The use of AI in digital health services and privacy regulation in GDPR and LGPD

Between revolution and (dis)respect

MATEUS DE OLIVEIRA FORNASIER

Abstract: This article studies the complexity of protecting personal data in the face of the challenges and risks that data collection and processing by AI offer to the fundamental right to privacy. Its hypothesis is that the General Data Protection Regulation (GDPR) and the Brazilian General Data Protection Law (LGPD) are not sufficient to cover several of the problems that emerge from the capture and treatment of sensitive data by companies that develop devices and services based on AI, although such laws have many important points for the regulation of such activities. Thus, new dialogic understandings, in addition to State regulatory efforts, must be developed. Methodology: hypothetical-deductive procedure method, with a qualitative approach and bibliographic review research technique.

Keywords: artificial intelligence; digital health; privacy; GDPR; LGPD.

O uso da IA em políticas públicas de saúde e a regulação da privacidade na GDPR e na LGPD: entre a revolução e o (des)respeito

Resumo: Este artigo estuda a complexidade da proteção de dados pessoais ante os desafios e riscos que as atividades de captação e tratamento de dados por IA oferecem ao direito fundamental à privacidade. Sua hipótese é de que o General Data Protection Regulation (GDPR) e a Lei Geral de Proteção de Dados (LGPD) brasileira não são suficientes para abarcar vários dos problemas que emergem da captação e tratamento de dados sensíveis por empresas que desenvolvem dispositivos e serviços embasados em IA, apesar de essas leis conterem muitos pontos importantes para a regulação de tais atividades. Assim, novos entendimentos dialógicos, para além dos esforços estatais de regulação, devem ser desenvolvidos. Metodologia: método de procedimento

Recebido em 30/6/21
Aprovado em 5/10/21

hipotético-dedutivo, com abordagem qualitativa e técnica de pesquisa de revisão bibliográfica.

Palavras-chave: inteligência artificial; saúde digital; privacidade; GDPR; LGPD.

1 Introduction

Rising costs of healthcare services, easier access to the internet, and a current cultural desire to self-manage health problems have led individuals to undertake some medical activities on their own with the help of electronics. To find a cancer, for example, there are currently several apps that allow one to use a smartphone to detect high odds of cancer simply by taking a picture of a suspect skin area – the UMSkinCheckApp app, developed at the University of Michigan (USA), is an example of a free tool for that. Generally, these applications depend on AI – which, in the diagnosis of skin cancer, can be more accurate than human physicians (TSCHIDER, 2020).

Due to its enormous ability to identify probabilities in datasets, AI has been used to solve some of the most complex health challenges. This technology can revolutionize home care for the elderly, allow to reduce nursing home costs, and improve quality of life for those patients. It can also improve diagnostic processes for rural, general, or low-resource physicians whose patients may not have access to specialists. It also allows the automation of low-risk healthcare tasks, freeing doctors to focus more energy on complex cases. That is, AI can provide a better quality of life by separating patients from physicians in relation to chronic, time-consuming and low-adherence tasks, such as diabetes control – where data is captured by wearables (such as smartwatches) and by devices monitorable via smartphone.

But as AI is integrated into medicine, a number of crucial challenges arise, especially in relation to data acquisition, the reporting based on it, and possible re-identification of patient data. Furthermore, cases of companies crossing ethical boundaries seeking for patient data to train their systems have been recently reported: one of them concerns to the partnership between the Royal Free NHS Foundation Trust and Google subsidiary DeepMind, which was considered illegal by the regulatory body of data protection of the UK, and was terminated due to insufficient patient informed consent regarding secondary use of private data –

and this example demonstrates the apparent struggle between regulators and industry over the prospecting of medical data for training algorithms. The most recent uses of AI allow the transfer of responsibility for care and monitoring from health professionals to the patients themselves. In addition, advanced AI is being used in smartwatches to intensively monitor patients with chronic obstructive pulmonary disease in a way that is impossible *in situ*, but which also requires patients to take care of the equipment and follow competent protocols by themselves (ROHRINGER; BUDHKAR; RUDZICZ, 2019).

Addressing the issue of data privacy of individuals in relation to the use of AI in the market for high-tech devices and services is of extreme legal relevance. From the standpoint of Sociology of Law, this is a pressing issue in society, which the law will also have to resolve: the issue of ownership of personal data in relation to the companies that process them, to the State and to science institutions in general, which will use personal data for a wide variety of studies – which, on the one hand, may allow huge advancements of knowledge; but on the other, it may end up with privacy, degenerating it into total social transparency. From the point of view of the Philosophy of Law, studying this issue concerns fundamental legally protected values – especially privacy and security – not only in relation to the market and the State, but to what is meant by personal identity, dignity and ethical limits. With regard to Constitutional Law, it is a question of observing how fundamental rights will have to be contextualized and interpreted in a new technological and social environment. Finally, with regard to Consumer Law, it is a matter of analyzing the protection of the consumer in what is most precious to him/her, beyond life and physical integrity – the moral integrity of his/her person.

The research problem that motivated this work can be expressed in the following question: in what ways can data protection legislation be complemented by other forms of regulatory efforts, in order to bring the law and public policies closer to the complexity that such a theme offers? As a hypothesis to such question, it is presented that the current data protection acts – at least the General Data Protection Regulation (GDPR) of the European Union, in comparison with the Brazilian General Data Protection Law (LGPD) – are not sufficient to cover several of the problems that arise from the capture and processing of sensitive data by companies that develop devices and services based on technologies dependent on AI, despite the fact that such laws have many important points for the regulation of such activities. Thus, new dialogic understandings, in addition to State regulation efforts, must be developed.

The main objective of this article, prepared according to the hypothetical-deductive method of procedure, with a qualitative approach and bibliographic review research technique, is to study the complexity of personal data protection in face of the challenges and risks that the activities of data capture and processing by AI offer to privacy. To achieve this objective, its development was divided into four sections.

Its first section establishes a relationship between the development of AI in applications and devices of the so-called *digital health*, critically observing the ways through which these new technologies have represented interesting promises, but which should be considered alongside the concern with the risk they may pose to the privacy of their clients/patients data. Its second section analyzes the risks and transformations that AI-dependent technologies – especially deep learning and Big Data analytics – pose to the right to privacy, in an era of hyperconnection, ubiquitous surveillance technologies, and heavy investment by companies and States. Therefore, its third section studies several devices of the European GDPR in comparison to the Brazilian LGPD, pointing out several worrisome and similar issues between such regulations – mainly with regard to the required consent of the users of the applications and data capture devices used for the AI training. Finally, its fourth section analyzes new proposals regarding the regulation of AI and data processing, in addition to State norms.

2 AI, digital health and data privacy

As per Chang (2020), the future of AI in digital medicine is extremely favorable, featuring a myriad of advanced techniques, such as deep learning, that will have to be in synergy with physicians to allow data analysis in order to facilitate new knowledge in different areas of Health Sciences. In the author's view, all health data will have to be released and shared without any obstacles so that AI might be omnipresent and invisible in the future health area and might discover new knowledge from all sources of data and information. There must also be an interface between physicians who should use data and computer scientists responsible for knowledge about analytics to ensure a continuum of data to information and, eventually, knowledge transfer.

As technology gets smarter, new ways to engage users (including physicians and providers) with devices must be found, hence customer experience becomes a serious task for any technology company that provides continuous services to its users through platforms or applications (KAZGAN, 2020). It is normal to expect patients to engage with their digital health tools more than any other standard user profile, as non-compliance would worsen their quality of life – although human behavior tends to be easily distracted from regular standards and the tasks required, even with the possibility of negative impacts. Thus, in addition to the ability to be wore and the comfort that their incorporation into routines has, a symbolic imagery is also being formed about the capabilities that the use of such devices provide (LUPTON, 2020). Their simple use can make people feel differently about themselves, potentially motivating them to behave differently. They therefore come to align themselves with the standards and objectives defined by the software incorporated into the wearable device, striving to achieve defined values of health, productivity or physical activity.

The possibility of easy visualization of data produced by such devices can motivate and inspire their users, thus generating feelings of pleasure, confidence, pride and achievement when goals and targets are reached or when the numbers "seem good". Their representations can inspire users to change their routines or maintain health practices that meet their goals. In other contexts, however, the sociotechnical imagery of such devices is not animated in daily use. People may simply choose not to wear them after a while because they find the users' experience disappointing because they may feel boring, inaccurate, or generate feelings of guilt or shame.

Although blockchain technology and the most varied forms of AI offer great promise to revolutionize healthcare, maybe it is too early for this revolution to happen, however (ILINCA, 2020). Healthcare sector is very complex, with many stakeholders whose incentives are often conflicting. It is also unclear whether these technologies can be implemented on a large scale with better outcomes for patients and more added value for stakeholders.

But data often considered sensitive must be shared for real benefits from data technologies in the healthcare sector – however, precisely because they are considered sensitive, private issues, access and storage of such information must be kept secure by data processing companies. Such data must also be correctly labeled and recorded to be really useful for AI, as high-quality data is the basis for achieving high-precision models – although it is extremely difficult to find them in current Big Data without discriminatory biases or possibility of identification of its subjects, for example. Thus, large upfront investments must be made by entrepreneurs in the field, for the acquisition or creation of clean data and the right incentives for data subjects. Furthermore, blockchain technology might help maintain data privacy and security while keeping information accurate. In addition, entrepreneurs must also establish close feedback loops with clinical experts in the field to quickly adjust their products and offload the burden of proof in any lawsuits to blame for errors.

Not only wearables, such as smartwatches, have been designed for health and data issues: there are several health monitoring and treatment technologies based on collecting data from devices that can be deployed or ingested by those who are being monitored. And one's data can be collected, stored, and analyzed using AI algorithms – by transmitting data over Wi-Fi to computers that process those algorithms and software, for example. There are seemingly limitless applications of ingestible technologies for monitoring health through many types of sensors and even treatments – micro and nanobots performing repairing microsurgeries, smart pills that correctly administer medications, and so on – which potentially could reduce commuting to doctors' offices, clinical analysis laboratories, outpatient clinics and operating rooms, thus saving more lives in less traumatic ways. However, such technologies can produce negative effects that are related not just health and medical safety.

Few ingestible product developers pay considerable attention to privacy issues related to user health data or to ways ingestible products can be used to embarrass and oblige users by health insurance companies (ILIADIS, 2020). Ingestible devices can create future problems if customers do not give proper consent. Furthermore, patients can be pressured into using ingestible products, providing valuable data about themselves that can be sold, exchanged or used against their will, often in ways that are unimaginable at the time they sign up the consent terms to use the technology. One's privacy is at risk when ingestibles are used to save data in the form of images, sounds and biological information (heart rate, body temperature, movement etc.). Such data can be used against people – insurers requiring users to track themselves in order to have to pay claims, for example. In other words, ingestibles could constitute new forms of surveillance, enhanced by AI.

In this sense, Pedersen (2020) argues that human body will become a platform. And as there is a social expectation that computing will become increasingly continuous, the idea of a networked body working autonomously through datasets does not seem to be the image of such a distant and unthinkable future. The popularity and commercial success of wireless communication has also raised expectations about how people understand human communication and the sharing of personal experiences. Wearable devices based on such technologies have been acquiring more comfortable and functional designs, becoming more and more ubiquitous not only because of the large investment that technology companies have been making, but also because of their possibilities for continuous use.

At the same time, the press has been glorifying automation, algorithmic decision systems and deep learning, although alarms about the opacity and ambiguity surrounding such systems and their processes are also frequent. And mass media communications about technological possibilities (in successful science fiction films and series or in video games, for example) is not a mere poetic license, but a reflection of the collaboration between the military-industrial complex and American cultures industries, which glorify technology in their products. Transhuman military ideologies promote fictional computing devices, making them look exciting and destined to emerge in the real world. There are, therefore, those who communicate in a massive way about a future that will transform the internet into an immersive landscape, a bright new reality, in which tablets, PCs and smartphones will no longer be needed, as electronic components will fill bodies and physical spaces. But the underground is a dimension where people passively offer data to the invisible networks that host them, where malicious third parties threaten attacks, and where facial expressions, medical monitoring data, thoughts, emotions, memories, sensations, and general behavioral information will be exchanged between distant spheres of data, beyond the control of the users holding such sensitive and private information.

Wearable self-tracking devices capture multidimensional health data and offer several advantages, including new ways to make search easier. However, they also provide for the emergence of conflicts between individual interests – mainly related to avoiding damage to privacy – and collective interests – regarding the collection and use of large health datasets for public benefit. Although there are some who advocate for accountability and transparency mechanisms for resolving such conflicts, average users are not able to access and process information regarding the consequences of their consent to new uses of their data. In this sense, Arora (2019) defends fiduciary relationships, which place the responsibility of deliberating on digital health data controllers for maintaining the interests of their data subjects in the foreground, and for the contextualization of privacy. In other words, the relationship between users, holders of health data, and digital data controllers must be recognized as a fiduciary relationship, so that health data controllers keep the interests of users at the forefront. This would guarantee the collective participation of user data (to improve digital health applications, contribute to scientific research etc.) and reduce the risks related to their privacy.

3 Privacy in the age of ubiquity in personal data capture and AI

AI and machine learning are often described as technological advances that will completely transform society, being implemented everywhere – medicine, transportation, finance, art, legal and social institutions, weapons development etc. (YANISKY-RAVID; HALLISEY, 2019). In many industries, their systems are already making decisions that were previously a human responsibility. In this sense, mankind is seen to be at the epicenter of an ongoing revolution in government and commercial surveillance – and as a result, much of the definitive public anonymity and obscurity that characterized urban life for centuries has been lost. Sensors, cameras, cell phone data access, social media platforms, and AI algorithms reading and interpreting these entire massive sets of data have been ubiquitous pieces in urban spaces, where the future radical transparency of human life is already emerging – and in times of rapid development of privacy and data protection norms, the state of urban life has much to illustrate about the long-term effectiveness of such standards. According to Keller (2019), the explanation for the contradiction between the right to information and the right to privacy is explained by the broader political economy behind the right to information, which continues to shape and limit the capacities of data protection and privacy laws.

Although the prevailing liberal democratic model of information norms is structured around two main concerns – ensuring that: i) the State can have ultimate access to information; and ii) the market may permanently do business with data (at least potentially) – the particular vulnerability of personal information to demands for access by the State and the market is much more than a matter of political and economic power imbalances, as the right to information has developed through a dynamic relationship between the uses of governmental and commercial information, as well as through the continuous application of new technologies that make information more usable and accessible. And the reconstruction of privacy through the law has been porous and compromised, particularly (KELLER, 2019): (i) by the transformation of the concepts of public space and public domain, often used to justify access to personal information with the minimum of safeguards; (ii) by the conflict between the principles of consent and individual choice, cornerstones for personal autonomy and for the commercialization of information; (iii) by the comparative structural weaknesses of privacy and data protection laws, being considered as a field within the broader sphere of Information Law.

Added to this is the fact that public companies and concessionaires/permissioners of public services (electricity providers, for example) are in a privileged position of power regarding their consumers' data, as they establish lasting relationships with them, and in most cases such customers do not have any choice in the market – either because of the absence of others that perform the same function (as in the case of electricity power plants), or because the customers are in such a situation of low sufficiency that makes it materially impossible for them to opt for the private service offered (such as education and health services) (STEIN, 2020).

In addition, with the increasing possibilities of use of smart technologies and Internet of Things (IoT), even more access to personal data comes with the advent of smart energy meters, for example: new forms of sensors and meters that can be remotely accessed, communicate information about user behavior and support intelligent applications for consumption and pricing of distributed resources. It is known that AI systems work better the greater the amount of data they have access to – therefore, data sharing will be critical to successfully implement AI technologies for smart consumption, which could make more rational use of multiple resources and improve efficiency in delivery. However, the growing use of such devices raises concerns about the private information that might be obtained about individuals through their behavior patterns, making the holders of such data fearful of accidental or malicious surveillance, targeted home invasions, creation of profiles, behavior tracking or identity theft. Thus, additional responsibilities are placed on the utilities as custodians of this data, and this fact raises important questions about the storage, use, transfer and disposal of these data (STEIN, 2020, p. 923).

These privacy issues directly conflict with efforts to minimize AI duplication training and to facilitate data sharing, steps that are crucial to enabling modernization of services (including power supply). To address this offset, stakeholders and regulators can take a number of important steps to minimize the negative privacy implications of using all of this energy data. There are at least two avenues to help facilitate these collaborations:

(I) *Adoption of strict procedures to anonymize data related to energy consumption*: data anonymization – the implementation of data de-identification processes so that information can no longer be identified, related, described, referenced, associated or linked, directly or indirectly, to a particular individual – is a commonly used technique to protect privacy. Anonymization techniques include randomization and generalization – however, such processes, technically, are not 100% effective, which still leaves a lot of uncertainty. Nevertheless, the Brazilian General Data Protection Law (LGPD) already states the mandatory adoption of data anonymization and pseudonymization processes in its arts. 12 and 13 (BRASIL, [2020]);

(II) *Regulation of Data Ownership*: generally, public services' customers have the right to access their own data, but there are different views on whether third parties can access this data, as well as who owns it. Brazilian LGPD already exists in this sense, as observed from its art. 5º, V (BRASIL, [2020]).

Even simpler applications using AI – such as car locators in parking lots from vehicle photographs, cross-referenced with GPS data – can raise privacy concerns, being the main ones related to (TUCKER, 2019):

(I) *The persistence of stored data*: information created by users can persist in storage even longer than the lifetime of the human being who created it, due to the relatively low cost of data storage;

(II) *The possibility of data reuse*: in addition to the practically indefinite persistence, it is not known how the generated data can be used in the future (by security services, by the State, by marketing or insurance companies etc.);

(III) *The data overflow*: data can record information not just about the data subject – for example, other people can have their images recorded in photographs read by AI algorithms (for example, a selfie taken in a parking lot by one person may reveal a license plate belonging to a third-party's car parked in the same lot), and such information can be cross-checked against others (such as facial recognition, license plate databases, social networks etc.). Although these third parties have not chosen to create data about them, its creation may have future repercussions.

These three problems pose new challenges to the legal treatment of privacy, as they contradict the traditional ways through which people can decide to create personal data that can later be used to inform an algorithm. And, more specifically, about the value of consent to privacy regulations around the world.

The collection of user data from online applications and services is reinforced by the significant profits that the private sector can make by quickly and conveniently providing a wide range of services to users (PELTZ; STREET, 2020, p. 95). In the current paradigm, terms of use and privacy agreements are confusing, being written to dull their impact, thus urging users to automatically accept a certain risk in exchange for convenience and "free" access. Third parties, including governments, also gain access to these data in a variety of ways. As if the erosion of individual privacy protections and the potential dangers that it poses to individual autonomy and democratic ideals weren't already alarming enough, the "digital substitute" of people created from this paradigm – that is, the digital profile of each AI-powered individual, containing their characteristics, preferences, and tendencies, based on the data collected from their behavior – can soon begin to freely share thoughts, buying habits, and standard of living with the owner of such data. The engine of the surveillance economy feeds on the 2.5 quintillion bytes of generated data daily. And AI will increase the ability to analyze, collect and refine data that will be used to target the consumers who generate that data.

Algorithmic forecasting in the insurance industry can usher in a new era of customizing policies, premiums, claims and coverage based on individual behavior and level of risk. Thus, external variables (gender, age, race, address etc.) are replaced by internal ones, that is, individual behavior, and insurance contracts can be fully configured accordingly to that. Prices related to insurance contracts, therefore, would no longer have as a reference the calculated uncertainty of a large group of policyholders – thus, everyone would have to pay only for their real exposure to risk (CEVOLINI; ESPOSITO, 2020). Although it seems fair and appropriate to customize insurance – as those who take more risks should pay more, according to such logic – there is fear that customizing prices could shape life chances and produce new forms of discrimination. Unlike the traditional stratification into social classes, with the new alliance between actuarial techniques and digital technologies, discrimination would be a consequence of individual lifestyle and generate classification situations that would affect the quality (and possibility) of individual life in ways that are still unpredictable. And for insurance companies, however, uncertainty is not just a problem, as shared uncertainty is a resource, and the availability of information about individual risks can undermine the principle of combination and distribution of risks on which the insurance industry is based. So the use of high data technology in insurance could spell the end of this industry – at least as it has been known for centuries.

It is also noted that the race to develop AI has already started, and several countries are making efforts to be the world leaders in the sector. While AI carries the promise of a smarter, more autonomous world, there are several legal concerns regarding its development – among them those related to privacy and the protection of consumer personal data. Although several countries are adopting varying degrees of personal data protection, the European Union

(EU) is a pioneer in such regulation, with its General Data Protection Regulation (GDPR). However, several aspects of such regulation raise concerns about the impact of its application on algorithms and machine learning necessary for the development of AI.

Maintaining the competitiveness of the AI sector in a country or region depends on a delicate balance of such a goal in relation to the protection of privacy (HUMERICK, 2018). There are public policies that can bring such a balance, such as public funding for AI development – a strategy adopted by China – and encouraging the development of less invasive AI techniques – such as Google's OpenAI, which, although not as effective, as for the unlimited AI in data access, it is cautious in the development and respect for consumer privacy. However, the regulation of the use of personal data without creating means to facilitate its use for the training and learning of AI systems will rather cause the perishing of the normative system for the protection of personal data that simply chooses to protect privacy of users without any balance in the face of the need to maintain technological innovation in the territory where such law applies, as organizations and private companies involved in the development of AI will seek ways to circumvent the protections that are too prohibitive to the use of data, given that the AI learning and development ability depends on analyzing huge amounts of data.

4 The fallacy of consent and the state of the art in privacy by design

The right to protect personal data has been structurally based on the consent of the owner of the personal data hitherto in Brazil – just observe art. 5º, XII, LGPD (BRASIL, [2020], our translation), which considers consent to be a "free, informed and unambiguous manifestation by which holders agrees to the treatment of their personal data for a specific purpose" – and on this notion underlies the permission for processing personal data. Data processing algorithms are being increasingly introduced into society, but data protection and privacy rules have presented difficulties to incorporate particularities of information societies with intensive use of data, and because of that, challenges to the role and concept of consent are particularly evident (GIANNOPOULOU, 2020). Although for some the LGPD clearly defines the forms of consent, not allowing the user to consent through long, exhaustive and obscure information on how the use of user data will take place (BARRETO JUNIOR; NASCIMENTO; FULLER, 2020, p. 20). Cotino Hueso (2017) considers that such a base is very fallible in ages of Big Data and AI. First, because the massive accumulation of data and its capture will overload the legal principles pertaining to the consensus for the protection of personal data. Second, because people are unwilling to give up the use of Information and Communication Technologies. And third, societies generally do not have a strong culture of privacy, which makes the guarantee of consent almost unrealistic or ineffective. Furthermore, in practice, consenting is standardized, which causes suspicion, as it is fallacious to believe that there is effective control of personal information through consent and the rights that complement it – and consent, in practice, becomes a "carte blanche" for the uncontrolled flow of personal data, having a merely symbolic function that, ultimately, leads to violations of the intended privacy and ineffectiveness of protective systems.

A currently widely discussed way of achieving data protection and security is the so-called *regulation by design* – which, in its simplest formulation, corresponds to the use of technical and organizational measures to achieve data protection goals (RUBINSTEIN; GOOD, 2020, p. 37). As an example, the obligation to program technological tools in such a way that it is impossible for them to violate the protection law may be cited. In the same sense of regulation by design, the concept of privacy by design was created – which corresponds to the prioritization of privacy from the conception (beginning and development) of a product or service, "permeating the feasibility studies of projects as it is done with costs, market, consumer public and others" (SOARES, 2020, p. 569, our translation). The idea of privacy by design has the scope to ensure that the future privacy of data might be guaranteed beyond compliance with procedures and/or standards, and privacy must now correspond to the organizational standard, with its incorporation into the modus operandi of each company.

While privacy regulators have endorsed privacy-enhancing technologies, art. 25 of GDPR, for example, innovates by transforming this idea into a binding legal obligation (EUROPEAN UNION, 2016; RUBINSTEIN; GOOD, 2020, p. 37). And with regard to the Brazilian LGPD (BRASIL, [2020]), its arts. 12 and 13 bring an order similar to that of GDPR, regarding the possibilities of using anonymization and pseudonymization techniques. Teixeira and Armelin (2019, p. 70-72) explain that obligations of anonymization should consider the reasonable and available techniques adopted at the time of data processing – that is, even if better techniques emerge later, it is the state of the art at the time of processing which must be considered, due to the exponential advance of technology over time, and what will be reasonable later is unpredictable. In addition, the Brazilian National Data Authority (ANPD) should regulate how access to data for research may be done, as well as the responsibility of the research body for information security. Bearing in mind, however, that contrary to art. 25 of the GDPR, the LGPD does not use the expression *state of the art* in security to address the issue – and it is important that the ANPD, when creating the regulations for such an issue, use that terminology, in order to obtain greater effectiveness with regard to the security of personal data.

The aforementioned European regulatory device, however, as currently conceived, is poorly aligned with privacy engineering methods and privacy-enforcement technologies – especially with regard to "hard" enforcement technologies, which end up causing little trust in third parties (including here data controller agents, for example), using cryptographic techniques to obtain data access minimization (RUBINSTEIN; GOOD, 2020). In order to promote data protection in its own right, instead of just reinforcing the general principles of the GDPR, its art. 25 should be interpreted as requiring the implementation of private engineering and harsh privacy-enforcement technologies. A bold way to achieve this is to require data controllers to use such available technologies to minimize data.

Moreover, for a gradual implementation of privacy techniques, the following steps should be taken: (i) the establishment of data protection regulators that insist on a central role for privacy engineering and privacy-enhancing technologies in projects from the Public Sector; (ii) the issuance of guidelines on art. 25 (and on arts. 12 and 13, LGPD, in the Brazilian scenario) in vigorous terms, which clearly require the implementation of privacy technology according to the "state of the art"; and (iii) rewarding good examples of privacy engineering, rather than simply penalizing flaws.

Regarding the use of data by public organizations, arts. 25 to 27 of the LGPD (BRASIL, [2020]) point out the ways through which personal data managed by such organizations can be shared. In this sense, only for the execution of public policies, provision of public services, decentralization of public activity and dissemination, and access to information by the general public may sharing occur. In addition, the transfer of personal data to private entities is prohibited – except when the data is publicly accessible, when there is a legal provision or the transfer is supported by contracts, agreements or similar instruments, or when the execution of a service or measure requires it (PAIVA, 2020, p. 170). There is also an exception in the case when the transfer of data is exclusively aimed at preventing fraud and irregularities, or to protect the security and integrity of the data subject, as long as processing for other purposes is prohibited.

Although AI has been appearing more frequently in public debate in recent years, little is known about the factors that shape people's attitudes towards such technology. In this sense, the study by Lobera, Fernández Rodríguez and Torres-Albero (2020) researched about such factors by analyzing data from a survey in Spain. The work has shown that cultural values and attitudes to science provide an effective explanation of people's opposition to AI – then, those who express egalitarian values and privacy concerns are more likely to oppose AI, as well as are people who express less confidence in the actual application of science and who are less predisposed to innovation and change. The strongest opposition to AI was presented in relation to robotization in the workplace by technology – emerging the "smart machine" as a new threatening element.

The widespread use of AI to make decisions about too many aspects of human lives has provoked controversy due to the risks and limitations of that technology. The impact of AI on digital privacy is of great concern, as AI leads to ubiquitous data collection, identification problems, and a lack of algorithmic accountability. Even so, Els (2017, p. 234-235) suggests that AI might also help alleviate many digital privacy challenges, and its use and development should be understood only as threats to privacy. New techniques, built into differential privacy and deep learning, minimize the amount of sensitive information collected, stored and shared with third parties, allowing companies to continue to learn a lot, and in a valuable way, about their users' activities. Auditors and AI officials could represent the interests of consumers through collectivization and correction of incentives, and monitor the likelihood of re-identification or discriminatory results in other systems. Furthermore, AI can help define what privacy is, a work that has often proved elusive and detrimental to the ability to enact more significant privacy protections. The successful implementation of these techniques will also depend on the coordination of legislation and private action to ensure that they realize their full potential.

Big Data analytics and AI make non-intuitive and unverifiable inferences and predictions about people's private information (their behaviors, preferences, and private lives). Such inferences are founded on very rich and diverse data, creating new opportunities to decide in a discriminatory, biased and invasive way. GDPR – and the Brazilian regulation that was inspired by it, LGPD –, while aiming to protect people's privacy, identity, reputation and autonomy, does not protect data subjects from the new risks of inferential analysis. According to Wachter and Mittelstadt (2019), individuals have little control or supervision over the ways in which their personal data are used to make inferences about them. Compared with other types of personal data, the inferences are effectively "economic class" personal data in GDPR, with the rights of data subjects to know (arts. 13-15), rectify (art. 16), suppress (art. 17), objecting (art. 21) or transporting (art. 20) personal data are significantly restricted for inferences. GDPR also offers insufficient protection against sensitive inferences (art. 9) or solutions to contest important inferences or decisions based on them (art. 22 (3)) (EUROPEAN UNION, 2016).

Thus, a new data protection right, a "right to reasonable inferences", could close the liability gap currently represented by "high-risk inferences" – those made from Big Data analytics that harm privacy or the reputation of data subjects, as they are predictive or based on opinions (WACHTER; MITTELSTADT, 2019). The right to reasonable inferences would require that an *ex ante* justification be provided by the data controller to establish whether an inference is reasonable. Such a justification would address: i) why certain data form a normatively acceptable basis from which to draw inferences; ii) why these inferences are relevant and normatively acceptable to the automated decision; and iii) the accuracy and statistical reliability of such data and the methods used to make inferences from them. This *ex ante* justification would be supported by an additional *ex post* mechanism, which would allow the holders to contest unreasonable inferences.

5 Regulation of data capture and AI: new proposals

Data is the most important aspect in training AI systems, as algorithms learn from huge sets of preexisting data. However, data used by AI systems sometimes are illegal, discriminatory, altered, unreliable, or simply incomplete. Therefore, the more data is provided to AI systems, the more likely they are to produce discriminatory decisions and privacy violations through their use. To solve this problem, Yanisky-Ravid and Hallisey (2019) propose an AI model based on data transparency and focused on data disclosure, not on the initial software and its programmers. Thus, audit regimes and certification programs administered by a government agency could verify the transparency of the algorithm – or, in its absence, by private institutions. Such a model would thus encourage industry to be proactive in taking steps to ensure that their datasets are reliable. Adapting this proposal to what institutes the Brazilian LGPD, the ANPD would be responsible not only for regulating practices related to data protection, but also for encouraging the private sector to create reliable mechanisms for auditing and transparency, taking advantage of the state of the art technology for this, and balancing, at the same time, the need to protect the privacy of personal data and the use of data in favor of technological innovation in the sector – considering that such mechanisms could become marketable tools and processes for security products and services.

Alamäki, Mäki and Ratnayake (2019) showed that data quality has several dimensions and factors that influence its reliability – which is related to accuracy, legal validity, and commercial value of the data. Concern about privacy affects data reliability, as users can manipulate the information they provide. The challenge for most AI systems today is their learning's inability to distinguish biased or corrupted data from high-quality data. That is, AI systems can process data, but cannot evaluate its creation process. Thus, data can technically meet certain requirements, but in fact may have its content biased or corrupted. Furthermore, data processing professionals are not always able to differentiate between bad data and high-quality data, especially when they do not know how such data was collected and pre-processed. Thus, the authors demonstrate that the quality of data affects the reliability of the results – with the concern with privacy being a factor that influences reliability. And they suggest, therefore, that emphasis should be placed on the early stages of data collection processes, when human factors or scarcity of data capture technology can corrupt data quality.

One of the main problems regarding security and privacy of consumer data is the non-accountability of companies that deal with them for the risk they represent for such legal assets (JIN, 2019). And the establishment of a regime of total responsibility presupposes the overcoming of three difficulties: i) observation of the real action of companies in collecting, storing and using data; ii) quantifying the consequences of their practices for consumers' personal data – in particular, prior to the realization of low-probability adverse events; and iii) establishing a causal link between the practice of data by a company and its consequences.

Although privacy has been seen as an obstacle to innovation, being considered by many as something that increases the costs of data governance without providing real benefits, the attitude of many stakeholders in the relationship between privacy and innovation has been changing, being that this is an increasingly fundamental right, being more and more adopted as a facilitator of innovation, as consumer confidence is essential for doing business with data-based products and services (BACHLECHNER; VAN LIESHOUT; TIMAN, 2020). In addition to building trust by demonstrating responsibility in processing personal data, companies are using privacy protection tools in areas such as data storage and archiving. A proactive approach to privacy, which means that the legal framework is not minimized but taken seriously, makes this much easier. In other words, fully considering not only the law but also additional measures to protect privacy may be a greater effort, but it will have a return in the medium and long terms, as well as responsible attitudes from a socio-environmental point of view by companies have been consumer-pleasing, responsibility for data privacy will undergo a similar transformation.

But privacy as a driver of innovation still faces challenges – being the main ones: the lack of profitability of privacy-friendly offerings, conflicts with new and existing business models, the low value placed on privacy by individuals, latent cultural specificities, gaps in skills, and regulatory gaps. Furthermore, for the success of the privacy markets not only the challenges related to profitability and business models need to be overcome, but also the challenges related to the individual assessment of privacy, cultural differences, skills and regulations.

Not only technical limitations cause such difficulties, but also misaligned regulation does. Currently, the practices of such companies can still be considered, many times, poorly regulated, which leads them to hide real data practices from the public, obfuscate information disclosed to consumers, and/or blame other random factors (act of God, force greater, fact caused by the consumer etc.) by the damage they perpetrate. In this regard, additional changes are needed to provide more transparency in the progression of data practice towards harmful outcomes, and to translate the results into incentives that directly affect companies' choice of data practice. Such changes cannot slow down technological innovation or end the viability of companies. However, regulation should aim to help build consumer-friendly data practices that stand out from harmful practices, which may promote respectful innovations consumer demands for privacy and data security.

There are several ways to deal with misaligned incentives – through new legislation, industry self-regulation, court rulings and consumer protection measures. Perhaps the most significant are the following ones (JIN, 2019):

(I) *Security regulation*: improper quality control of privacy and data security issues can have random and noisy consequences, such as identity theft and fraud. Furthermore, the ways through which companies decide how they will handle consumer data are often not observable by end consumers. The common solution for this is to directly regulate the company's actions – pre-establishing the conditions under which companies must store and process data, standards to be observed regarding periodic inspections and audits etc. But these regulations are based on the assumption that good and harmful practices are known – which is not easy to find in data practice, as the rapid technological evolution of the sector makes it very difficult for public authorities (judges, politicians, experts, technical committees etc.) to evaluate good practices. Thus, it is difficult to ensure that regulations are updated in parallel to each round of technological advancement;

(II) *Company disclosure and consumer choice-dependent approach*: to make this approach effective, it is assumed that consumers are able to make the best choices for themselves, provided that they have adequate information at hand. But this is not effective for privacy and data security, as it is already widely scientifically reported that most consumers do not read the notices and terms relating to privacy practices. Furthermore, many data-intensive companies may not have an interface with consumers, and it may be difficult for consumers to choose, as they are not able to assess different data practices, so they may also not know what options are available to mitigate potential damage. And companies' data practices can change very often in reality as well, in the light of technological advancement – so providing up-to-date notices to consumers can be impractical and even overwhelming;

(III) *Self-regulation*: this approach assumes that, as companies have greater know-how about data technologies and practices, they would be better positioned than State authorities, for example, to identify best practices. In fact, for authors such as Katyal (2019), it would be fruitless to look only at the role of the (so reluctant) State to address issues of algorithmic accountability – and the focus of regulation on algorithmic accountability should also cover other ways to ensure more transparency and accountability, originated in the private industry. The question of algorithmic responsibility before the realization of fundamental rights represents a crucial new world of concerns. Currently, the activities that raise the greatest concerns about due process, discrimination, privacy and data security are those of private companies, not so much of the States. Thus, self-regulatory practices such as codes of conduct, impact statements and whistleblower protection could encourage greater endogeny in the application of fundamental rights. But history suggests that self-regulation may not occur without the threats posed by State regulation, and this suggests that government efforts can be complemented, but not replaced, by industry companies' attempts to build self-regulation (JIN, 2019). Even so, there are technical obstacles in relation to the construction of an effective self-regulation, as many organizations are trying to develop classification systems in the practice of data, but there is no comprehensive and updated information related to each particular company to facilitate such a posture;

(IV) *Definition and requirement of obligations relating to privacy in the use of data as rights*: in practice, EU has followed the approach of privacy as being a part of Human Rights, which restricts transfer and contracting rights. Thus, EU has recognized individual rights to access, process, rectify and erase data in its GDPR. Because it is so recent, the impact of GDPR has not had very salient concrete effects yet, but two challenges to its applicability should be mentioned – which may impede data-based innovations if the innovator has to obtain data usage rights from multiple parties with advance: (i) in relation to many products and services that use data (autonomous cars, for example), data does not exist until the user interacts with the system, often with the support of third parties (GPS services, vehicle insurance companies etc.), and this raises serious doubts as to who the data should belong to (whether the user, the producer or third parties); (ii) even if data ownership is clearly defined in public regulations, this does not mean perfect compliance – piracy and counterfeiting are good examples of that.

Finally, the issue of data privacy regulation becomes even more complex because of the existence of particularities of each type of organization that work with them. Especially with regard to organizations that provide humanitarian aid (such as the Red Cross), compliance with data protection principles is not enough, as such actors must also comply with humanitarian principles to ensure the provision of impartial and neutral assistance that does not harm the beneficiaries in any way. Therefore, Barboza, Jasmontaitè-Zaniewicz and Diver (2020) analyze a hypothetical AI-based facial recognition system that could assist humanitarian organizations in their efforts to identify missing persons. Scholars recognize that such a system could create risks by providing information on missing persons that could be used by harmful third parties to identify and target vulnerable groups; therefore, such a system should be implemented only after carrying out a holistic impact assessment, to ensure its adherence to data protection and humanitarian principles. Thus, humanitarian principles such as the obligation to not cause damage, participation of beneficiaries, building local capacity and responsibility must be harmonized with those concerning data protection, such as limitation of the purpose of use, security of data and justice in the face of possible discriminatory trends.

6 Conclusion

This research aimed to address the complexity of protecting privacy in the face of the challenges and risks that AI data capture and processing activities pose to the fundamental right to privacy. As a result of this objective, the popularization of various types of electronic devices, added to the ubiquity of the internet and the increase in spending on health services, has led people to become interested in performing various health monitoring tasks. This has created an impression that patients themselves can take responsibility for their treatments, in addition to professionals. But companies that develop and promote the use of AI in health do not always pay attention to the most sensitive issues of its popularization regarding the risks that the capture, treatment and storage of sensitive data represents for the right to privacy of their users and patients. Furthermore, regulation of the use of AI tools that handle personal data must take into account not only data protection and privacy principles, but also other principles relating to the nature of its activities. Therefore, a dialogic and transdisciplinary normative posture must be built, considering the type of organization that works with such technologies.

The use of predictive algorithms can change the reality of various types of commerce and services. Prices can now be calculated based on external, behavioral variables, and no longer on external generalized ones. However, as fair as the individualization of prices may seem, it can generate new forms of discrimination, which are somehow different from the current prejudices based on generalized social stratification, and which are still unpredictable. On the other hand, it is necessary to balance the right to privacy regarding personal data and the goal of developing the AI sector, as protection without considering the great need that such sector has for personal data for training and learning can lead to its economic collapse. Public funding for digital health and encouraging the development of less invasive techniques for using data are interesting strategies for this purpose.

Security and privacy regulation on the use of data by companies – data that serve as a basis for the development and technological innovation based on AI – should not only curb harmful practices to privacy and security, but encourage good practices developed throughout innovation process. However, given the complexity and the recent nature of the proliferation of AI use in the market, several regulatory practices must be considered simultaneously, in a complex way, as each one has its particular problems and positive potentials. Thus, regulation by data authorities must be complemented with self-regulation by sector organizations and companies, with transparency practices by companies being required (and, in turn, qualified with consumer choice, when possible), and addressing the issue of data security and privacy from enforceable human rights perspective. Respecting privacy builds consumer confidence; therefore, a proactive stance on the part of companies – not only respecting data privacy protection laws, but also developing social responsibility in this regard – can be considered an incentive for technological innovation (although this may encounter obstacles to various natures). Thus, recognizing the relationships between users of health data collection applications/devices and their data controllers – that is, companies that perform health data treatment services – as being fiduciary could be a legal method of privacy protection users, which would not compromise the evolution of the state of the art of technologies related to health data.

Data might proof to be too persistent, reused indefinitely, and concern third parties who have not consented to its production or its processing by companies using AI. The value of consent, which is the basis of legal data protection systems, is this time significantly impaired in terms of its practical effectiveness. Even so, personal data protection legislation (especially the GDPR and the LGPD) has basically relied on the idea of the data subject's consent for its use – through digital consent terms, for the most part. That is, they have centered their systematics on a fallacious idea in practice. Users will not relinquish the use of ICTs, but there is not a strong culture of privacy in society, and the taking of consent thus has a merely symbolic function which, ultimately, leads to non-compliance with the duty to protect private data. Given the advancement of techniques for obtaining and processing personal data, as well as ICTs (among them, AI), it is essential that data protection laws around the world establish, in detail and rigorously – and if necessary, with specific regulations just for that – about the adoption of anonymization and pseudonymization techniques concerning the state of the art of such processes, therefore.

AI has not been opposed by its future users because of damage to privacy in general. The argument that most causes such technology to be opposed by users is that of replacing people with machines. However, AI is not a technology that only threatens the right to privacy. If well-coordinated with legislative regulation and with private self-regulation, several gains to the protection to privacy may occur through the application of AI in a digital networked environment.

Sobre o autor

Mateus de Oliveira Fornasier é doutor em Direito pela Unisinos, São Leopoldo, RS, Brasil; pós-doutor em Direito e Teoria (Law and Theory) pela University of Westminster, Londres, Reino Unido; professor do programa de pós-graduação (mestrado e doutorado) em Direito da Universidade Regional do Noroeste do Estado do Rio Grande do Sul, Ijuí, RS, Brasil.
E-mail: mateus.fornasier@unijui.edu.br

Este artigo foi elaborado no âmbito do projeto "A democracia no século XXI e as novas tecnologias", financiado pelo Programa Pesquisador Gaúcho, da Fundação de Amparo à Pesquisa do Estado do Rio Grande do Sul.

Como citar este artigo

(ABNT)
FORNASIER, Mateus de Oliveira. The use of AI in digital health services and privacy regulation in GDPR and LGPD: between revolution and (dis)respect. *Revista de Informação Legislativa*: RIL, Brasília, DF, v. 59, n. 233, p. 201-220, jan./mar. 2022. Disponível em: https://www12.senado.leg.br/ril/edicoes/59/233/ril_v59_n233_p201

(APA)
Fornasier, M. de O. (2022). The use of AI in digital health services and privacy regulation in GDPR and LGPD: between revolution and (dis)respect. *Revista de Informação Legislativa: RIL*, *59*(233), 201-220. Recuperado de https://www12.senado.leg.br/ril/edicoes/59/233/ril_v59_n233_p201

References

ALAMÄKI, Ari; MÄKI, Marko; RATNAYAKE, R. M. Chandima. Privacy concern, data quality and trustworthiness of AI-analytics. *In*: FAKE INTELLIGENCE ONLINE SUMMIT, 1., 2019, Pori, FI. *Proceedings* […]. Pori, FI: Satakunta University of Applied Sciences, 2019. p. 37-42. Available at: http://urn.fi/URN:NBN:fi-fe2019051315372. Access on: Oct. 19, 2021.

ARORA, Chirag. Digital health fiduciaries: protecting user privacy when sharing health data. *Ethics and Information Technology*, [*s. l.*], v. 21, n. 3, p. 181-196, Feb. 2019. DOI: https://doi.org/10.1007/s10676-019-09499-x. Available at: https://link.springer.com/article/10.1007%2Fs10676-019-09499-x. Access on: Oct. 19, 2021.

BACHLECHNER, Daniel; VAN LIESHOUT, Marc; TIMAN, Tjerk. Privacy as enabler of innovation. *In*: FRIEDEWALD, Michael; ÖNEN, Melek; LIEVENS, Eva; KRENN, Stephan; FRICKER, Samuel (ed.). *Privacy and identity management*: data for better living: AI and privacy. Cham: Springer, 2020. p. 3-16. (IFIP AICT Tutorials, v. 576).

BARBOZA, Júlia Zomignani; JASMONTAITÈ-ZANIEWICZ, Lina; DIVER, Laurence. Aid and AI: the challenge of reconciling humanitarian principles and data protection. *In*: FRIEDEWALD, Michael; ÖNEN, Melek; LIEVENS, Eva; KRENN, Stephan; FRICKER, Samuel (ed.). *Privacy and identity management*: data for better living: AI and privacy. Cham: Springer, 2020. p. 161-176. (IFIP AICT Tutorials, v. 576).

BARRETO JUNIOR, Irineu Francisco; NASCIMENTO, Ariane Azevedo Carvalho do; FULLER, Greice Patrícia. Lei Geral de Proteção de Dados Pessoais: efetividade jurídica do consentimento do titular para tratamento dos registros. *Revista de Constitucionalização do Direito Brasileiro – RECONTO*, [*s. l.*], v. 3, n. 2, p. 1-23, jul./dez. 2020. DOI: https://doi.org/10.33636/reconto.v3n2.e037. Available at: http://revistareconto.com.br/index.php/Reconto/article/view/80. Access on: Oct. 19, 2021.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Access on: Oct. 19, 2021.

CEVOLINI, Alberto; ESPOSITO, Elena. From pool to profile: social consequences of algorithmic prediction in insurance. *Big Data & Society*, [*s. l.*], v. 7, n. 2, p. 1-11, July/Dec. 2020. DOI: https://doi.org/10.1177/2053951720939228. Available at: https://journals.sagepub.com/doi/10.1177/2053951720939228. Access on: Oct. 19, 2021.

CHANG, Anthony. The role of artificial intelligence in digital health. *In*: WULFOVICH, Sharon; MEYERS, Arlen (ed.). *Digital health entrepreneurship*. Cham: Springer, 2020. p. 71-81. (Health Informatics).

COTINO HUESO, Lorenzo. *Big data* e inteligencia artificial: una aproximación a su tratamiento jurídico desde los derechos fundamentales. *Dilemata*, [*s. l.*], año 9, n. 24, p. 131-150, 2017. Available at: https://www.dilemata.net/revista/index.php/dilemata/article/view/412000104. Access on: Oct. 19, 2021.

ELS, Andrea Scripa. Artificial intelligence as a digital privacy protector. *Harvard Journal of Law & Technology*, [*s. l.*], v. 31, n. 1, p. 217-235, 2017. Available at: https://jolt.law.harvard.edu/assets/articlePDFs/v31/31HarvJLTech217.pdf. Access on: Oct. 19, 2021.

EUROPEAN UNION. *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). Brussels: EUR-Lex, 2016. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Access on: Oct. 19, 2021.

GIANNOPOULOU, Alexandra. Algorithmic systems: the consent is in the detail? *Internet Policy Review*, [*s. l.*], v. 9, n. 1, p. 1-19, Mar. 2020. DOI: https://doi.org/10.14763/2020.1.1452. Available at: https://policyreview.info/articles/analysis/algorithmic-systems-consent-detail. Access on: Oct. 19, 2021.

HUMERICK, Matthew. Taking AI personally: how the E.U. must learn to balance the interests of personal data privacy & artificial intelligence. *Santa Clara High Technology Law Journal*, [*s. l.*], v. 34, n. 4, p. 393-418, 2018. Available at: https://digitalcommons.law.scu.edu/chtlj/vol34/iss4/3/. Access on: Oct. 19, 2021.

ILIADIS, Andrew. Computer guts and swallowed sensors: ingestibles made palatable in an era of embodied computing. *In*: PEDERSEN, Isabel; ILIADIS, Andrew (ed.). *Embodied computing*: wearables, embeddables, ingestibles. Cambridge, MA: The MIT Press, 2020. p. 1-20.

ILINCA, Dragos. Applying blockchain and artificial intelligence to digital health. *In*: WULFOVICH, Sharon; MEYERS, Arlen (ed.). *Digital health entrepreneurship*. Cham: Springer, 2020. p. 83-101. (Health Informatics).

JIN, Ginger Zhe. Artificial intelligence and consumer privacy. *In*: AGRAWAL, Ajay; GANS, Joshua; GOLDFARB, Avi (ed.). *The economics of artificial intelligence*: an agenda. Chicago: The University of Chicago Press, 2019. p. 439-462. (National Bureau of Economic Research Conference Report).

KATYAL, Sonia K. Private accountability in the age of artificial intelligence. *UCLA Law Review*, [*s. l.*], v. 66, n. 1, p. 54-141, Jan. 2019. Available at: https://www.uclalawreview.org/private-accountability-age-algorithm/. Access on: Oct. 19, 2021.

KAZGAN, Mehmet. Real challenge in digital health entrepreneurship: changing the human behavior. *In*: WULFOVICH, Sharon; MEYERS, Arlen (ed.). *Digital health entrepreneurship*. Cham: Springer, 2020. p. 7-15. (Health Informatics).

KELLER, Perry. The reconstruction of privacy through law: a strategy of diminishing expectations. *International Data Privacy Law*, [*s. l.*], v. 9, n. 3, p. 132-152, Aug. 2019. DOI: https://doi.org/10.1093/idpl/ipz012.

LOBERA, Josep; FERNÁNDEZ RODRÍGUEZ, Carlos J.; TORRES-ALBERO, Cristóbal. Privacy, values and machines: predicting opposition to artificial intelligence. *Communication Studies*, [*s. l.*], v. 71, n. 3, p. 448-465, Mar. 2020. DOI: https://doi.org/10.1080/10510974.2020.1736114.

LUPTON, Deborah. Wearable devices: sociotechnical imaginaries and agential capacities. *In*: PEDERSEN, Isabel; ILIADIS, Andrew (ed.). *Embodied computing*: wearables, embeddables, ingestibles. Cambridge, MA: The MIT Press, 2020. p. 49-69.

PAIVA, Danúbia. A tutela dos dados processuais na era do "big data". *In*: ALVES, Isabella Fonseca (org.). *Inteligência artificial e processo*. Belo Horizonte: D'Plácido, 2020. p. 157-176.

PEDERSEN, Isabel. Will the body become a platform? Body networks, datafied bodies, and AI futures. *In*: PEDERSEN, Isabel; ILIADIS, Andrew (ed.). *Embodied computing*: wearables, embeddables, ingestibles. Cambridge, MA: The MIT Press, 2020. p. 21-48.

PELTZ, James; STREET, Anita C. Artificial intelligence and ethical dilemmas involving privacy. *In*: MASAKOWSKI, Yvonne R. (ed.). *Artificial intelligence and global security*: future trends, threats and considerations. Bingley, UK: Emerald Publishing, 2020. p. 95-120.

ROHRINGER, Taryn J.; BUDHKAR, Akshay; RUDZICZ, Frank. Privacy versus artificial intelligence in medicine. *University of Toronto Medical Journal*, [*s. l.*], v. 96, n. 1, p. 51-53, Jan. 2019. Available at: http://utmj.org/index.php/UTMJ/article/view/1158. Access on: Oct. 19, 2021.

RUBINSTEIN, Ira S.; GOOD, Nathaniel. The trouble with Article 25 (and how to fix it): the future of data protection by design and default. *International Data Privacy Law*, [*s. l.*], v. 10, n. 1, p. 37-56, Feb. 2020. DOI: https://doi.org/10.1093/idpl/ipz019.

SOARES, Paulo Vinícius de Carvalho. A diluição das esferas de privacidade e de intimidade diante da era dos dados. *In*: LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro; LAUX, Francisco de Mesquita; RAVAGNANI, Giovani dos Santos (coord.). *Direito, processo e tecnologia*. São Paulo: Revista dos Tribunais, 2020. p. 555-574. (Coleção Direito e Novas Tecnologias).

STEIN, Amy L. Artificial intelligence and climate change. *Yale Journal on Regulation*, [*s. l.*], v. 37, n. 3, p. 890-939, 2020. Available at: https://www.yalejreg.com/print/artificial-intelligence-and-climate-change/. Access on: Oct. 19, 2021.

TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. *Lei Geral de Proteção de Dados Pessoais*: comentada artigo por artigo. Salvador: JusPODIVM, 2019.

TSCHIDER, Charlotte A. The healthcare privacy-artificial intelligence impasse. *Santa Clara High Technology Law Journal*, [*s. l.*], v. 36, n. 4, p. 439-443, 2020. Available at: https://digitalcommons.law.scu.edu/chtlj/vol36/iss4/2. Access on: Oct. 19, 2021.

TUCKER, Catherine. Privacy, algorithms, and artificial intelligence. *In*: AGRAWAL, Ajay; GANS, Joshua; GOLDFARB, Avi (ed.). *The economics of artificial intelligence*: an agenda. Chicago: The University of Chicago Press, 2019. p. 423-438. (National Bureau of Economic Research Conference Report).

WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, [*s. l.*], v. 2.019, n. 2, p. 494-620, May 2019. DOI: https://doi.org/10.7916/cblr.v2019i2.3424. Available at: https://journals.library.columbia.edu/index.php/CBLR/article/view/3424. Access on: Oct. 19, 2021.

YANISKY-RAVID, Shlomit; HALLISEY, Sean K. "Equality and privacy by design": a new model of artificial intelligence data transparency via auditing, certification, and safe harbor regimes. *Fordham Urban Law Journal*, [*s. l.*], v. 46, n. 2, p. 428-486, 2019. Available at: https://ir.lawnet.fordham.edu/ulj/vol46/iss2/5. Access on: Oct. 19, 2021.