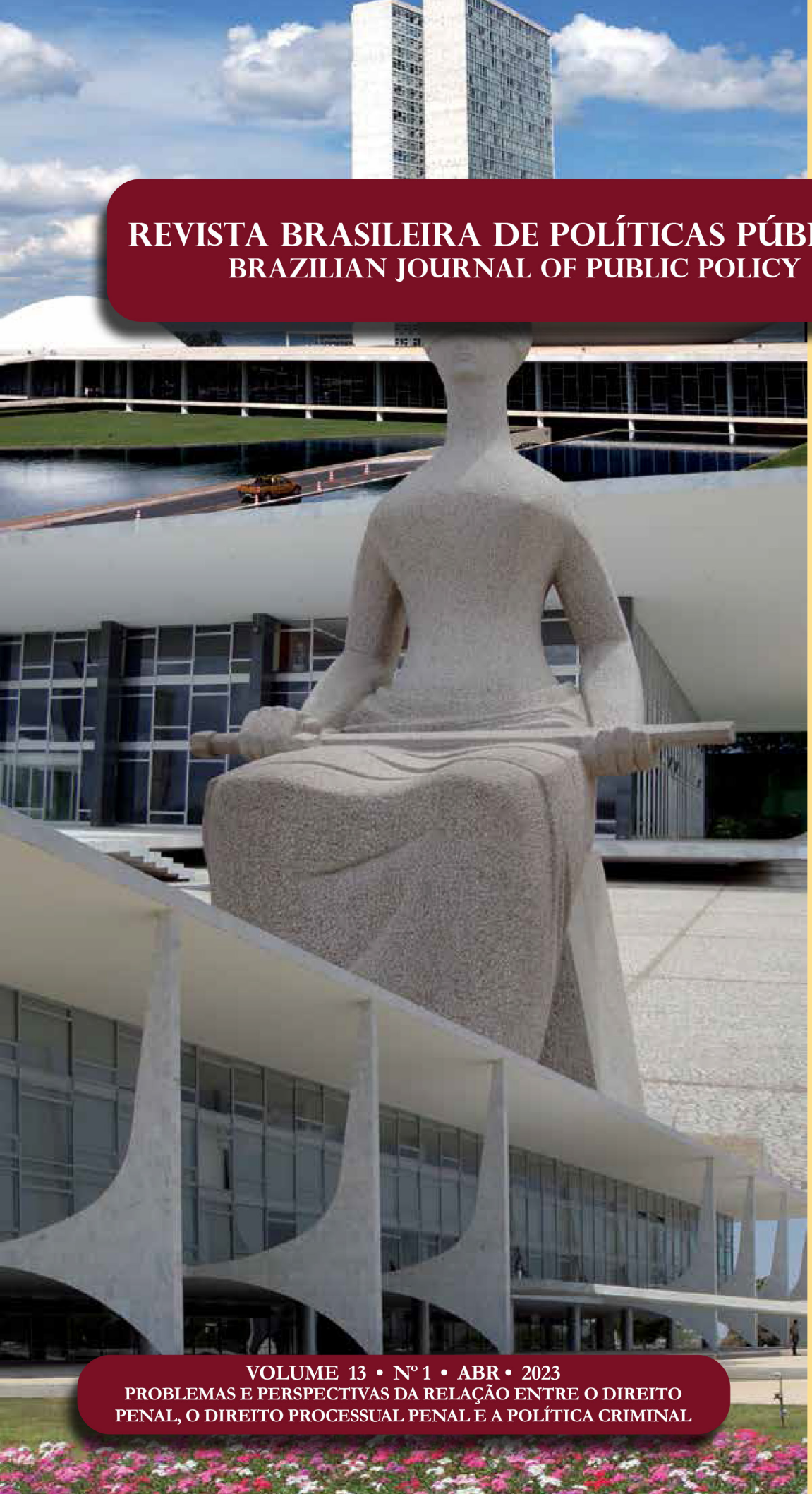

CEUB
EDUCAÇÃO SUPERIOR
ISSN 2236-1677

REVISTA BRASILEIRA DE POLÍTICAS PÚBLICAS
BRAZILIAN JOURNAL OF PUBLIC POLICY

The chinese ´sharp eyes´ system in the era of hyper surveillance: between state use and risks to privacy

O sistema chinês ´sharp eyes´ na era da hipervigilância: entre o uso estatal e os riscos à privacidade

Mateus de Oliveira Fornasier

Gustavo Silveira Borges

VOLUME 13 • Nº 1 • ABR • 2023
PROBLEMAS E PERSPECTIVAS DA RELAÇÃO ENTRE O DIREITO PENAL, O DIREITO PROCESSUAL PENAL E A POLÍTICA CRIMINAL

Sumário

doi: 10.5102/rbpp.v13i1.7997

The chinese ´sharp eyes´ system in the era of hyper surveillance: between state use and risks to privacy*

O sistema chinês ´sharp eyes´ na era da hipervigilância: entre o uso estatal e os riscos à privacidade

Mateus de Oliveira Fornasier**

Gustavo Silveira Borges***

Abstract

This article studies contemporary digital hyper surveillance and the ways through which citizens' sensitive data are collected and analyzed for different purposes, contextualizing it in the sharp eyes system, originated in China. As a hypothesis, it is assumed that society is mediated by networked information and communication technologies (ICTs). However, within such a digital life data is collected about users, which can serve various purposes (sometimes beneficial, other times harmful to fundamental rights, especially about privacy). With this, a data-based surveillance society is configured, in which the ways of obtaining data are complex and based on the growing and increasingly elaborate use of algorithms, with risks that are not always known by users when granting online permissions. Specific objectives: i) to describe technological forms of surveillance based on personal and behavioral data generated in individuals' online communications; ii) to understand how States and private organizations use electronic data surveillance; iii) to comprehend the use of a high-tech surveillance system by the Chinese State, the Sharp Eyes system. Results: i) the current society is interconnected through ICTs that satisfy the needs of individuals, but they do not understand the complexity of the online permissions they grant, nor the destination of their personal data; ii) public and private organizations and institutions use surveillance in the most varied ways, and algorithms are used to obtain, organize and access such data, but this can jeopardize several values associated with fundamental rights — but the sensitive design to these values, whose binding force must be established through public policies nationally and internationally, can mitigate or even solve the problems associated with such risks; iii) the Sharp Eyes program, which aims to inspect 100% of public space and transform people, residents, into agents of China's surveillance networks, serves to reflect on the (hyper)risks that can be seen impacting fundamental rights related to privacy.Methodology: hypothetical-deductive procedure method, with a qualitative approach and bibliographic review research technique.

Keywords: privacy; surveillance; sharp eyes.

* Recebido em 02/09/2021
Aprovado em 23/09/2022

** Professor do Programa de Pós-Graduação Stricto Sensu (Mestrado e Doutorado) em Direito da Universidade Regional do Noroeste do Estado do Rio Grande do Sul (UNIJUI). Doutor em Direito pela Universidade do Vale do Rio dos Sinos (UNISINOS), com pós-doutorado pela University of Westminster (Reino Unido). E-mail: mateus.fornasier@unijui.edu.br.

*** Professor do Programa de Pós-Graduação Stricto Sensu (Mestrado) em Direito da Universidade do Extremo Sul Catarinense (UNESC). Doutor em Direito pela Universidade Federal do Rio Grande do Sul (UFRGS), com Pós-Doutorado em Direito pela Universidade do Vale do Rio dos Sinos (UNISINOS) com bolsa de pesquisa PNPD/CAPES. E-mail: gustavoborges@hotmail.com.

Resumo

Este artigo estuda a hipervigilância digital contemporânea e a forma pela qual os dados sensíveis dos cidadãos são recolhidos e analisados para diferentes propósitos, contextualizando-o no sistema *sharp eyes*, proveniente da China. Como hipótese, tem-se que a sociedade é mediada por tecnologias de informação e comunicação (TICs) em rede. No entanto, dentro de tal vida digital são coletados dados sobre os usuários, que podem servir a vários propósitos (às vezes benéfico, outras vezes, lesivos aos direitos fundamentais, principalmente sobre a privacidade). Com isso, configura-se uma sociedade de vigilância baseada em dados, na qual as formas de obtenção dos dados são complexas e baseadas no uso crescente e cada vez mais elaborado de algoritmos, com riscos que nem sempre são conhecidos pelos usuários ao conceder permissões online. Objetivos específicos: i) descrever formas tecnológicas de vigilância a partir de dados pessoais e comportamentais gerados nas comunicações online dos indivíduos; ii) entender como Estados e organizações privadas se utilizam da vigilância de dados eletrônicos; iii) compreender o uso de um sistema de alta tecnologia de vigilância por parte do Estado Chinês, o sistema *Sharp Eyes*. Resultados: i) a atual sociedade está interligada mediante TICs que satisfazem necessidades dos indivíduos, mas estes não entendem a complexidade das permissões online que concedem, nem o destino de seus dados pessoais; ii) organizações e instituições públicas e privadas valem-se da vigilância das mais variadas formas, e algoritmos são utilizados para obtenção, organização e acesso a tais dados, mas isso pode colocar em risco vários valores associados a direitos fundamentais — mas o design sensível a esses valores, cuja obrigatoriedade deve ser estabelecida mediante políticas públicas nacional e internacionalmente, pode mitigar ou até mesmo resolver os problemas associados a tais riscos; iii) o programa Sharp Eyes, que visa inspecionar 100% do espaço público e transformar pessoas, moradores, em agentes das redes de vigilância da China, serve para refletir sobre os (hiper)riscos que podem ser visto impactando direitos fundamentais relacionados à privacidade. Metodologia: método de procedimento hipotético-dedutivo, com abordagem qualitativa e técnica de pesquisa de revisão bibliográfica.

Palavras-chave: privacidade; vigilância; *sharp eyes*.

1 Introduction

The classification of current society as being a digital one is frequent due to the ubiquitous mediation of new information and communication technologies (ICTs) in social, economic and knowledge production/dissemination relations, which makes ICTs to be used, too, in new forms of surveillance (LUPTON, 2015, p. 2-189). Such technologies, moreover, have been playing a fundamental role in the globalization process as a phenomenon characterized by the wide circulation of people, ideas and habits — and which, although it has not historically started with technologies, has developed at high speed through them (DE MUL, 2015, p. 106).

In English, the term surveillance is derived from the French verb *surveiller*, which, in turn, is related to the Latin term *vigilare*. Such a word is linked to verbs such as "to look", "to observe", "to supervise", "to control", "to inspect", "to monitor", "to keep" or even "to follow" (MARX, 2015, p. 735-737). Many of the examples to understand contemporary ways of obtaining information are based on cognitive skills using technological artifacts such as software and automated processes. However, such technical means can also involve sophisticated forms of manipulation with seduction, coercion, deception, unambiguous information and other special forms of observation. Surveillance has thus become more elusive over time, and may be seen as more difficult to defeat than before, after all many forms are so ubiquitous that they are generally assumed to be omnipotent.

Surveillance can succinctly take place on human routine, on the unconscious "autopilot" and, often, even on the biological instinct of sensory receptors ready to receive information from anyone who is territorially close (MARX, 2016, p. 16). These notions allow one to distinguish two forms of surveillance, at least: a traditional one and a new one. Traditional surveillance relies on unattended senses, and is characteristic of pre-industrial societies. With the development of numerical and written languages, as well as the evolution of distinct forms of social organization involving larger political entities, more complex and systematic forms of surveillance emerged, based on counting, recording, interrogation, information, infiltration, confessions and the expanded use of tests (MARX, 2016, p. 17). With the emergence of the industrial society, new surveillance and communication tools emerged, which improved the senses and cognition.

Visual content is generally an element of surveillance, even when it is not the initial means of data collection, and the new surveillance can be defined as scrutiny of individuals, groups and contexts through the use of technological means to extract, infer or create information (MARX, 2016, p. 19-20). Examples of it can be found in computer profiles, which have large data sets, video cameras, data about genomic analysis, geo-positioning (GPS), electronic monitoring, pharmacological tests and monitoring made possible by social media and cell phones. The new surveillance is, therefore, more intensive and extensive, expanding the meanings, reducing operating costs, reaching more remote locations and relying predominantly on aggregating data and big data. Thus, there is less visibility of their operations, which directly involve the involuntary compliance of the individual (MARX, 2015, p. 735-736).

The new surveillance (omni)present nowadays is the scrutiny of individuals and groups, through the use of highly sophisticated technological means, which are capable of extracting information unprecedentedly. In this sense, the use of technical means to extract and create information implies the ability to go beyond what is naturally offered to the senses and minds or what is voluntarily reported. The big data industry establishes a system in society, a system in which the world and life are transformed or mediated by data, and this fact constitutes a fundamental paradigm shift (BERALDO; MILAN, 2019, p. 01). The nature of databases is inherent to any software, which basically performs data programming that can be divided into four operations (DE MUL, 2015, p. 106): adding, searching, transforming and destroying data (which can be sorted by insert, select, update and delete options). Together, these commands constitute the dynamics of database ontology.

In that sense, studying the interfaces between technology, (hyper)surveillance activities and fundamental rights (especially with regard to security and privacy) has great social relevance — and for Social Sciences in general as well — as it contributes to the unveiling of a transformation perhaps still little explored in capitalism today, based on knowledge of the behavior of internet users against their moral decision-making capacity and their privacy — as it is not up to the individual to choose whether to share such data or not, they concern facets of their way of being that go beyond the conscious, penetrating even into the realm of desires and personal unnoticed attitudes. Legally, such a study is relevant because it is focused on forms of social communication and economic generation that challenge constitutionally established norms in every democracy: respect for private life and contractual adherence. Every social network, application and/or website that captures data exposes its intentions in electronic adhesion contracts that are so long and complex that it becomes impossible, in a normal daily life, to have enough time and knowledge to understand such obligations. All that scenario threatens rights, and it is aggravated by the fact that technological tools are increasingly more necessary for the realization of life in society, economic/labor activities, entertainment, etc.

On the Chinese case, it is known that the issue of data is also relevant for that country as their big data industry market was valued around US$ 2.5 billion in 2016 (LIANG *et al.*, 2018). On this issue, their government launched the Sharp Eyes program intending to connect public and private security cameras and integrate them into a national surveillance platform as well, including a facial recognition system enabled by AI to identify any citizen in order to promote greater protection (PANÍC, 2018). However, the issue of data

produced within that program crosses issues related to personal privacy and information security (LIANG *et al.*, 2018).

The main hypothesis of this research is that our society is mediated by (and, why not say, to a large extent, dependent on) networked information and communication technologies (ICTs): economic activities in general (supply of products, services, relationships of work and employment, etc.), education (and obtaining knowledge in general), interpersonal relationships, democratic procedures, conflict resolution... In short, practically everything that concerns life in society finds its virtual/digital correlate. However, within such a digital life — which, very significantly, reflects the personal behavior and sensitive data of users — data is collected about users, which can serve several purposes: sometimes beneficial to the users' interests; other times, harmful to their fundamental rights, especially with regard to their private lives. This sets up a scenario where a new form of surveillance gains space in society: surveillance based on data. Furthermore, the way to obtain data is complex, and is based on the growing and increasingly elaborate use of algorithms capable of collecting and organizing it — and the risks are not always known by users when granting online permissions when using applications or electronic devices.

In this sense, the general objective of this article, elaborated with case study method of procedure, qualitative approach, and literature review research technique, is to study contemporary digital surveillance, and how sensitive user data are collected and analyzed for different purposes. To achieve such a general objective, the article was divided into two sections. The first of them deals with the description of technological forms of surveillance based on personal and behavioral data generated in individuals' online communications. The second one, by its turn, seeks to understand how States and private organizations use electronic data surveillance. Finally, the third part studies the case of the "Sharp Eyes" Chinese surveillance system, which was highly developed in that social context, representing a serious threat to what is understood as the right to privacy.

2 Digital technologies and surveillance

The dynamics of databases is not necessarily digital: old telephone directories and printed indexes of the most varied natures are also ways of gathering, grouping and organizing data. However, digital databases are much more flexible, and easier to add information or delete it. In these media, data becomes increasingly essential for the repertoire of surveillance actions, through which several political disputes occur currently. Transforming data into data activism is a complex topic, in which data is defined based on their function or usefulness in people's lives; and the emphasis is on human/political destination, and not necessarily about its size (BERALDO; MILAN, 2019, p. 4). Currently, what is perceived is a sophistication in the ways of analyzing and operationalizing data so that they are used for specific purposes; in the same context, the technologies that collect data are capable of offering services to protect data and users (COWLS, 2018, p. 145).

Petzold (2015, p. 158) establishes notions about human algorithms, and how they are structured in "scaffolding". Such a metaphor is attributed to the fact that scaffolding suggests something that is constantly linked to ideas of combination, adaptation and replacement — since scaffolding is used to build something, generally. Thus, the fundamental tools for the progress of these social structures are the changes brought about by technological evolution. With data automation through the dependence of algorithms, it is possible to understand that there is a combination of elements that can serve different systems and applications that can later be recombined in different possible ways in the virtual environment.

De Mul (2015, p. 107-108), on the other hand, considers that what preponderantly differentiates Web 1.0 from 2.0 is not its social characteristic — after all, the first virtual applications already had possibilities for online interpersonal conversation — but rather, the presence of software capable of generating pages

through database entries where each fragment is ready to be reassembled again, allowing numerous recombinations and nested corrections; that is, Web 2.0 is based on data, not on pages. From these findings it is possible to understand that Web 2.0 operates through software processing rather than rendering files. Furthermore, in the era of big data, these databases are increasingly connected to each other and with connected data streams such as Google searches, social media interactions (Twitter, Facebook, Instagram, LinkedIn, Reddit, etc.) and online commerce. These big data-derived connections are tracked and used for real-time data mining and user profile configuration purposes by private and public organizations. From this same logic it can be inferred that, due to data from production processes, money transfers, GPS devices, surveillance cameras, biometric measurements and the use of smartphones and other locatable devices, a huge global database is being formed, and it will transform ways of life, work and thinking.

Such a scenario somehow includes numerous risk factors of the asymmetric infrastructure for data collection, a systematic distortion in data analysis and discriminatory ways in which the insights of algorithmic systems are deployed (COWLS, 2018, p. 145). Human language itself can be observed as a system of complex codes and, after all, it allows the continuity of productivity, which in its turn is equipped with technologies. Human algorithms also refer to impulses caused by current linguistic diversity, whose relationship with artificial languages is highly complex (PETZOLD, 2015, p. 160-162).

Language in the digital and technological context, as well as its translations, are capable of multiplying meanings, and also play significant roles in terms of the increase in the number of social networks available. However, there are several risks in this area, such as the delivery of unexpected results or economic uncertainties (PETZOLD, 2015, p. 166). The impact of databases is vast as well, since it is not limited only to the universe of computing, since they evoke acts in the material world. Examples of this are the biotechnological databases used for genetic engineering purposes, implementations in industrial robots and the profile detection system at airports, with the objective of identifying possible terrorists (DE MUL, 2015, p. 107). In theory, everything that can be identified through data becomes a control object of such databases.

Between human and computational power, such processes sometimes allow for an extension of the fundamentals of diversity, literally to new heights; but sometimes it triggers reverse effects (PETZOLD, 2015, p. 168). Digital media have resulted in new forms of participatory surveillance, as many websites and social networks offer users the opportunity to upload images, videos, files and textual information about themselves and others around them, for third parties to have access. The purpose of such platforms is in fact to keep such a content under the scrutiny of other people, thus fulfilling the desire to be seen, self-promotion and the sharing of information and observations about the other (LUPTON, 2015, p. 177).

Celebrities, politicians, and other public figures, are subject to constant monitoring (whether in public or private life), and the great facilitators of such an exhibition are not just the paparazzi — after all, anyone with a mobile device can instantaneously broadcast footage alive. In these cases, it is clear that there is an incidence of participatory synopticons linked to surveillance and its ways of operating. Human identity consists of several heterogeneous elements that often conflict with each other, and one express oneself in everyday interactions, through clothing, routines, and "likes", and this denotes the construction of the individual's "self-image" (DE MUL, 2015, p. 99-100).

All those who are currently users of social media can engage in self-surveillance practices (LUPTON, 2015, p. 178-179) — after all, they are able to manage the content they are going to publish and thus, consequently, to present a certain type of desired identity. Individuals in general can exert a high degree of relevance in social media in terms of the viewer's gaze; great profiles with many followers, celebrities, and even world leaders, have control over the content they generate and disseminate on social networks; however, in contrast, they place themselves as objects of other people's gaze, being targets of intense scrutiny derived from the notions of surveillance and synoptic observation.

When one works with the theme of technology and what emerged from it, given its wide scope for destinations, it may primarily seem that technology is not compatible with human empathy — which is considered a very human skill, and indeed there is no denying that computers are considered a true antithesis of empathic thinking, and this is capable of being reflected in our language (CRAIG; SEÏLER, 2016, p. 57).

When a person lacks empathy, he/she is usually described as a "robot" or "machine", cold and calculating, after all empathy is part of what seems to be the concept of being human. On the other hand, an emotional computer may also be seen as an undesired thing, as it is known that computers are able to process data faster and perform calculations based on information for humans. Thus, human apprehension about computers capable of emulating the greatest human abilities may be considered a natural fact, so that they do not exceed our position of authority. Currently, self-tracking cultures have emerged in a sociocultural context, in which various reasons, discourses and technological practices that are converging with each other are based. In a way, this includes complex concepts such as self-knowledge, self-awareness and self--entrepreneurship (LUPTON, 2016, p. 113). Thus, a social and political environment is established in which the ability of digital technologies to monitor a growing variety of aspects of the human body, behaviors, habits and environments is disseminated in virtual environments through new surveillance technologies, which in turn are diversified.

Applications on mobile phones have been available on the market for over a decade already, and classically were presented by Apple in 2008 through its online store (App Store) and soon this feat was followed by Google's app store (the Google Play). Today, each of these online stores offers millions of apps of the most diverse genres, with a wide variety of purposes and functions, and among them, health-related apps comprise a widely searched key category (LUPTON, 2019, p. 2). In that sense, children become increasingly data-powered through technologies such as mobile media, social media platforms and educational software, and data generated by these technologies is often used for surveillance or for monitoring and evaluating such technologies of those young people, by themselves or by others, which may include recording and evaluating details about appearance, growth, development, health, social relationships, mood, behavior, educational standards and assessments, among others (LUPTON; WILLIAMSON, 2017, p. 781).

For many users of such technologies, it is evident that biographical, embodied, interpersonal and situational elements of their lives provide a basis for the desire to closely monitor their behavioral aspects and the motivation to continue. Thus, it was evident for Lupton (2019, p. 7) in her field research that people who use automatic tracking practices are imbued with emotion, after all the pleasure and satisfaction resulting from these practices are essential to continue with them as part of of their daily routines. In that same research, it was clear that such applications operate as ways for the agent to "feel more in control" and to better deal with risks, anxieties and fears and uncertainties about their future.

There are countless "smart" devices able to help the individuals to self-monitor in their daily lives; cars are currently able to monitor driving habits and drowsiness, alerting drivers, for example, if they are at risk of falling asleep at the wheel. Specific mattresses already monitor sleep patterns and body temperature; chairs can detect physical movement and "smart" shoes and clothing can record activities and other physical data (LUPTON, 2016, p. 105).

Moreover, "smart" residences already use sensors to monitor their users' movements, and "smart meters" track household energy use. In fact, the term "smart cities" is often used to define data captured by smart objects located in public spaces and used for personal reasons in private areas; while "smart schools" use predictive learning analytics to profile data on individual students in many European countries to achieve certain educational purposes. With these points highlighted, it is evident that digital technologies as a whole are in growing expansion and are part of the daily routine of millions of people, even if they are not aware of it (LUPTON, 2015, p. 188). Such technologies are intimately linked to the social construction of the individual and their other relationships, whether they are loving, professional, family, with space and even with the environment.

3 On the use of data for surveillance by States

The use of data from government, security, commercial and even criminal agencies — so that such information obtained by automatic tracking can be mobilized for their own purposes — are classic examples of monitoring, which arrive in the hands of the private initiative or even ordinary individuals with the advent of new forms of screening, with only one smartphone in the hands (LUPTON, 2016, p. 114). Surveillance as such is not ontologically good or bad: context and behavior characterize it in one way or another (MARX, 2015, p. 734), and the same can be said to the concept of privacy. Context refers to the type of institution, organization, and its objectives, rules and expectations; and behavior refers to the type of behavior that expected — whether based on the law or in less formal cultural expectations.

Differences in surveillance contexts involving coercion (government), assistance (parents and children), contracts (work and consumption) and accessible and free personal data (personal and private in public) need to be considered — after all, surveillance is about a generic process which is typical of living systems with information borders, not only something restricted to governments, espionage or secrecy. And so, surveillance and privacy are not always opposed, being that the second one can be a means of ensuring the first. Despite the media attention to problems associated with inadequate surveillance (mainly by government) is present, there are also problems associated with failure to use surveillance when appropriate (MARX, 2015, p. 734).

There is much potential for vigilance by algorithms to undermine human values considered important for both end users and data holders (HAYES; VAN DE POEL; STEEN, 2020), such as privacy. And adverse privacy implications represent problems to be addressed during design, implementation and deployment and are not insurmountable challenges. This demonstrates the importance of values sensitive design (VSD) and incorporation of values within the design process. The challenge of designing algorithms that maximize their contribution to human evolution in the context of justice and safety without causing damage should not be lightly faced, but rewards are potentially large. Lives and properties can be protected if the design, implementation and deployment of algorithms is executed effectively and ethically. These challenges will not always be possible to be solved with mathematical solutions, as some problems require philosophical deliberation.

Studies on surveillance has had significantly increased attention through scholars after 9/11, although they have been through significant research interests since the 1950s at least; and has happened because of the greatest awareness of human rights and abuses caused by colonialism, fascism and communism as well as antidemocratic behavior even in democratic societies (MARX, 2015, p. 734-735). It should be noted that surveillance, particularly because of its íntimos involvement with States and their organizations, plays a significant role in private social. And its applications happen in different circumstances, and in this systematics it is necessary to understand that such a concept is propagated through different forms of power.

Control and domination are typical central goals for human surveillance with regard to protection or entertainment, and the authorities concerning to that logic and their power relations are intimately related to the ability of agents to collect and use data — after all, access and use of information are propor elements of democratic societies (MARX, 2015, p. 735-736). Scanned automatic tracking technologies promote a data surveillance culture (LUPTON, 2016, p. 102-103), and so, a distinction must be distinguished between the type of data surveillance realized for self-tracking and other forms of surveillance that use monitoring technologies. For example, several data surveillance activities monitor people in ways they do not know, such as cameras of closed internal television circuit, monitoring through people's movement sensors in public spaces, surveillance done national security agencies and even policing organs that use commercial data from Internet companies.

The potential of Big Data grows daily and, because of that, such a technology may now be used to map gangs in the US, due to past (and present) terrorist mapping (FERGUSON, 2017). Large-scale DNA databases, iris exams, photographies and several forms of biometrics can now exponentially capture more personal data. All these development techniques encouraged interest in Big Data policing. Although the underlying goal of collecting, cataloging and using data on criminal agents is as old as policing, new technological tools make this work increasingly easy and efficient. In turn, police and public administrators are increasingly interested in the possibilities of hi-tech surveillance, and this belief has generated enthusiasm, innovation and faith in data-oriented ways of future. Each of these factors increases the argument that data-oriented policing can help turn the page at a time of crisis in law enforcement. For police chiefs, Big Data policing offers an escape, a talk point to change the conversation from the past to the future. For the community, Big Data offers a more objective way to solve the very human problem of biased policing. For the media, it offers numerous news worthy of tinnitus on the futuristic policing analog to those in *Minority Report*. And for technologists, it offers a new world of opportunities and innovation.

The use of cybernetic technology generally implies an exchange, as well as the export of technology to several other countries. Thus, cybernetic surveillance technologies may be used in such a way that compromises human rights, especially the right to privacy and freedom of expression (KANETAKE, 2019a, p. 16). Cybernetic technology exportation may bring benefits or malefits, as intended for specific countries. A good example of that is the export of computers used to intercept private online communications. Such an artifact may serve the State, and thus police agencies are able to detect fraudulent transactions, and thus, to prevent organized crime. However, on the other hand, this same computer can also be used to suppress freedom of expression and the right of privacy of the intercepted ones (KANETAKE, 2019a, p. 2).

There are already several international guidelines, including UN guiding principles for business and human rights, which are expected to take account of human rights and carry out due diligence in human rights. Proposals about duty-based data export control have established an environment where various social sectors and stakeholders may dialogue about to what extent human rights can be accommodated in the export of control practices (KANETAKE, 2019a, p. 16).

Soon after the Arab Spring, the political climate in the European Union (EU) has led to legislative reforms with regard to better human rights risk management of ICT exports. In 2015 the European Parliament repeatedly denounced the need to regulate the export of human rights-sensitive cyber technology, and the proposal regulates the cross-border transfer of items that meet "civil and military purposes." Within the EU, the export of double-use items was governed by the Council Regulation, 428/2009, of May 5, 2009, which is an integral part of the Common Committee of the European Union (KANETAKE, 2019b, p. 156).

In response to the Appeal of the European Parliament, the European Commission submitted, in September 2016, the proposal to reformulate the current dual-use regulation of the European Union. In short, the Commission proposal places human rights as one of the fundamental pillars of the dual use and control of data export. Its biggest hindrance, however, is in the fact that export control has basically developed to cushion military risks, especially in regard to what involves the proliferation of chemical, biological and nuclear weapons.

Legal instruments for data protection and user privacy are thought by legislators around the world, and they must enable individuals to have a legally supported solution for each violation of their right to privacy. Among these, it is still discussed the following problematic: to include or not a right to be forgotten in such a role; more specifically, the convenience of granting a right to oblivion, independently of any infringement of informational identity, thus giving individuals a prerogative to erase the traits of their past in order to prevent others from accessing it and knowing it (DURANTE; PAGALLO, 2014, p. 28).

4 'Sharp Eyes', the (hyper)surveillance system in the Chinese context

In 2005, the Chinese government launched the *skynet* project to address urban public security needs by installing video surveillance equipment in public places such as traffic lanes and security checkpoints (WANG, 2021). Currently, China already has more than 200 million surveillance cameras spread across its territory. Since 2015, that surveillance system has had 100% coverage in Beijing (CUSTES, 2015), Shanghai and Guangzhou (WANG, 2021). Surveillance cameras detect and recognize pedestrians in real time, also identifying their age, gender and clothes. Technology can also identify vehicles. In addition, the system shows the matching level of an individual's image with personal information specified in the database in real-time. This tracking and recognition technology helps police officers find criminals (CHINA DAILY, 2017). The government project's slogan has become "20 million cameras protecting you, leaving criminals nowhere to hide" (WANG, 2021). The result is a decrease in the crime rate of 42.7% between 2012 and 2016 for eight types of crimes, including drug trafficking, theft and intentional bodily harm in China (YU, 2017). But this surveillance system is concentrated in large urban spaces, where funding and population density facilitate centralized surveillance (GERSHGORN, 2021).

Chinese Government started the implementation of a surveillance camera system with facial recognition in 2010, but it has been since from 2015 that the Sharp Eyes Project has been developed by the National Development and Reform Commission (QIANG, 2019). Its main objective is to implement ubiquitous surveillance in the country (ROLLET, 2018) — noting that, as of 2017, China already had 176 million cameras installed on its streets as part of the Skynet project (QIANG, 2019).

The term sharp is used in order to refer to the authoritarian implement as opposed to the so-called soft power. Its main characteristic is the acute/pervasive power of authoritarian regimes through manipulation techniques (WALKER; LUDWIG, 2017). Other researchers claim that the term refers to the phrase "people have penetrating eyes" by Mao Tse-Tung (GERSHGORN, 2021).

The novelty about the program was represented by advances in the learning algorithms for facial and vocal recognition — from which the code would be able to determine the sex of people in the frame of real-time monitoring cameras, in addition to recognizing characteristics of their clothes and vehicles, and the number of people in a given location (QIANG, 2019). In 2012, a public-private partnership project between the Chinese government of Anhui and the iFlytek company collected around 70,000 voice samples for tests carried out in 2017. The tests resulted in automatic detection of voices through individual phones and, according to Chinese government reports, they will be used for stability and counterterrorism purposes (HINCKS, 2017).

Despite the advances in technological preparation, only in 2015 the Chinese government started implementing Sharp Eyes (Xueliang) Project, as part of the 13th five-year plan for 2016-2020 (GERSHGORN, 2021). In order to be implemented, the selected location is divided into grids for organizational delimitation purposes; the place is then flooded by surveillance cameras made publicly available through the WeChat application to residents within pre-established boundaries so that a kind of self-surveillance and local monitoring is carried out.

To better illustrate, a Chinese article describes the implementation of the Sharp Eyes project in Pingyi County, popularly known as an unsafe area, that presented high crime rates, extreme poverty and lack of public safety: with the advent of the Xueliang project its about 1 million residents (and only 321 police officers) described enthusiastically their experiences about the opportunity to watch over their neighbors. One of the villagers reported that he noticed a manhole cover collapse; another noticed and denounced a suspicious marketing group meeting in a local building, among others (SHUJIN, 2016).

According to the Chinese government, in 2015, avoidable public safety cases in that city dropped by 48%, and people's satisfaction with the public safety environment greatly increased. The project is sup-

ported by surveillance cameras throughout the city, but instead of presenting only police and automated facial recognition algorithms monitoring, residents also have access through special TVs installed in their homes and smartphones, and when they see something suspicious, they should press a button to call the police. However, what is reported to the police by the Sharp Eyes program is not limited only to crime. The principle is to divide the city or town into a grid, and each square in the grid acts as its own administrative unit. However, depending on the needs of the city, the project may work differently, in adaptive manners (GERSHGORN, 2021).

In that intense scenario of surveillance and data collection, individuals are more exposed to violations of their fundamental rights; self-determination and free personality development suffer limitations when opposed to social and collective values derived from Confucian ideology/philosophy. So it is a next step in the history of regulating the right to privacy in China and the West.

The Chinese government has already announced in the 14th Five-Year Plan (2021-2025) that they ought to emphasize social governance to local municipalities through the network system, as well as build even more security projects, to "strengthen the construction of the prevention and control system for the safety public" (GERSHGORN, 2021).

Western news sometimes criticize the system on the grounds that it is used as a form of social control, an Orwellian nightmare to be feared for because of the massive amounts of data that individuals constantly generate, and for processing it to deliver a quantified score that creates an ideological vision, like a straitjacket for every Chinese citizen (JINWOO, 2017). On the other hand, in a survey conducted by The Washington Post in 2018 involving the opinions of 2,209 Chinese citizens and dozens of in-depth interviews about different types of social credit systems in China, it was found that the majority of Chinese approve that system. In total, 80% of respondents approve of the systems, with only 1% reporting strong or moderate disapproval. And only 1% believe that a national social credit system should not be implemented. Respondents (59%) also demonstrated strong confidence in the Chinese central government, reporting a desire for a unified and managed social credit system (CAGE, 2019). It is important to highlight that most of those in favor of this system belong to the group of wealthier and better educated urban residents, in addition to the elderly. Their justifications are embodied, first, in the increase in benefits that provide more advantages to the richest, such as quotas for buying cars without deposits and quick check-ins at hotels. Second, this group tends to perceive social credit systems less as an instrument of state surveillance and more as a means of improving quality of life and what they consider to be honest and law-abiding behavior in society (CAGE, 2019).

During a lecture at the China Development Forum in Beijing in 2018, the CEO and co-founder of internet giant Baidu, Robin Li, issued a controversial statement that the Chinese seem more willing to trade privacy for personal safety, convenience and effectiveness. Despite causing unrest (CHENYU, 2018), the Chinese public is generally pleased that their personal safety is assured, but at the same time, they are concerned about their privacy, according to an online survey conducted by People's Weekly (WANG, 2021). Citizens are challenging the legitimacy of the system, including in lawsuits over the excess collection and abuse of personal data through facial recognition and other forms of surveillance technology during the COVID-19 epidemic (HORSLEY, 2021).

But China still does not have complete and comprehensive regulations on information collection (WANG, 2021). In the country's Constitution, only the privacy of personal mail is protected (art. 40). However, the first Chinese Civil Code , enacted in 2020, deals with the protection of privacy in personality rights, defined in its art. 1.032 as, in addition to the non-disruption of private life, the "private information that one does not want others to be known". The following article of the Code, in its turn, prohibits any organization or individual from processing other individuals' personal information. And State bodies and regulated institutions that assume administrative functions must keep confidential the private and personal

information of natural persons known to them during the performance of their responsibilities, and must not unlawfully disclose or provide to third parties, according to article 1039 of the Code.

In an informational country, the Chinese government has an urgent need to fill the regulatory gaps about the issue of personal data gathering. Therefore, the first Personal Information Protection Act[1] is being drafted to regulate the collection, storage, use, processing, transmission, provision and disclosure (collectively, "handling") of personal information by "organizations and individuals". The drafts impose personal information handling requirements on companies and "state agencies" alike. Horsley (2021) asserts that the draft suggests that China is taking the protection of personal information seriously and establishing legal checks related to the government authority for common operations.

5 Conclusion

This article mainly aimed to study contemporary digital hypersurveillance and the way through which citizens' sensitive data are collected and analyzed for different purposes, contextualizing it in the Chinese Sharp Eyes system.

The specific objective of its first section was, therefore, to describe technological forms of surveillance based on personal and behavioral data generated in individuals' online communications. In this regard, it can be concluded that the current society is interconnected in its most diverse spheres due to digital technologies that serve as a means to satisfy the most diverse needs of individuals who communicate in such a social environment. And while users are often aware of the risks associated with using these devices, they don't understand the complexity of such online permissions they grant, nor the destination of their personal data. Furthermore, "surveillance" is a terminology that did not emerge with the digitization of technologies, but was equipped with such an advent when expanded by such means. Not only security cameras and establishments are able to capture images and sounds, after all, applications and mobile devices are the most common among technological devices today.

The second specific objective of this work was to understand how States and private organizations use electronic data surveillance. Therefore, it was possible to conclude that public and private organizations and institutions use surveillance in the most varied ways — from government coercion, through forms of assistance and service provision, establishment of contracts, reaching access and processing of data provided free of charge in the public and private spheres. Algorithms are used to obtain, organize and access such data, but this can put several values associated with fundamental rights at risk, especially those associated with the privacy of individuals. A design sensitive to these values — a set of techniques for building and using such algorithms — can mitigate or even solve the problems associated with such risks. But the obligation of such techniques must be established through well-established public policies, not only internally, but mainly internationally, since such technologies are usually developed in some national scenarios, but are exported to several other countries, where often the constitutional values Constitutions can differ greatly.

Finally, the specific objective of the third section of its development was to understand the use of Sharp Eyes, a high-tech surveillance system used by the government of the People's Republic of China. In this sense, the Chinese mass hyper surveillance system was built through preventive and repressive apparatuses for the existence and maintenance of public security — which can be considered the main fundamental value of Chinese society. For the Western World, this hyper-surveillance project may cause estrangement, even

[1] Chinese Personal Information Protection Law (PIPL) was enacted in September 2021 and brings personal information as subjects of protection, which are data that can be used to identify a specific person, but such data are not generalized (CAI; CHEN, 2022). Thus, PIPL can apply to Sharp Eyes related issues and surveillance camera issues as they deal with data that is strictly personal (such as physical appearance).

be associated with dystopian future scenarios. However, in the Chinese context, it is a current reality that is already in full implementation, that is, "surveillance" mechanisms are adopted by the government with the objective of seeking the collective security of Chinese citizens.

Thus, the "Sharp Eyes" program, which aims to inspect 100% of public space and transform people, residents, into agents of China's surveillance networks, serves to reflect on the (hyper)risks that can be seen impacting fundamental rights related to privacy.

The results above confirm the hypothesis initially formulated. It is clear that a surveillance society is being configured based on data obtained in complex and algorithmic ways, which poses risks to fundamental rights, risks that are not always known to users who grant online permissions. However, there are possibilities for the development of public policies at the domestic and international levels, based mainly on the establishment of a design that is sensitive to values related to human rights. It is clear that this development is extremely complex — mainly due to the mismatch between the rhythms of technological innovation and the democratic establishment of regulatory policies — but this is the beginning of the discussion of possibilities for that.

References

BERALDO, Davide; MILAN, Stefania. From data politics to the contentious politics of data. *Big Data & Society*, v. 6, n. 2, p. 1-11, 2019.

CAGE, Monkey. *What do people in china think about 'social credit' monitoring?*. The washington post, 2019. Available at: https://www.washingtonpost.com/politics/2019/03/21/what-do-people-china-think-about-social-credit-monitoring/. Access on: 27 May 2021.

CAI, Peiru; CHEN, Li. Demystifying data law in China: a unified regime of tomorrow. *International Data Privacy Law*, 2022.

CHENYU, Liang. Are chinese people 'less sensitive' about privacy? *Sixth tone,* 2018. Available at: https://www.sixthtone.com/news/1001996/are-chinese-people-less-sensitive-about-privacy%3F. Access on: 27 May 2021.

CHINA. *Civil Code*. 2020. Available at: http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf. Access on: 27 May 2021.

CHINA. *Constitution of the People's Republic of China*. 1982. Available at: http://www.npc.gov.cn/zgrdw/englishnpc/Constitution/2007-11/15/content_1372964.htm. Access on: 27 May 2021.

CHINA'S Skynet Project finds people in minutes. *China daily*, 2017. Available at: http://www.chinadaily.com.cn/a/201712/12/WS5a2fa4f7a3108bc8c6727f5c.html. Access on: 27 May 2021.

COWLS, Josh. Privacy risks and responses in the digital Age. *In*: ÖHMAN, Carl; WATSON, David (org.). *The 2018 yearbook of the digital ethics lab.* Oxford: Springer, 2018. p. 113-148.

CRAIG, Paul; SEÏLER, Néna Roa. Empathetic technology. *In*: TETTEGAH, Sharon Y.; NOBLE, Safiya Umoja (org.). *Emotions and technology:* communication of feelings for, with, and through digital media. London: Elsevier Academic Press, 2016. p. 55-81.

CUSTES, C. *Skynet achieved:* Beijing is 100% covered by surveillance cameras, and nobody noticed. Techinasia, 2015. Available at: https://www.techinasia.com/skynet-achieved-beijing-100-covered-surveillance-cameras-noticed. Access on: 27 May 2021.

DE MUL, Jos. database identity: personal and cultural identity in the age of global datafication. *In*: DE BEEN, Wouter; ARORA, Payal; HILDEBRANDT, Mireille (org.). *Crossroads in new media, identity and law:* the shape of diversity to come. Houndmills: Palgrave Macmillan, 2015. p. 97-118.

GERSHGORN, Dave. *China's 'sharp eyes' program aims to surveil 100% of public space*. 2021. Available at: https://onezero.medium.com/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space-ddc22d63e015. Access on: 27 May 2021.

DURANTE, Massimo; PAGALLO, Ugo. Legal Memories and the Right to be forgotten. *In*: FLORIDI, Luciano. *Protection of information and the right to privacy:* a new equilibrium? Cham: Springer, 2014. p. 17-30.

FERGUSON, Andrew G. *The rise of big data policing***:** surveillance, race, and the future of law enforcement. New York : New York University Press, 2017.

HAYES, Paul; VAN DE POEL, Ibo; STEEN, Marc. Algorithms and values in justice and security. *AI & Society*, 2020.

HINCKS, Joseph Hincks. China is creating a database of its citizens 'voices to boost its surveillance capability: report. *TIME,* 2017.

HORSLEY, Jamie. How will China's privacy law apply to the chinese state?. *Brookings Institute,* 2021. Available at: https://www.brookings.edu/articles/how-will-chinas-privacy-law-apply-to-the-chinese-state/. Access on: 27 May 2021.

JINWOO, K. Orwell s nightmare: China's social credit system. *The Asian Institute for Policy Studies*, v. 28, 2017. Available at: http://en.asaninst.org/contents/orwells-nightmare-chinas-social-credit-system/. Access on: 27 May 2021.

KANETAKE, Machiko. The EU's dual-use export control and human rights risks: the case of cyber surveillance technology. *Europe and the World*: a law review, v. 3, n. 1, p. 1-16, 2019a.

KANETAKE, Machiko. The Eu's export control of cyber surveillance technology: human rights approaches. *Business and Human Rights Journal*, v. 4, n. 1, p. 155-162, 2019b.

LIANG, Fan *et al*. Constructing a data driven society: China's social credit system as a state surveillance infrastructure. *Policy & Internet*, v. 10, n. 4, p. 415-453, 2018.

LUPTON, Deborah. *Digital sociology*. New York: Routledge Taylor & Francis Group, 2015.

LUPTON, Deborah. The diverse domains of quantified selves: self-tracking modes and dataveillance. *Economy and Society*, v. 45, n. 1, p. 101-122, 2016.

LUPTON, Deborah. Data mattering and self-tracking: what can personal data do? *Continuum:* Journal of Media & Cultural Studies, 2019a.

LUPTON, Deborah. "It's made me a lot more aware": a new materialist analysis of health self-tracking. *Media International Australia,* v. 171, n. 1, p. 1-14, 2019b.

LUPTON, Deborah; WILLIAMSON, Ben. The datafied child: the dataveillance of children and implications for their rights. *New Media & Society,* v. 19, n. 5, p. 780-794, 2017.

LUPTON, Deborah; MICHAEL, Mike. 'Depends on who's got the data': public understandings of personal digital dataveillance. *Surveillance & Society,* v. 15, n. 2, p. 254-268, 2017.

MARX, Gary T. Surveillance studies. *In*: SMELSER, Neil J.; BALTES, Paul B. (ed.). *International Encyclopedia of the Social & Behavioral Sciences*. 2. ed. Oxford: Elsevier, 2015. p. 733-741.

MARX, Gary T. *Windows into the soul:* surveillance and society in na age of high technology. Chicago: The University of Chicago Press, 2016.

PANIĆ, Ilja. *China's all-seeing 'Sharp Eyes'*. 2018. Available at: https://iljapanic.com/essays/china-sharp-eyes/. Access on: 28 Aug. 2022.

PETZOLD, Thomas. Human-algorithmic scaffolding *In*: DE BEEN, Wouter; ARORA, Payal; HILDEBRANDT, Mireille (org.). *Crossroads in new media, identity and the law:* the shape of diversity to come. Houndmills: Palgrave Macmillan, 2015. p. 156-176.

QIANG, Xiao. The road to digital unfreedom: president Xi's surveillance state. *Journal of Democracy*, v. 30, n. 1, p. 53-67, 2019.

SHUJIN, Wang. 临沂“雪亮工程”:治安防控 群众真正参与进来. 2016. Available at: https://archive.li/7gpbm. Access on: 27 May 2021.

WALKER, Christopher; LUDWIG, Jessica. From 'soft power' to 'sharp power': rising authoritarian influence in the democratic world. *National Endowment for Democracy*, 2017.

WANG, Wendi. *Surveillance madness:* the future of China? Available at: https://mfadt.parsons.edu/darkdata/surveillance-madness.html. Access on: 27 May 2021.

YU, Zhang. Facial recognition, AI and big data poised to boost chinese public safety. *Global times*, 2017. Available at: https://www.globaltimes.cn/content/1070546.shtml. Access on: 27 May 2021.

王淑静. 临沂“雪亮工程”:治安防控 群众真正参与进来了. China Peace, 2016. Available at: https://archive.li/7gpbm. Access on: 27 May 2021.

最高法打造“天网”破解执行难 去年615万老赖被“限行”. 中国网. Available at: https://www.creditchina.gov.cn/lianhejiangcheng/lianhejiangchenganliguiji2/201712/t20171221_103496.html. Access on: 27 May 2021.

Para publicar na revista Brasileira de Políticas Públicas, acesse o endereço eletrônico www.rbpp.uniceub.br
Observe as normas de publicação, para facilitar e agilizar o trabalho de edição.