZ, Michael. *Computer forensics*: An essential guide for accountants, lawyers, and managers. Hoboken: Wiley, 2007. Available at: https://books.google.ps/books?id=kYymPswUXrIC. Accessed on: 29 Sep. 2022.

SLOBOGIN, Christopher. Policing, databases, and surveillance. *Actual Problems of Economics and Law*, Kazan, v. 13, n. 1, 2019.

STOYKOVA, Radina *et al*. Legal and technical questions of file system reverse engineering. *Computer Law & Security Review*, Amsterdam, v. 46, 105725, 2022.

VOGIATZOGLOU, Plixavra; FANTIN, Stefano. National and Public Security within and beyond the Police Directive. *In*: VEDDER, Anton *et al*. (ed.). Security *and law*: Legal and ethical aspects of public security, cyber security and critical infrastructure security. Cambridge: Intersentia, 2019. p. 27-62.

WILLIAMS, Robin; JOHNSON, Paul. *Genetic policing*: The uses of DNA in police investigations. London: Willan, 2013.

YADAV, Saurav *et al*. Artificial intelligence: An advanced evolution in forensics and criminal investigation. *Current Forensic Science*, Sharjah, v. 1, e190822207706, 2022.

Referência bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

JORDANOSKI, Zoran. Citizens' right to privacy in data protection during criminal investigations in Brazil. *Revista do Ministério Público do Distrito Federal e Territórios,* Brasília, n. 12, p. 45-86, 2022. Anual.
