DOI: https://doi.org/10.26512/rfmc.v8i3.34503

Zero-Order Privacy Violations and Automated Decision-Making about Individuals

[Violações de Privacidade de Ordem Zero e Tomada de Decisão Automatizada sobre Indivíduos]

Bernardo Alonso*

Abstract: In this article, it is presented the notion of zero-order privacy violation as a grounding practice within a new type of human exploitation, namely, data colonialism: the massive appropriation of social life through data extraction, acquiring digital "territory" and resources from which economic value can be extracted by capital (Couldry Mejias, 2019). At first, I claim that privacy violations do not depend on the nature of the agents involved. Robots read your email, and not having humans involved in the process does not make it less of a violation. It is considered that the harvested data stream is better understood as being a commodity when clean, well-formed, meaningful data standards are respected. Then, it is suggested that scenarios like the covid-19 pandemic make a perfect case to expand surveillance via tracking applications. Companies and governments with pre-existing tendencies to secrecy, tech-enabled authoritarianism, and austerity, capitalize on disinformation strategies. Finally, remarks on the value of encryption, and strategic deleting as measures to reinforce privacy are made.
Keywords: Zero-Order Privacy Violations. Privacy. Artificial Agents. Data. Information.

Resumo: Neste artigo, é apresentada a noção de violação de privacidade de ordem zero como uma prática fundadora dentro de um novo tipo de exploração humana, a saber, o colonialismo de dados: a apropriação massiva da vida social através da extração de dados, adquirindo "território" digital e recursos dos quais pode ser extraído valor econômico pelo capital (Couldry Mejias, 2019). A princípio, alego que as violações de privacidade não dependem da natureza dos agentes envolvidos. Os robôs leem seu e-mail, e não ter pessoas envolvidas no processo não o torna menos violento. Considera-se que o fluxo de dados coletados é melhor compreendido como uma mercadoria quando os padrões de dados limpos, bem formados e significativos são respeitados. Em seguida, sugere-se que cenários como a pandemia do covid-19 sejam um caso perfeito para expandir a vigilância por meio de aplicativos de rastreamento. Empresas e governos com tendências pré-existentes ao sigilo, autoritarismo capacitado pela tecnologia, e austeridade capitalizam estratégias de desinformação. Finalmente, são feitas observações sobre o valor da criptografia e exclusão estratégica como medidas para reforçar a privacidade.
Palavras-chave: Violações de Privacidade de Ordem Zero. Privacidade. Agentes Artificiais. Dados. Informação.

*Professor of philosophy at the Universidade Federal do Mato Grosso (UFMT). PhD in philosophy from the Universidade Federal do Rio de Janeiro (UFRJ). E-mail: berr.alonso@gmail.com. ORCID: https://orcid.org/0000-0003-3595-4907.

> Each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and social norms set by the society in which he lives.
> — Alan Westin, Privacy and Freedom, 1968

Introduction

At a glance, even though the only entity accessing our personal data is an artificial agent, e.g. "google bot", it does not change the fact that a privacy violation has occurred. Privacy to be understood in a normative way, treated as a collective moral value and human right. What is relevant, in the case of email, is what the artificial agent is capable of doing with that information, taking into account that mechanisms of natural language processing, data extraction and recognition of intents as well as domains of users' spoken and written language utterances are increasingly efficient (Liu et al. 2020, Vedula et al. 2020), be it language-specific or many languages approach (Pyysalo et al. 2020).

One major concern is the colossal amount of personal and sensitive data[1] being stored daily in databases of companies and governments, whose access policies do not necessarily respect the privacy of users. Some can point out that you should not be worried with digital privacy if you have nothing to hide, in the sense of doing something you are not supposed to. For those there is a simple but overwhelming answer. I have nothing to hide, but I have nothing to show you either, and as Edward Snowden once said "Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say" (Snowden 2015). A well-known mechanism that challenges our best intuitions about non-humans violating privacy is the so called Google AdSense, a program that allows publishers to serve automatic text, image, video, or interactive media advertisements, targeted to site content and audience. As an illustration, imagine a musician who exchanges emails with a friend about his guitar that is being repaired. After email exchanges both the musician and his friend

[1] "Personal data" refers to any piece of information that someone can use to identify, with some degree of accuracy, a person, for instance, email address, internet protocol address (IP), name, surname, geolocation, home and job addresses, advertising identifiers, gadgets identifiers, among others. "Sensitive data" makes reference to a subset of personal data which includes specific categories such as genetic and biometric data, ethnic group, sex orientation, political opinions and/or affiliations, religious beliefs, philosophical perspectives, purchase history, passwords, credentials, among other possible distinct information.

are seemingly receiving advertisements about musical instrument stores, audio streaming websites and the like. If you send an email containing the term "Rio de Janeiro" in the body of the text, advertisements about hotels in Ipanema, tickets to Carnival in Sapucaí or invites by social networking websites showing locals looking for the perfect match are serious candidates to populate the commercial space of your mailbox, as well as your near future web searches and social media content.

The Google company (LLC)[2] defends itself by pointing out the non-involvement of humans in the process.

> "The practice of automatic processing has caused some to speculate mistakenly that Google "reads" your emails. To be absolutely clear: no one at Google reads your Gmail, except in very specific cases where you ask us to and give consent, or where we need to for security purposes, such as investigating a bug or abuse." (Frey, S. 2018 p.1)

In a nutshell, it is contented that if humans do not directly read your communications and private conversations, your privacy has not been violated. However, the problem is not as simple as it seems or at least as some want to make it look like. With the advancement of practices such as datamining and machine learning, that enable artificial agents to identify patterns in large data sets and sophisticated statistical techniques that empower intelligent artificial agents to "learn" and potentially improve their performance, three questions are asked: to what extent can agents access our sensitive information[3]? Does it matter that it is not a human who is reading my email? Should we be concerned when information that we would not trust humans, as it concerns aspects of private life and information that users are not willing to share, is collected, stored and analysed by a mere program? The first question is difficult and properly tackling it is one of the ambitions of this article, on the assumption that artificial and natural agents make use of data and not all uses might be leveraged for profit[4]. Nonetheless, it seems that we already have the answer to the last two questions. Yes, it matters that non-humans access our data, and also yes, we must be concerned that information is manipulated by programs, after all it is the technical capabilities of programs and

[2] A limited liability company (LLC) is a business structure in the United States whereby the owners are not personally liable for the company's debts or liabilities. Limited liability companies are hybrid entities that combine the characteristics of a corporation with those of a partnership or sole proprietorship.

[3] "Information" considered as well-formed, meaningful, truthful data (Floridi 2004).

[4] For instance, data from a clinical trial of drugs commonly used to fight cholesterol was reused in a process to destroy a protein associated with nearly half of all known cancers (Parrales et al. 2016).

artificial agents that are relevant, not their ontological status.

Value of Privacy

In a seminal Harvard Law Review article "The Right to Privacy" (1890), Samuel Warren and Louis Brandeis argue that "political, social and economic" changes and "the right to be alone" impose on the law that it offers privacy protection of individuals. Responding to the technological changes of the time, the advent of photography, Warren and Brandeis claim that the general right to privacy should protect *mental life* that could be shared with others in order to offer "peace of mind" and the "right to one's personality", interpreted as a protection of the individual's autonomy (Warren and Brandeis 1890, p.200, 207). Although the Fourth Amendment already offered protection at a certain level of privacy at the time – search in homes and its interiors – the authors argue that the new technology is potentially intrusive and that it would be necessary to formalize protection under the rubric of privacy, a well-known formulation as the "control of information about oneself". This formulation does not say anything about the identity of the agent who is in control of the information obtained. In the case of Warren and Brandeis, a photograph taken by an automatic device that is mounted outside a person's home constitutes a violation of privacy, as the resident has no control over the dissemination of information. The mere "leak of information" already constitutes a breach of privacy, a breach that occurs when the photograph is taken and not when it is seen by someone.

Three major American justice cases echoed Warren and Brandeis' concerns. The first, *Olmstead v. United States* (1928), is a surveillance case in which the United States Supreme Court ruled that a warrant was not required for federal agents to implant wiretapping. The court asserted that the Fourth Amendment only protected citizens from "physical intrusions" by law enforcement officials[5]. In 1967 the United States Supreme Court changed that decision in the *Katz v. United States* in judging that tapping telephone conversations on public phones was a violation of the Fourth Amendment. For the court it was a case of "reasonable expectation of privacy" in public places. Finally, in 1995 the United States military court cited Katz's case in determining that an individual has a reasonable expectation of privacy in his private email, even if stored and sent by an online service. The right to privacy of

[5]Without taking into account that federal agents at some point invade the private space to implant wiretaps. The invasion criterion is taken in this case as non-physical due to the fact that electronic devices capture the conversations, and not people themselves, which does not make sense if we take the eavesdropping as mere artefacts that facilitate the listening of agents in the end.

information has since been understood not only against surveillance and monitoring or searches without mandate, but also against appropriation and misuse of personal communications.

It is important to note that such determinations make no distinction or judgment based on the nature of the agent that violates the citizen's right to privacy. A common point in modern analyses of information privacy is the notion of "loss of autonomy", when the appropriation of information happens without the individual's consent. Lessig (2006, p.20) argues that the right to privacy provides a measure of dignity. He tests our intuitions with a hypothetical situation: The United States National Security Agency (NSA) releases a type of virus on the internet (worm) in order to try to find a file that is missing from your servers. This worm enters all computers on American soil residents and scans their hard drives. If it finds the file, the program sends a report to the NSA, if it does not find it, it continues scanning on other machines. This program is "smart" enough to use only ideal machine cycles, making the intrusion unnoticed. There is no disturbance, no content on the hard drive was sent to the government, not even illegal copies of music, books and movies which were eventually there. An artificial agent, not a human, examined my files. No human eye saw my data and yet our intuitions regarding the sense of dignity and personal autonomy were offended, as no permission was given by us to search our files and we were held as potential suspects until the scan was over.

The principle of privacy is based on the intuition that we experience moral damage in situations such as the example of Lessig. In this way, the right to privacy, regardless the nature of the agent involved in the violation, can be understood with normative weight and dignity as a moral good, as well as individual autonomy. Understanding informational privacy as an expression of autonomy and dignity, in addition to seeing it as a constitutional limitation to government and corporate power, enables the understanding of privacy as a moral good, liable to be protected from the assaults that changes in technological capabilities provide, due to increased efficiency in invasive scanning systems and datamining. When we can say that an artificial agent and its owner "are informed" or "hold information" it is crucial to determine if there was a breach in our privacy when accessing our data. One of the main points to be made is that the ability of the artificial agent to pass the information on to its owner is the relevant factor to be considered in this scena-

[6]Not to be mistaken with first degree, second degree privacy violation distinctions which are familiar to Law vocabulary. Second order privacy violation first appears at R. v. Duarte, [1990] 1 S.C.R. 30 in Austin 2003, p.141 and then Etzioni 2014, p.641. It is not a common terminology in Law parlance.

rio, also known as second order privacy violation[6]. Artificial agents should be considered as repositories of legally relevant information on behalf of their owners, a tempting approach if we consider that most of the information held by large corporations and governments is in the form of electronic files.

A distinction is suggested between electronic records ready to be used, considered as part of the corporation's knowledge despite human knowledge of its contents[7], and physical records about which no knowledge is presumed without a human or artificial agent having been effectively informed about its contents. The attribution of knowledge, therefore, does not depend on the traditional notion of transmitting information as in meetings, orders, letters, bulletins or telephone calls between members of a company's management hierarchy. Rather, it depends on the functions granted to agents, natural or artificial. If information is made available in corporation's databases, even if no employee of the corporation has read about that piece of information, the corporation and its agents, human and artificial, are the holders of the information and liable to knowledge from it.

Who is reading my email? A well known type of marketing and ad strategy used by Google in Gmail service is a major concern given the vast popularity of the platform. One of the answers that is usually given by the company is that users are free to give up part of their privacy, and are constantly asked if they want to give it up in exchange for certain services — the too long to read infamous "privacy policy" —, and further says that there is no real problem of privacy violation based on the fact that humans are not reading users' emails.

> 1. Is Google reading my email? No. Google scans the text of Gmail messages in order to filter spam and detect viruses, just as all major webmail services do. Google... uses this scanning technology to deliver targeted text ads and other related information. This is completely automated and involves no humans. (http://mail.google.com/mail/help/about_privacy.html).

However, thirty-one international organizations dealing with civil liberties have a different position:

> 2. (...) a computer system, with its greater storage, memory, and associative abi-

[7] Also *new* content that is systematically crunched and extracted through machine learning, data crossing and various other techniques.

> lity than a human's, could be just as invasive as a human listening to the communications, if not more so. (http://www.privacyrights.org/ar/GmailLetter.htm).

The fact that humans are not involved in reading users' personal electronic correspondence does not seem to be relevant either in the legal or moral spheres. The same argument extends to various social media platforms, virtual reality gadgets, smartphones, smartwatches, and virtually all technological services and artefacts that collect personal data and usage statistics.

However, the Google privacy policy recognizes the automated process of reading emails and it is also said that if the information extracted through the automated reading process were passed on to third parties, such a practice would be a misdeed, allowing most users feel free to exchange emails of all sorts of subjects and levels of intimacy. But, that comfort is not a defence against breach of privacy. At this time, Google is able to identify users who are interested in terrorism, Nazism or child pornography. People with interests in such matters may have reasons considered pertinent or sometimes even innocent, whether they are academics, bailiffs at work, individuals motivated by mere curiosity or even those who arrive at such websites by accident. However, it is known that other groups of individuals have interests, say, not at all innocent on those topics. Information of this nature is an extremely valuable commodity in today's world.

Profiling can go very wrong depending on context, depending on governments, depending on maybe too many variables. The profiling of billions of users who daily interact with different services of companies like Google allow any well tailored advertising to be super efficient, and as companies naturally aim at profit, we have to admit the grim possibility of any well tailored advertising to the highest bidder.

While the big data collected and crunched by companies can be processed and analysed in order to find patterns and paths that lead to potential malefactors, also services and applications offered by tech companies have an increasingly abundant reach and power to collect data, compute and generate patterns, profiling, and whatever they want to sell with amazing efficiency, even elections results[8].

[8]Pace 2016 Cambridge Analytica US elections and Brexit scandals using Facebook, Google and Youtube data. Cambridge Analytica alongside its parent company Strategic Communications Laboratories had worked in more than 200 elections across the world, including Kenya, Brazil, Nigeria, Mexico, India and Malaysia (Kleinman 2018).

Zero-Order Violations

I claim that a new kind of violation of privacy called *zero-order privacy violation* is a grounding practice within a new type of human exploitation, namely, data colonialism: massive appropriation of social life through data extraction, acquiring digital territory and resources from which economic value can be extracted by capital (Couldry Mejias, 2019). But, first I need to explain what a zero-order privacy violation is.

It seems that Google does not *read* my email, as software do not yet have a semantic analysis capability that we can commonly call "reading" in a strong sense. However, we can argue that the process of extracting information from sets of data is compromising enough. It also seems that artificial agents do not know what we are saying and what emotions we want to express about what we are talking about. Be that as it may, companies can refine their software to allow content (or part of it) on the web to be scanned and gradually assimilated and known by the programs. Machine learning algorithms build mathematical models based on sample data, known as "training data", in order to make predictions or decisions without being explicitly programmed to do so (Caliskan et al. 2017). Systems can categorize data in a way that clean, well formed and meaningful data standards are respected, so that in the end valuable information can be extracted. This can be done not only by the types of subjects matters internet users refer to, but also by the type of relationship a user has with the subject and what reactions to the referenced topics have possibly been expressed.

Empowered by tech companies, advertisers can go deeper and deeper into the consumer's desires. Based on consumer's expectations, general characteristics, social class, skin colour, religious affiliations, sexual preferences, political tendencies, intellectual aspirations, fears and desires, tech companies are able to draw increasingly accurate profiles of their target audience. Perhaps companies such as Google do not yet read my email in the strict sense, but actively use information extracted from communications for their own purposes in a non-transparent way, which constitutes a severe risk to privacy.

Etzioni (2014, p.642) says that when Warren and Brandeis published their innovative article "considered the 'genesis of the right of privacy,' they were not concerned about gossip *per se* (a first order privacy violation), but about the wider distribution of intimate details through the media", i.e., second order privacy violations are not about direct violations of privacy such as pocket inspections by jealous lovers, peeping tom, wiretapping or any sort of direct unsolicited appropriations of information. Second order violations concern

what is done to content after its appropriation. It is about the distribution of information and the process of drawing attention to the public.

Diversely, a zero-order privacy violation is not necessarily related to distribution of content as in cases of second order violations, neither it is a direct violation like first order ones. Born in the digital age or what Floridi calls Fourth Revolution era (Floridi 2014), this type of violation is a systematic and automated harvesting of data, linked to new technologies exploitation — from social media to IoTs (internet of things) — and often associated with tracking and profiling users, alongside information asymmetry phenomenon[9]. Everyday users do not know the full range of data that connected devices generate or what is collected and extracted by servers, therefore they are not able to commit into protecting themselves. Zero-order violations are better understood through the perspective of what security industry calls *zero-day*, i.e., a computer-software vulnerability that is unknown to those who should be interested in mitigating the vulnerability. So, until the vulnerability is patched, hackers can exploit it to adversely affect computer programs, harvesting data, modifying additional computers behaviours and networks. The relation to zero-days vulnerabilities by itself is sufficient to distinguish a zero-order privacy violation from first and second order ones, given the spooky, omnipresent and novel nature of such practice. But, there is another peculiarity to a zero-order violation making it rather heterogeneous to commonly known types of privacy violations. Zero-order privacy violations are also closely related to what Kit Fine calls *zero-grounded* statements (Fine 2012, p.47), but a discussion of this matter is way beyond the scope of this paper[10], yet I must take into consideration a key point about its grounding[11] nature. According to Fine, there is a distinction to be made between truths that do not have grounds (ungrounded), and truths that are grounded in the empty plurality of truths T (Fine 2017). The truth that "if it is raining then it is raining" is an example of the latter. I take it that a zero-order violation can be read as a mere "it leaks", and if a vulnerability cannot be mitigated because of reasons yet to be known in a future time, "if it leaks, then it leaks". And when the cause of the leakage is known and named, the sentence can still be read

[9]Concept developed in economics, which extends to non-economic behaviour such as International Relations theory. Roughly speaking it deals with the study of decisions in transactions where one party has more or better information than the other. A straightforward example is the asymmetric information between what national leaders know at a certain time t, given the discrepancy in resources, before going into war. (Jackson and Morelli 2011).

[10]A detailed defence of zero-order privacy violations using the notion of Kit Fine's truth maker semantics for grounds can be found in Alonso, B. "What is a zero-order privacy violation?" *forthcoming* (2021).

[11]Simply put, in a conditional the antecedent grounding or being a ground for the consequent fact, making some sort of modal connection between explanandum and explanans (Fine 2012, p.38)

as a plausibly zero-grounded necessity if conceded that cases of kripkean necessities a posteriori such as "water is H_2O" are also zero-grounded (De Rizzo 2020), i.e., it was always leaking, but we did not know about it (nor had a name for it).

Scenarios like Covid-19 pandemic make a perfect case to expand surveillance via tracking applications, since governments, international agencies and tech companies have all announced measures to help contain the spread of the Coronavirus, facilitating unprecedented levels of data exploitation around the world. Complicity between tech giants and governments to liberalise international data flows in the name of saving economies and keeping world populous healthy allow corporations for cross-border data transfers without regard for rules that guarantee minimum data protection standards. Governments' poor understandings of technology, and their hopes for an easy fix only empower huge corporations to consolidate and expand their dominium. Eventually governments started to capitalise on tracking as well, since elections in many countries happened or are about to happen in the middle of the pandemic period. Opposition and dissidents can be easily tracked, possibly having their behaviour predicted and manipulated. With worldwide contact tracing apps working without any regard to privacy in a temporary emergency period, no government has ever known as much about their citizens as they do.

Final remarks

Some convincing arguments see in Big Data processing the mechanism for a new stage of capitalism (Cohen 2018), while others critically point out that data colonialism is a combination of predatory extractive practices of historical colonialism with the abstract quantification methods of computing (Couldry Meijas 2019, p.121), when data abstracts life by converting it into information that can be stored and processed by computers and appropriates life by converting it into value for a third party. We have learned that during periods of global distress not only companies capitalise on mass surveillance and tracking grounded on zero-order violations, but also governments use crisis as an opportunity to expand their powers via planned authoritarianism.

As a rule, agents assume that some content is by default an instance of information. What they often speculate and generally disagree upon is whether and how far that content may contribute to the formulation of their choices, the development of their decision processes and goals. In the face of contemporary challenges to privacy and autonomy, last remarks on the value of cryptography and the simple practice of de-

leting personal information are made in a very practical manner. In contempt of *keeping* and *deleting* rivalry, three categories of what to delete are introduced (plus prophylactic considerations when suited):

(1) Have to delete: necessary for a healthy online life, this category is related to basic urgent security measures, such as deleting sensitive information on social media platforms, credit cards details from unprotected files, plain text passwords, payments data (can also be preventive by not letting websites and/or applications record data, if option available), old useless files and garbage in general (obvious garbage like old system's install files, malware, uninstalled apps leftovers and salient vulnerabilities);

(2) Should delete: files that can be compromising in long run scenarios, such as internet cache, cookies, trackers (minimize web fingerprints), most social media platforms' content (not only sensitive information as in 1), files and programs you no longer work with nor will work anymore, e.g. that album of a band someone said it is incredible, however after downloading it you disliked the music but kept it anyway since why not mindset of having available incredibly large spaces of storage for accessible figures.

(3) Could delete: Agents can in principle delete all their information, trivially. However, taking for granted some sort of strict necessitist stance, i.e. "agents necessarily can delete their info", is quite a naive move and would make this category innocuous. The role of this third category is of a relational nature: to package control/version control what could actually be deleted and thus avoid accidental deletion of files which necessarily can't be erased given relevance criterion. Family pictures, doctoral thesis text files, work projects, encrypted passwords, among others.

Promises of anonymization on the Web have to deal with the paradox of learning nothing about an individual while learning useful information about a population, and the fact that data cannot be fully anonymized and remain useful (Dwork Roth 2014, p.217). As a rule internet users should encrypt everything. The very nature of zero-order violations make the cat and mouse play a dangerous game, a virtually impossible to win one.

References

AUSTIN, L. (2003). "Privacy and the Question of Technology". *Law and Philosophy* 22:119-166.

COHEN, Julie E. 2018. "The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy." *Philosophy Technology*. 31 (2): 213–33.

COULDRY, N.; MEIJAS, U. (2019). *The Costs of Connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.

CALISKAN, Aylin; BRYSON, Joanna J.; Narayanan, Arvind. (2017). "Semantics derived automatically from language corpora contain human-like biases". *Science*. 356 (6334): 183–186. arXiv:1608.07187.

DOWRK, C.; ROTH, A. (2014). "The Algorithmic Foundations of Differential Privacy". *Nos*. Vol. 09 3-4:211-417.
ETZIONI, A. (2014). "A Cyber Age Privacy Doctrine: A Liberal Communitarian Approach". *I/S Journal of Law and Policy for the Information Society*, 10 (2):641-669.
DE RIZZO, J. (2020). "Grounding grounds necessity". *Analysis*. anz083.
FINE, K. (2012). Guide to ground. In *Metaphysical Grounding: Understanding the Structure of Reality*, eds. F. Correia and B. Schnieder, 37–80. Cambridge: Cambridge University Press.
FINE, K. 2017. A theory of truthmaker content I: conjunction, disjunction and negation. *Journal of Philosophical Logic* 46: 625–74.
FLORIDI, L. (2004). "Outline of a Theory of Strongly Semantic Information". *Minds and Machines* 14: 197.
FLORIDI, L. (2014). The 4th Revolution: How Infosphere is Reshaping Human Reality. Oxford University Press.
FREY, S. (2018, July 3). Ensuring your security and privacy within Gmail [blog post]. Retrieved from https://www.blog.go-ogle/technology/safety-security/ensuring-your-security-and-privacy-within-gmail.
JACKSON, Matthew O.; MORELLI, Massimo (2011). "The Reasons for Wars – an Updated Survey". In Coyne, Chris J.; Mathers, Rachel L. (eds.). *The Handbook on the Political Economy of War*. Edward Elgar Publishing.
KLEINMAN, Z. (2018, March 20). Cambridge Analytica: The data firm's global influence. Retrieved from https://www.b-bc.com/news/world-43476762.
LESSIG, L. (2006). *Code: version 2.0*, Basic Books, New York.
LIU et al. (2020). "Evolving Normalization-Activation Layers", *Machine Learning*, arXiv:2004.02967 [cs.LG].
PARRALES et al. (2016). "DNAJA1 controls the fate of misfolded mutant p53 through the mevalonate pathway". *Nature Cell Biology*, 18 (11): 1233.
PYYSALO et al. 2020. "WikiBERT models: deep transfer learning for many languages". *Computation and Language*, arXiv:2006.01538 [cs.CL].
SNOWDEN. E. (2015). Just days left to kill mass surveillance under Section 215 of the Patriot Act. We are Edward Snowden and the ACLU's Jameel Jaffer. AUA. • /r/IAmA". Reddit. Retrieved at https://www.reddit.com/r/IAmA/comments/36ru89/just_days_left_to_kill_mass_surveillance_under.
VEDULA et al. (2020). "Automatic Discovery of Novel Intents Domains from Text Utterances". *Computation and Language*, arXiv:2006.01208 [cs.CL].
WARREN BRANDEIS. (1890). "The Right To Privacy". *Harvard Law Review*. Vol. IV, 5.
WESTIN, A. (1968). Privacy and Freedom (Fifth ed.). *Atheneum*, New York.
https://en.wikipedia.org/wiki/Olmstead$_{v.}{}_{U}nited_{S}tates$. Retrieved 12-07-2020.

Received / Recebido: 30/09/2020
Approved / Aprovado: 13/01/2021
Published / Publicado: 31/01/2021