

# IJDL

## International Journal of DIGITAL LAW





# Segurança pública e inteligência artificial: novos paradigmas

## *Public security and artificial intelligence: new paradigms*

**Rogério Gesta Leal\***

Universidade de Santa Cruz do Sul (Santa Cruz do Sul, Rio Grande do Sul, Brasil)  
rleal@unisc.br  
<https://orcid.org/0000-0003-1372-6348>

**Recebido em/Received:** 31.08.2024 / August 31<sup>st</sup>, 2024

**Aprovado em/Approved:** 28.09.2024 / September 28<sup>th</sup>, 2024

**Resumo:** O objeto de estudo do presente trabalho é enfrentar a problemática das condições e possibilidades de políticas públicas de segurança com o uso de inteligência artificial e tecnologias de informação, levando em conta direitos e garantias fundamentais individuais e sociais demarcadas pelo Estado democrático de direito, nomeadamente no Brasil. A hipótese e proposta de enfrentamento destas questões se dá a partir do estabelecimento de marcos normativos claros e políticas de garantias por parte do Estado, a partir do que tais políticas podem se instituir e desenvolver, com permanente controle interno e externo, notadamente social.

**Palavras-chave:** Segurança pública; políticas públicas; direitos fundamentais; Estado de direito; controle de políticas públicas.

**Abstract:** The object of study of this work is to confront the problem of the conditions and possibilities of public security policies with the use of artificial intelligence and information technologies, taking into account fundamental individual and social rights and guarantees demarcated by the Democratic Rule of Law, namely in Brazil. The hypothesis and proposal for tackling these issues is based on the establishment of clear normative frameworks and guarantee policies by the State, from which such policies can be instituted and developed, with permanent internal and external control, notably social.

Como citar esse artigo/*How to cite this article:* LEAL, Rogério Gesta. Segurança pública e inteligência artificial – Novos paradigmas. *International Journal of Digital Law*, Belo Horizonte, ano 5, n. 2, p. 81-99, maio/ago. 2024. DOI: 10.47975/digital.law.vol.5.n.2.leal.

\* Professor Titular da Universidade de Santa Cruz do Sul (Santa Cruz do Sul-RS, Brasil) e da Fundação Superior do Ministério Público do Rio Grande do Sul – FMP (Porto Alegre-RS, Brasil), nos cursos de Mestrado e Doutorado em Direito. Doutor em Direito pela Universidade Federal de Santa Catarina – UFSC e pela Universidad Nacional de Buenos Aires. Mestre em Desenvolvimento Regional da Universidade de Santa Cruz – USC. Graduado em Direito pela Universidade de Santa Cruz do Sul. Desembargador do Tribunal de Justiça do Estado do Rio Grande do Sul. *E-mail:* rleal@unisc.br.

**Keywords:** Public security; Public policies; Fundamental rights; Rule of law; Control of public policies.

**Sumário:** 1 Notas introdutórias – 2 Sociedade do conhecimento x sociedade de vigilância – 3 Reações à sociedade da vigilância: perspectivas – 4 Notas conclusivas – Referências

## 1 Notas introdutórias

É inegável que, em todas as áreas da vida, a inteligência artificial (IA) tem se mostrado cada vez mais presente e com mais funcionalidades, que facilitam nas tarefas do cotidiano.<sup>1</sup> Por apresentar sofisticação e otimização tecnológica, pode facilmente ser percebida como ferramenta que é destituída de erros, não apresentando preconceitos e estereótipos, características comumente atreladas ao ser humano. Todavia, se vivemos numa sociedade na qual tudo que (re)produzimos é atravessado por fatores históricos, de natureza cultural e social, por que as IAs – criadas pelo homem – também não replicariam estigmas relacionados à classe, raça, gênero, etnias, dentre outros?<sup>2</sup>

A *algoritmização da vida*,<sup>3</sup> que está presente nas redes sociais e *streamings*, e tem ganhado espaço em inúmeros campos, tem influenciado cada vez mais políticas de segurança pública. A despeito disto, problemas de discriminação e preconceito estrutural em determinadas políticas desta natureza continuam os mesmos, e o uso discriminatório e preconceituoso da IA não pode tirar a responsabilidade do Estado no ponto (porque, se houve erro, foi culpa do algoritmo, e não de quem programou).<sup>4</sup>

É interessante perceber esse paralelo: por um lado, a tecnologia é colocada como solução, mas ao mesmo tempo a sociedade civil em diferentes momentos vai contestar isso.

<sup>1</sup> Um exemplo claro é o uso da inteligência artificial na tomada de decisões judiciais e administrativas: VALLE, Vivian Lima López; FUENTES I GASÓ, Josep Ramón; AJUS, Atílio Martins. Decisão judicial assistida por inteligência artificial e o Sistema Victor do Supremo Tribunal Federal. *Revista de Investigações Constitucionais*, Curitiba, v. 10, n. 2, e252, maio/ago. 2023. DOI: 10.5380/rinc.v10i2.92598; BITENCOURT, Caroline Müller; MARTINS, Luisa Helena Nicknig. A inteligência artificial nos órgãos constitucionais de controle de contas da administração pública brasileira. *Revista de Investigações Constitucionais*, Curitiba, v. 10, n. 3, e253, set./dez. 2023. DOI: 10.5380/rinc.v10i3.93650; TOLEDO, Claudia; PESSOA, Daniel. O uso de inteligência artificial na tomada de decisão judicial. *Revista de Investigações Constitucionais*, Curitiba, v. 10, n. 1, e237, jan./abr. 2023. DOI: 10.5380/rinc.v10i1.86319; SIERRA CADENA, Grenfieth de Jesus. Implementación de la Inteligencia Artificial en las Altas Cortes de Colombia: los casos de la Corte Constitucional y el Consejo de Estado. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 11, n. 1, e253, ene./jul. 2024. DOI 10.14409/redoeda.v11i1.13824.

<sup>2</sup> SÁNCHEZ DÍAZ, María Fernanda. El impacto de la inteligencia artificial generativa en los derechos humanos. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 11, n. 1, e252, ene./jun. 2024. DOI: 10.14409/redoeda.v11i1.13612.

<sup>3</sup> PUSCHEL, André Felipe Silva; RODRIGUES, Roberto Tassis; VALLE, Vivian Cristina Lima López. O dilema ético da decisão algorítmica na administração pública. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 22, n. 90, p. 207-226, out./dez. 2022. DOI: 10.21056/aec.v22i90.1737.

<sup>4</sup> RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. Personal data protection and State surveillance: the risks of digital discrimination and the Federal Supreme Court's vision. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 22, n. 90, p. 63-85, out./dez. 2022. DOI: 10.21056/aec.v22i90.1658.

São estes cenários e seus riscos, assim como iniciativas para controlá-los, que este trabalho pretende abordar. Para tanto, elegemos como objetivos específicos: (i) demarcar as relações entre sociedade do conhecimento e sociedade da vigilância; (ii) as reações institucionais e políticas à sociedade de vigilância; (iii) propor premissas viabilizadoras de políticas de segurança pública democráticas para o uso de novas tecnologias com o uso de IA no âmbito da segurança pública.

Pretendemos utilizar neste trabalho o método dedutivo, testando nossas hipóteses com os fundamentos que passam a ser declinados. Utilizaremos, para tanto, técnica de pesquisa com documentação indireta, nomeadamente bibliográfica.

## 2 Sociedade do conhecimento x sociedade da vigilância

O termo “sociedade da informação” foi incorporado nos últimos anos no discurso político, acadêmico e midiático global. Manuel Castells afirma que esta sociedade é um novo sistema tecnológico, econômico e social; uma economia na qual o incremento de produtividade não depende do incremento quantitativo dos fatores de produção (capital, trabalho, recursos naturais), mas de aplicação de conhecimentos e informação na gestão, produção e distribuição, tanto nos processos como nos produtos.<sup>5</sup>

Estas sociedades se caracterizam por serem baseadas no conhecimento e nos esforços para converter informação em conhecimento. Quanto maior a quantidade de informação gerada por uma sociedade, maior será a necessidade de convertê-la em conhecimento.

Um aspecto de singular relevância no desenvolvimento das “sociedades da informação e do conhecimento”, pois, é a *velocidade* com que a informação é gerada, transmitida e processada. Hoje, a informação pode ser obtida de forma praticamente instantânea e, muitas vezes, da mesma fonte que a produz, transcendendo fronteiras e limitações de espaço e tempo.

Embora existam várias interpretações sobre a amplitude e o significado do conceito desta sociedade, o certo é que nela são reconfiguradas as formas como todas as pessoas realizam a maior parte das suas atividades, a partir de novas formas de empreender e realizar ações quotidianas; portanto, podemos afirmar que ela é também síntese de mudanças de paradigmas estruturais em múltiplos campos da vida.<sup>6</sup>

<sup>5</sup> CASTELS, Manuel. *La sociedad en red – La era de la información. Economía, sociedad y cultura*. Madrid: Alianza Editorial, 1997. v. 1. p. 67.

<sup>6</sup> Tratamos de forma mais aprofundada disto no livro LEAL, Rogerio Gesta. *Segurança pública no Estado democrático de direito – Avanços e recuos*. São Paulo: Tirant lo Blanch, 2023.

Alvin Toffler, no início da década de 1980, antecipou com singular clareza o advento da sociedade da informação, lembrando que, há mais de 10 mil anos, a primeira onda introduziu mudanças importantes na história, impulsionada pela revolução agrícola, transformando as condições de vida dos primitivos caçadores e coletores, que formaram sociedades camponesas nas quais a produtividade dependia principalmente da demonstração de força humana e animal, bem como do sol, vento e água. Os beneficiários desta transformação foram aqueles que entenderam que a nova organização estaria focada no campo.<sup>7</sup>

Com a segunda onda, a revolução industrial desencadeou mudanças profundas na história,<sup>8</sup> dando origem a uma nova civilização centrada na indústria e na produção em grande escala. A produtividade dependia da relação que o homem estabelecia com as máquinas. Aqueles que não compreenderam o significado e o alcance da racionalidade imposta pela nova ordem ficaram para trás, significativamente limitados nas suas capacidades de produção.

A terceira onda introduz, por sua vez, uma nova sociedade, que se assenta na informação, no conhecimento e na criatividade. Nestas sociedades, a produtividade depende do desenvolvimento de novas tecnologias, que – afirma Toffler – permitiriam ao homem fazer menos e pensar mais. Ou seja, o desenvolvimento de tecnologias avançadas de informação e comunicação permite a configuração de novo espaço social, como um terceiro ambiente, marcado por inéditos modelos de mercados, culturas e percepções do mundo.<sup>9</sup>

Imaginava-se que, neste novo mundo de possibilidades infinitas de conhecimento/ilustração, a racionalidade humana chegaria a um nível de excelência que seria capaz de desenvolver a vida e relações humanas de forma mais civilizada e sustentavelmente, com harmonia, justiça social e *segurança*. Ledo engano!

Um inédito *marco paradigmático de colapso* desta sociedade do conhecimento/informação: os ataques terroristas do 11.9.2001 das torres gêmeas, de New York (EUA), inauguraram o que podemos chamar de quarta onda civilizatória: a Era Panóptica da Sociedade da Vigilância.

Quando imaginávamos que as novas tecnologias geradas pela sociedade da informação poderiam nos assegurar a prevenção de problemas das mais diversas ordens, estas têm se revelado impotentes diante de contínuas situações de emergências, riscos e perigos que vão se criando hodiernamente em todo o globo,

<sup>7</sup> TOFFLER, Alvin. *La tercera ola*. México: Edivisión, 1981. p. 81.

<sup>8</sup> MARTNEZ GARBIRAS, María Margarita; SÁNCHEZ-HUERTAS, Luis Fernando. Los atajos de la Cuarta Revolución Industrial a la democracia: una reflexión de lecciones aprendidas en clave de Lafont y Berlin. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 23, n. 94, p. 43-62, out./dez. 2023. DOI: 10.21056/aec.v23i94.1725.

<sup>9</sup> Neste sentido DAVARRA RODRIGUEZ, Miguel Angel. *De las autopistas de la información a la sociedad virtual*. Madri: Aranzadi Editorial, 2008. p. 51 e seguintes.

provocadas por atos terroristas e de violência imensos, bem como por fatores ambientais, de consumo, energéticos, raciais, étnicos, biológicos, de criminalidades, dentre outros, atestando ser ilusória a crença de que, por meio do conhecimento e das inovações tecnológicas, nos libertaríamos de quaisquer medos, deixaríamos de ser criaturas e passaríamos a ser criadores da comunidade em que vivemos.<sup>10</sup>

Em outras palavras, medos e incertezas, como nos indica Mongardini, continuam a ser traços cada vez mais característicos de nossos quotidianos,<sup>11</sup> e bastou um vírus microscópico, gerador da Covid-19,<sup>12</sup> para voltarmos a nos encontrar sozinhos e desesperados! De repente regressamos ao tempo da terrível gripe espanhola,<sup>13</sup> com as mesmas máscaras, com os mesmos medos, mas sobretudo com os mesmos erros, como exemplo, o de não revelar à sociedade a propagação da doença em tempo certo; ou, pior ainda, o de comunicar notícias manipuladas e muitas vezes até falsas,<sup>14</sup> nomeadamente por redes sociais virtuais, justamente aquelas que poderiam em muito auxiliar os cenários trágicos que passamos.

<sup>10</sup> Ver o excelente texto de Ver o excelente texto de HARARI, Yuval Noah. *Homo Deus*. Uma breve história do amanhã. São Paulo: Companhia das Letras, 2016. Ver igualmente o texto de DOMINICI, Piero. *La società dell'irresponsabilità*. Milano: Franco Angeli, 2015. p. 28 e seguintes.

<sup>11</sup> MONGARDINI, Carlo. *Le dimensioni sociali della paura*. Milano: Franco Angeli, 2010. p. 46. Na mesma linha o excelente texto de ZOLO, Danilo. *Sula paura – Fragilità, aggressività, potere*. Milano: Feltrinelli Editore, 2011. p. 49 e seguintes. Neste texto o autor se pergunta: “perché così spesso la paura mi rendeva aggressivo e perché l'aggressività mia e la prepotenza degli altri erano strettamente intrecciate. Mi domandavo, in sostanza, qual era il rapporto fra la paura, l'aggressività e la violenza scatenata dai miei simili nel corso dei millenni” (p. 11). É importante debater esses temas, pois, muitas vezes, como cita o autor, lembrando de Arnold Gehlen: “Con grande abilità abbiamo sospinto la morte al di fuori del nostro campo visivo. La morte gioca dietro porte laccate di bianco”.

<sup>12</sup> Sobre os impactos jurídicos da Covid-19 nos direitos humanos e no direito administrativo, ver: CASTILLO ARJONA, Mónica. El fenómeno de la Covid-19 y sus efectos sociales en el derecho administrativo del siglo XXI. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 8, n. 1, p. 173-187, ene./jun. 2021. DOI: 10.14409/redoeda.v8i1.9548; SÁNCHEZ DIAZ, María Fernanda; ROMERO TELLO, Ana Guadalupe. Covid-19, Derechos Humanos y Estado frente al manejo de la Pandemia. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 8, n. 1, p. 233-254, ene. /jun. 2021. DOI 10.14409/redoeda.v8i1.9525; HERNANDES, Luiz Eduardo Camargo Outeiro; PIOVESAN, Flávia. Desafios judiciais em tempos de pandemia: fortalecendo o diálogo entre a Comissão Interamericana de Derechos Humanos e o Supremo Tribunal Brasileiro para a proteção dos direitos humanos. *Revista de Investigações Constitucionais*, Curitiba, v. 9, n. 2, p. 371-388, maio/ago. 2022. DOI: 10.5380/rinc.v9i2.86138; NÓBREGA, Marcos; HEINEN, Juliano. As forças que mudarão a Administração Pública pós-Covid: transparência 2.0, blockchain e smart contracts. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 21, n. 85, p. 217-230, jul./set. 2021. DOI: 10.21056/aec.v21i85.1405; RODRÍGUEZ-ARANA MUÑOZ, Jaime. Administrative Law and human dignity (on the post-pandemic reconstruction of Administrative Law). *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 22, n. 88, p. 11-33, abr./jun. 2022. DOI: 10.21056/aec.v22i88.1646; BOMTEMPO, Eugênio Morais; CARMONA, Paulo Cavichioli. A solidariedade social na pandemia de Covid-19. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 22, n. 89, p. 251-276, jul./set. 2022. DOI: 10.21056/aec.v22i89.1662.

<sup>13</sup> A *gripe espanhola* foi causada por um vírus influenza que se espalhou pelo mundo entre 1918 e 1919, não se sabendo ao certo de onde partiu, tendo causado a morte de cerca de 50 milhões de pessoas, sendo que algumas estatísticas falem em até 100 milhões de mortos, conforme dados coletados no *site*: <https://www.historiadomundo.com.br/idade-contemporanea/gripe-espanhola.htm>. Acesso em: 22 mar. 2023.

<sup>14</sup> VALLE, Vivian Cristina Lima López; RUIZ, María Guadalupe Fernandes; BÜTTNER, Marcielly. Fake news, influência na formação da opinião pública e impactos sobre a legitimidade da decisão pública. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 24, n. 95, p. 73-97, jan./mar. 2024. DOI: 10.21056/aec.v24i95.1898.

Estes fatos têm nos demonstrado como a construção social dos riscos e perigos que nos cercam (entendidos como atributos socialmente construídos) tem fornecido bases teóricas e empíricas sólidas para o desenho de políticas muitas vezes autoritárias (inclusive de segurança pública). Daí porque autores como Ferrajoli insistem na tese de que o neoconstitucionalismo, para estar à altura destes novos desafios, deve construir garantias capazes de criar alternativas racionais e credíveis às previsões de um futuro caracterizado pela incerteza, violência, desigualdade e devastação ambiental.<sup>15</sup>

Mesmo que as Constituições contemporâneas tenham se ocupado de criar instrumentos de gestão de crises, é preciso permanentemente refletir sobre possível paradoxo de regimes democráticos que conseguem se autodestruir usando processos e procedimentos (por eles criados) de forma antidemocrática. Como nos dizem D'Agostini e Ferrera, em tempos de crise é fácil superestimar a necessidade de segurança e subestimar o valor da liberdade; e isto porque, sem segurança, não há liberdade.<sup>16</sup> Mas também é verdade que a história constitucional hodierna nos mostra claramente como a ruptura da proteção dos direitos e liberdades em nome da defesa da segurança está presente desde há muito.<sup>17</sup>

Por isto podemos dizer que a segurança, enquanto bem constitucional multifacetado e polissêmico, pode se dar em sentido material e ideal; objetivo e subjetivo; individual e coletivo; interno e externo, submetendo-se cada vez mais, e de forma ordinária, a juízos de ponderação com outros interesses de importância constitucional, mesmo além de ambientes de emergência tradicionais. Como nos diz Walzer, sem segurança nenhuma forma de representação política baseada no consenso é possível; e a liberdade, aqui, figura como aquela tranquilidade de espírito decorrente da convicção de se estar seguro.<sup>18</sup>

Por todas estas razões, a prevenção e a precaução tornaram-se, nos dias atuais, as *règles de droit*<sup>19</sup> por excelência, o mantra de todas políticas públicas

<sup>15</sup> FERRAJOLI, Luigi. *La democrazia attraverso i diritti*. Roma: Laterza, 2013. p. 27.

<sup>16</sup> D'AGOSTINI, Franca; FERRERA, Maurizio. *Le verità del potere – Sei diritto aleatici*. Roma: Einaudi, 2019. p. 81. Em verdade, a história já nos ensinou que por trás do aparente império da lei há sempre homens que governam e legislam, razão pela qual toda a norma jurídica está destinada a formalizar vontades/desejos e escolhas de poder.

<sup>17</sup> No ponto ver o excelente texto de COLE, David. *Enemy Aliens – double standards and constitutional freedoms in the war on terrorism*. New York: The New Press, 2003. p. 77. No mesmo sentido o livro de CERI, Paolo. *La società vulnerabile – Quale sicurezza, quale libertà*. Roma/Bari: Laterza, 2003. p. 38 e seguintes.

<sup>18</sup> WALZER, Michael. *La libertà e i suoi nemici nell'età della guerra al terrorismo*. Roma/Bari: Laterza, 2010. p. 43.

<sup>19</sup> Como quer VERHOEVEN, Charles Leben. *Le principe de précaution – Aspects de droit international et communautaire*. Paris: Éditions Panthéon-Assas, 2022. p. 41. Lembra-nos o autor que o princípio da precaução intervém quando convém adotar as medidas adequadas, mesmo face a riscos não totalmente apurados cientificamente, diferindo-se, pois, do princípio da prevenção, que, no entanto, opera quando a informação científica sobre o perigo e a nocividade são certos, concordantes e conclusivos.

preocupadas em minimizar riscos, perigos e medos capazes de prevalecer sobre outros direitos, e conformar a ação da administração pública como um todo. E em nome de tudo isto foram se criando políticas públicas globais – físicas e virtuais – de segurança máxima contra riscos e perigos conhecidos e desconhecidos, mesmo que em detrimento de alguns direitos e garantias fundamentais individuais a duras penas conquistados, como privacidade e intimidade.

Lembremos que foi sob o pretexto de sua cruzada contra o terrorismo internacional que o governo do Presidente Bush promoveu, pós-11.9.2001, iniciativas legislativas que impuseram restrições significativas à liberdade de expressão e aos direitos relacionados com a privacidade pessoal, dentre as quais: Estatuto de Escuta Telefônica, Lei de Privacidade de Comunicações Eletrônicas, Lei de Fraude e Abuso de Computadores, Lei de Vigilância de Inteligência Estrangeira, Lei de Direitos e Privacidade de Educação Familiar, Lei de Lavagem de Dinheiro, Lei de Imigração e Nacionalidade, Lei de Sigilo Bancário, Lei de Direito à Privacidade Financeira, Lei Patriótica dos EUA, e Lei Antiterrorismo de 2001.<sup>20</sup>

Para exercer funções panópticas eficazes sobre as informações que circulam pela internet, o governo do Presidente Bush promoveu a adaptação do quadro regulamentar referido, nomeadamente por meio do *USA Patriotic Act*, concedendo amplos poderes às áreas de segurança do governo para fiscalizar as informações que circulam na internet, autorizando a interceptar todas as comunicações que considerassem “suspeitas”.<sup>21</sup> Ao lado destas, criou também o programa CAPPs II (*Computer Assisted Passenger Pre-Screening*), pré-inspeção assistida por computador de passageiros.<sup>22</sup> Este sistema provém das informações que as companhias aéreas armazenam no registo dos passageiros, e inclui dados relativos às viagens realizadas, bem como possíveis antecedentes criminais e informações não especificadas.

Por outro lado, instrumentos de IA e novas tecnologias de acesso, coleta e gestão da informação podem ser, ao mesmo tempo, viabilizadores de espaços democráticos; mas também autoritário, basta vermos os regimes no Irã e da China, usando-as para suprimir a liberdade de expressão, aprimorar técnicas de vigilância, disseminar propaganda de ponta e pacificar suas populações com entretenimento

<sup>20</sup> “Wiretap Statute, Electronic Communications Privacy Act, Computer Fraud and Abuse Act, Foreign Intelligence Surveillance Act, Family Education Rights and Privacy Act, Money Laundering Act, Immigration and Nationality Act, Bank Secrecy Act, Right to Financial Privacy Act, USA Patriotic Act, Anti-Terrorism Act 2001” – conforme informações do site: <https://epic.org/privacy/terrorism/usapatriot/>. Acesso em: 27 abr. 2024.

<sup>21</sup> Já sabemos hoje que a internet pode, de fato, ser utilizada como meio capaz de desempenhar funções úteis de vigilância e controle individual e social, o que representa bem novo ciclo do panoptismo foucaultiano, conforme sua obra *FOUCAULT, Michel. Vigilar y castigar*. Nascimento de la prisión. México: Siglo XXI, 1983. p. 43 e seguintes.

<sup>22</sup> O sistema CAPPs está em funcionamento desde 1998 e provém dos ataques terroristas ocorridos durante os Jogos Olímpicos de Atlanta, em 1996, bem como do trágico desfecho do voo 800, da TWA, que em consequência de uma *avaria mecânica* colidiu com o Oceano Pacífico. Mais dados podem ser obtidos no site: <https://www.gao.gov/products/gao-04-385>. Acesso em: 27 abr. 2024.

digital alienante.<sup>23</sup> Para além disto, tem se formado um *capitalismo da vigilância*<sup>24</sup> a partir da IA e das redes sociais, com a instalação de grandes monopólios económicos caracterizadores do que se tem chamado de *feudalismo tecnológico*,<sup>25</sup> o que se percebe em corporações como Facebook, Google, Amazon, Apple, Microsoft, Netflix, governantes autocráticos e sem controle de cidadãos que ocuparam um espaço que se pensava ser coletivo.<sup>26</sup>

Por conta disto é que a Lei dos Mercados Digitais, recentemente aprovada pela Europa, estabelece um conjunto de critérios objetivos claramente definidos para qualificar grandes plataformas *on-line* como *gatekeepers*,<sup>27</sup> visando garantir que elas se comportem de modo a respeitar direitos e garantias individuais e sociais.<sup>28</sup>

A despeito disto, é em nome da segurança pública contra atos de terrorismo e de criminalidade organizada que vários governos têm desenvolvido programas de vigilância de seus cidadãos ao redor do mundo, como nos informa Federico Kukso, ao referir que, na China, bancos, aeroportos, hotéis e até banheiros públicos verificam a identidade das pessoas inspecionando seus rostos, por meio do *software* chamado *Xue Liang* (olhos agudos), que analisa milhões de imagens para rastrear pessoas, detectar comportamentos suspeitos e até prever crimes.<sup>29</sup> Demonstra o autor iniciativas governamentais – isoladas ou em colaboração global – para acessar dados e informações privados e públicos, de pessoas físicas e jurídicas, em nome da segurança preventiva e curativa, sem qualquer informação e prestação de contas àqueles que são atingidos por suas políticas.<sup>30</sup>

<sup>23</sup> Ver a interessante matéria publicada no *site*: <https://www.poder360.com.br/poder-tech/tecnologia/leis-rigorosas-garantem-controle-social-na-internet-chinesa/>. Acesso em: 30 abr. 2024.

<sup>24</sup> Tema bem explorado por ZUBOFF, Shoshana. *The age of surveillance capitalism*. New York: Perseus Books, 2019. p. 61 e seguintes.

<sup>25</sup> MOROZOV, Evgeny. *The net delusion: the dark side of internet freedom*. New York: Public Affairs, 2019. p. 38. Na mesma linha o livro de VAROUFAKIS, Yanis. *Technofeudalism*. London: Bodley Head, 2023. Para Varoufakis, as grandes empresas tecnológicas Meta, Amazon, Apple, Alphabet controlam a nossa atenção e medeiam as nossas transações, transformando os humanos em servos digitais que publicam, navegam e compram incessantemente nas suas plataformas. Em vez de perseguir os lucros que derivam do trabalho, os senhores da tecnologia, a quem ele chama de *cloudalistas*, extraem rendas.

<sup>26</sup> Nos dias de hoje, já se fala de um novo mercado no qual é possível transferir dados pessoais em troca de benefícios de produtos personalizados. Desta forma, o usuário pode considerar a possibilidade de ceder os seus dados em troca da utilização daqueles (ainda mais quando a maioria cede os seus dados sem receber qualquer tipo de compensação por isso).

<sup>27</sup> Entendidas como grandes plataformas digitais que fornecem um conjunto predefinido de serviços digitais, como motores de pesquisa *on-line* e lojas de aplicações e serviços de mensagens. Essas empresas têm: (i) posição econômica forte, com impacto significativo no mercado interno, operando em vários países da UE; (ii) forte posição de intermediação, o que significa que ligam grande base de utilizadores a grande número de empresas; (iii) posição consolidada e duradoura no mercado. A Comissão Europeia, em 6.9.2023, designou como *gatekeepers*: Alphabet, Amazon, Apple, ByteDance e Meta, Microsoft.

<sup>28</sup> Ver notícia no *site*: [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en). Acesso em: 29 abr. 2024.

<sup>29</sup> Ver a matéria publicada no *site*: <https://wtm.inf.br/artigos/170-milhoes-de-cameras-monitoram-possiveis-terroristas-na-china/>. Acesso em: 30 abr. 2024.

<sup>30</sup> KUKSO, Federico. Una historia de control. In: STANCANELLI, Pablo. *El Atlas de la revolución digital – Del sueño libertario al capitalismo de vigilancia*. Buenos Aires: Capital Intelectual, 2019. p. 12. Lembra o

Lembremos ainda da ferramenta de espionagem digital chamada *Pegasus*, criada pela empresa israelense NSO Group, usada para grampear *smartphones*, computadores e redes de comunicação e gestão de dados de forma global, tudo isto em nome da promoção da segurança da democracia e dos povos democráticos.<sup>31</sup>

E mais, estes recursos tecnológicos utilizados pelo setor público (Estado) e privado (mercado), por se valerem, em regra, de *software* com códigos fechados, impossibilitam níveis de transparência e visibilidade dos elementos constitutivos neurais de suas operações, inviabilizando controles sociais, políticos e jurídicos mais eficazes.<sup>32</sup>

Por conta destes cenários, tem se tornado cada vez mais comum falarmos na emergência de uma sociedade da vigilância e de uma democracia vigiada, chegando ao ponto de alguns jornalistas afirmarem que privacidade e intimidade configuram já direitos e garantias em certa medida ultrapassados, nomeadamente em tempos de níveis de insegurança global crescente.<sup>33</sup> Daí porque haver muita preocupação disseminada no tecido social em face das dinâmicas de quotidiana expansão incontrolável da vigilância comunitária, que conta com arquitetura e logística sem precedentes na história da civilização, basta atentarmos para o contingente de câmeras de monitoramento em espaços públicos e privados os mais diversos (lojas, bancos, praças públicas, ruas etc.).<sup>34</sup>

---

autor que estes sistemas também podem ser usados para rastrear objetivos políticos escusos envolvendo ofensivas contra dissidentes ou opositores e críticos e governos de ocasião.

<sup>31</sup> Ver a excelente matéria publicada no *site* das empresas Globo: <https://g1.globo.com/economia/tecnologia/noticia/2021/07/19/entenda-o-que-e-o-pegasus-software-de-espionagem-que-teria-sido-usado-para-invadir-smartphones-de-milhares-de-pessoas.ghtml>. Acesso em: 25 abr. 2023, dando conta de que, uma vez instalado, o Pegasus permite que os invasores tenham acesso a qualquer tipo de dado disponível no aparelho invadido, inclusive o uso do microfone e câmera, razão pela qual é vendido a várias agências governamentais para coletar dados de agentes suspeitos de crimes e terrorismo.

<sup>32</sup> O FBI, nos EUA, desde há muito utiliza *softwares* de configuração fechada os mais diversos para espionar pessoas físicas e jurídicas em nome da segurança pública nacional, e isto bem antes dos atentados às Torres Gêmeas de 2001, basta lembrarmos os programas Omnivore (1991) e Carnivore (1997), que monitoravam correios eletrônicos e comunicações eletrônicas – mais tarde substituídos por *softwares* disponíveis no mercado. Neste sentido ver a matéria de BAMFORD, James. The shadow factory: the ultra-secrets NSA from 9/11 to the eavesdropping on America. *Democracy Now*, 14 out. 2008. Disponível em: [https://www.democracynow.org/2008/10/14/james\\_bamford\\_the\\_shadow\\_factory\\_the](https://www.democracynow.org/2008/10/14/james_bamford_the_shadow_factory_the). Acesso em: 29 abr. 2024.

<sup>33</sup> Como quer Scott McNealy, CEO da Sun Microsystems, no texto *Private Lives? Not ours!* Disponível em: [https://www.pcworld.com/article/163331/private\\_lives\\_not\\_ours.html](https://www.pcworld.com/article/163331/private_lives_not_ours.html). Acesso em: 23 maio 2022. Há também ótima crítica a estes tempos de VATTIMO, Gianni. *La società trasparente*. Roma: Garzanti, 2000. Abordamos estes temas no livro LEAL, Rogerio Gesta e LEAL, Rogerio Gesta; SILVA, Ricardo Machado da. *O direito fundamental social à segurança pública no Estado democrático de direito – Parâmetros para políticas públicas de implementação*. Cruz Alta: Ilustração, 2023.

<sup>34</sup> Veja-se como alguns jornais divulgam estes temas, sublinhando somente aspectos positivos: “Com essas soluções é possível que sejam criados eventos de alerta e realizadas análises forenses no vídeo, reduzindo o tempo necessário para a realização de uma investigação, permitindo a notificação automática ou a realização de buscas com filtros para identificação de indivíduos e veículos, como filtros de cor de vestuário, acessórios como bolsas e mochilas, tamanho do objeto, sentido do deslocamento, placa de veículo, marca, modelo entre outras informações. Entre as principais tecnologias utilizadas no monitoramento urbano podemos citar o reconhecimento facial (FR), as tecnologias de leitura de placas de veículos (LPR)

### 3 Reações à sociedade da vigilância: perspectivas

A despeito de todos estes cenários, a sociedade tem reagido a movimentos panópticos como os anteriormente referidos e bem demarcados por Ryan McKinley, investigador do *MIT Media Lab*,<sup>35</sup> ao desenvolver um sistema denominado *Government Information Awareness (GIA)*,<sup>36</sup> que se apresenta como resposta dos cidadãos às iniciativas de controles digitais de governos.

A iniciativa do GIA baseia-se num raciocínio simples: se o governo tem o direito de saber detalhes pessoais dos cidadãos, os cidadãos também têm o direito de saber informações críticas sobre os seus governos. O projeto GIA desenvolveu tecnologias amigáveis que permitem as pessoas criar as suas próprias agências de inteligência para obter, classificar e agir com base nas informações que obtêm sobre os seus governos, bem como documentar assuntos de interesse público, como informações relacionadas com o financiamento de campanhas eleitorais, os currículos dos funcionários públicos, documentando a existência de reclamações, as relações secretas ou confidenciais de grandes corporações, informações que têm sido mantidas classificadas, e até um sistema de construção de perfis baseado no estudo de padrões.

Nesta mesma linha, temos a criação dos chamados *weblogs*.<sup>37</sup> Inicialmente os *weblogs* foram concebidos como sistemas estruturados na internet que permitiam a qualquer pessoa publicar informações pessoais, de forma semelhante a um diário, com capacidade de cadastro de endereços eletrônicos, inclusão de imagens e interação assíncrona. Porém, rapidamente evoluíram para verdadeiros jornais digitais, nos quais é possível encontrar diferentes pontos de vista sobre determinado acontecimento. Estas ferramentas competem hoje – no espaço virtual – com as mídias informativas convencionais.<sup>38</sup>

Como a mudança tecnológica é ecológica e não aditiva, tudo é redefinido, incluindo antigas práticas criminosas, que descobrem inéditas oportunidades com

---

e as soluções de detecção e classificação de áudio” (*Jornal Diário do Comércio*, 5 out. 2022. Disponível em: <https://diariodocomercio.com.br/opiniao/videomonitoramento-para-cidades-seguras/>. Acesso em: 2 maio 2024).

<sup>35</sup> Disponível em: <https://www.media.mit.edu>. Acesso em: 27 abr. 2024.

<sup>36</sup> Ver o *site*: <https://www.media.mit.edu/projects/open-government-information-awareness/overview/>. Acesso em: 27 abr. 2024. Ver também o interessante *site*: <https://www.wired.com/2003/07/slideshow-government-prying-the-good-kind/>. Acesso em: 27 abr. 2024.

<sup>37</sup> Em 1996, Dave Winer implementou um *weblog*, criando o espaço virtual *24 Horas pela Democracia*, uma reunião *on-line* realizada para apoiar a liberdade de expressão na internet. Algumas *tecnocelidades* participaram do evento inovador, como Bill Gates, fundador e proprietário da Microsoft, e Phillippe Kahn, da Novell. Mais tarde, o próprio Winer fundou uma empresa especialmente dedicada à criação e desenvolvimento de programa que facilitasse a criação de *weblogs*. O resultado desse projeto foi o *blog* pessoal de Winer, uma das principais referências mundiais da tendência (SAUER, Moritz. *Weblogs, podcasting & online-journalism*. Cambridge: O'Reilly Verlag GmbH & Co., 2017). p. 34 e seguintes.

<sup>38</sup> SAUER, Moritz. *Weblogs, podcasting & online-journalism*. Cambridge: O'Reilly Verlag GmbH & Co., 2017. p. 29.

a introdução de novas tecnologias de informação e comunicação a partir da IA.<sup>39</sup> Um exemplo disto é o cibercrime, atividade que representa ameaça real ao desenvolvimento da economia (física e digital) e da sociedade da informação, razão pela qual foi instituída a Convenção sobre o Crime Cibernético, em Budapeste, em 23.11.2001, firmada por inúmeros países do Conselho da Europa.<sup>40</sup>

O problema é que este documento implicou diminuição significativa de algumas garantias em termos de direitos fundamentais, entre as quais a sugestão de que fornecedores de acesso e serviços de internet mantenham registos das atividades realizadas pelos seus clientes no ciberespaço (arts. 17, 18, 24, 25), violando a privacidade e outros direitos dos usuários da internet, além de ser contrárias aos princípios estabelecidos na Declaração Universal dos Direitos Humanos.<sup>41</sup>

As estruturas institucionais dos Estados têm aumentado também para o enfrentamento destes problemas, como podemos ver no Chile, com a criação da *Brigada Investigadora del Cibercrimen* – BRICIB,<sup>42</sup> vinculada à polícia de investigações; no México, com a *Polícia Cibernética*,<sup>43</sup> vinculada à Polícia Federal Preventiva; na Espanha, com a *Brigada Central de Investigación Tecnológica*,<sup>44</sup> vinculada à Direção Geral da Polícia espanhola; em Portugal, com a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica, vinculada à Polícia Judiciária; no Brasil, com a Unidade Especial de Investigação de Crimes Cibernéticos, vinculada à Polícia Federal.<sup>45</sup> Todos estes órgãos desenvolvem políticas de vigilância da internet, com

<sup>39</sup> Sobre a regulamentação da inteligência artificial na União Europeia: MIRANZO DÍAZ, Javier. El Reglamento de Inteligencia Artificial de la Unión Europea: regulación de riesgos y sistemas de estandarización. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 24, n. 96, p. 43-78, abr./jun. 2024. DOI: 10.21056/aec.v24i96.1932.

<sup>40</sup> O Brasil editou o Decreto nº 11.941, de 12.4.2023, promulgando a Convenção sobre o Crime Cibernético no território nacional, ratificada pelo país em 1º.3.2023.

<sup>41</sup> De lembrar que a Convenção nº 108, vinculativa para os Estados-Membros do Conselho Europeu, em seu art. 6º, proíbe o tratamento automático de dados reveladores de origem racial, opiniões políticas, crenças religiosas, saúde ou vida sexual, a menos que a legislação nacional estabeleça salvaguardas adequadas. No entanto, em seu art. 9º, permite exceções para proteger a segurança do Estado, segurança pública, interesses financeiros do Estado, repressão de infrações penais ou para proteger os direitos e liberdades de terceiros. A ver como ficarão estas questões no novo documento a Convenção 108+, adotada em 2023, com previsão de entrada em vigor em junho de 2023.

<sup>42</sup> Maiores informações no *site*: <https://www.pdichile.cl/institucion/unidades/cibercrimen>. Acesso em: 29 abr. 2024.

<sup>43</sup> Maiores informações no *site*: <https://www.ssc.cdmx.gob.mx/organizacion-policial/subsecretaria-de-inteligencia-e-investigacion-policial/policia-cibernetica>. Acesso em: 29 abr. 2024.

<sup>44</sup> Maiores informações no *site*: [https://www.policia.es/\\_es/tupolicia\\_conocenos\\_estructura\\_dao\\_cgpoliciajudicial\\_bcit.php#](https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php#). Acesso em: 29 abr. 2024.

<sup>45</sup> Esta Unidade foi criada recentemente, em 28.6.2022, conforme notícia no *site* da Polícia Federal brasileira: <https://www.gov.br/mj/pt-br/assuntos/noticias/policia-federal-cria-unidade-especial-para-intensificar-a-repressao-a-crimes-ciberneticos>. Acesso em: 30 abr. 2024. Também os estados brasileiros começam a criar unidades especializadas para tal fim, como mostra a notícia veiculada em 18.12.2020, do Estado de São Paulo: <https://www.saopaulo.sp.gov.br/spnoticias/governo-do-estado-inaugura-divisao-de-crimes-ciberneticos-2/>. Acesso em: 30 abr. 2024. No Rio Grande do Sul, em 3.7.2010, já fora criada Delegacia de Repressão aos Crimes Informáticos – DRCl, conforme anuncia o *site* oficial do governo: <https://ssp.rs.gov.br/policia-civil-gaucha-cria-delegacia-pioneira-em-crimes-virtuais>. Acesso em: 30 abr. 2024.

foco nas ações de *hackers*, *sites* da internet, comunidades e salas de *chat* em que a pornografia infantil é promovida (analisando as atividades de organizações pedófilas locais e internacionais, redes de prostituição infantil e redes de tráfico de crianças que as exploram em outros países), crimes contra a propriedade intelectual, fraudes eletrônicas, lavagem de dinheiro, tráfico de armas, pessoas e drogas.

No Brasil temos avançado nestes temas, nomeadamente a partir da edição de algumas legislações focadas no uso de novas tecnologias, a saber:

- (i) Lei nº 12.258/2010, que modificou a Lei de Execuções Penais no sentido de promover a possibilidade de *utilização de equipamentos de vigilância pelos condenados pela justiça – monitoração eletrônica – para as hipóteses de saída temporária no regime semiaberto e cumprimento de pena em regime domiciliar*;
- (ii) Lei nº 12.403/2011, que modificou o Código de Processo Penal e instituiu o monitoramento eletrônico como *medida cautelar*, nos termos do art. 319, inc. IX, desta norma;<sup>46</sup>
- (iii) Lei nº 12.681/2012, instituindo o Sistema Nacional de Informações de Segurança Pública, Prisionais, de *Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Drogas* (SINESP), o qual utiliza plataforma de informações integradas das bases de dados do Governo Federal e dos estados, com o escopo de criar estrutura de gestão de informações em nível nacional, produzindo, coletando, sistematizando e disponibilizando informações para a segurança pública;
- (iv) Lei nº 12.737/2012, criando a tipificação criminal de delitos informáticos, com penas baixas de detenção de três meses até dois anos;
- (v) Lei nº 12.965/2014, que cria o Marco Civil da Internet no Brasil;
- (vi) Lei nº 13.675/2018, regulamentada pelo Decreto nº 9.489/2018, criando o Sistema Único de Segurança Pública (SUSP), instituindo políticas de governança, por meio da *padronização de dados, integração tecnológica, de inteligência e operacional* entre os agentes de segurança do país;
- (vii) Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais;<sup>47</sup>

<sup>46</sup> Nesta ferramenta, o usuário é rastreado via satélite através de um aparelho eletrônico (bracelete, pulseira ou tornozeleira) que funciona por meio de radiofrequência e informações criptografadas dos dados sobre a posição em que ele se encontra. Os dados colhidos pelo sistema são enviados a um servidor e podem ser acessados por terminal conectado à internet. Os argumentos a favor desta opção ponderam que ela operaria redução significativa da população carcerária, bem como diminuição de gastos públicos com presos e reinserção social; enquanto que os argumentos contrários se centram: (i) na possibilidade de retorno a um Estado totalitário, em que a sociedade seria a própria prisão, (ii) na estigmatização social da pessoa em razão da utilização do equipamento de monitoramento em público, (iii) na violação ao direito a intimidade e privacidade. Neste sentido ver o texto de GRECO, Rogério. *Direitos humanos, sistema prisional e alternativas à privação de liberdade*. São Paulo: Saraiva, 2011. p. 118.

<sup>47</sup> FÁCIO, Rafaella Nátaly. A transparência e o direito de acesso no tratamento de dados pessoais: considerações sobre intersecções entre Lei Geral de Proteção de Dados e Lei de Acesso à Informação no Brasil. *Revista*

(viii) em 2018, o Conselho Nacional de Justiça (CNJ) criou o Banco Nacional de Monitoramento de Prisões (BNMP), base de dados e sistema eletrônico em que constam os *dados cadastrais das pessoas presas no sistema carcerário do Brasil*, com o objetivo de centralização das informações e contribuição para o acesso às informações pelas autoridades judiciárias e policiais, auxiliando as autoridades judiciárias da justiça criminal na gestão de documentos atinentes às ordens de prisão/internação e soltura expedidas em todo o território nacional, materializando um Cadastro Nacional de Presos.

O Plano Nacional de Segurança Pública de 2018 introduziu, como estratégia nº 8, o *videomonitoramento com reconhecimento facial biométrico*, destacando-se as habilidades que *softwares* de computadores possuem de analisar rostos humanos constantes de uma base de dados específica, utilizando conexões de internet para catalogar indivíduos, via captação de sua biometria extraída por *smartphones*, computadores e câmeras de vigilância.<sup>48</sup> Esta política pública, no Brasil, estava voltada precipuamente para a fiscalização de fronteiras, divisas interestaduais, portos, aeroportos, rodoviárias e ferrovias.<sup>49</sup> Mas agora também espaços públicos urbanos estão sendo tomados por estes mecanismos, como ocorre na experiência da plataforma de videomonitoramento *Smart Sampa*, em São Paulo, que tem previsão de integrar mais de 20 mil câmeras até 2024 na capital.<sup>50</sup> As polêmicas acerca do projeto são muitas: questionamentos judiciais,<sup>51</sup> edital suspenso, muita resistência da sociedade e histórico de corrupção pela empresa responsável.<sup>52</sup>

---

*Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 10, n. 2, e247, jul./dic. 2023. DOI 10.14409/redoeda.v10i2.13413.

<sup>48</sup> Na Europa, o Conselho Europeu de Proteção de Dados, encarregado de aplicar o Regulamento Geral de Proteção de Dados, emitiu a Diretriz 05/2022, sobre o uso desta ferramenta, entendendo que ela representa interferência desproporcional nos direitos dos titulares dos dados, vez que compromete a expectativa das pessoas de permanecerem anônimas, contrariando os princípios de autodeterminação e participação livre em sociedades democráticas. Ver o documento integral no *site*: [https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area\\_en](https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en). Acesso em: 29 abr. 2024.

<sup>49</sup> Inúmeros países se valeram destas tecnologias para fins de: (i) monitorar o cumprimento do *lockdown* adotado ao longo da pandemia de Covid-19 (China); (ii) monitoramento comportamental de pessoas na Olimpíada de 2020, no Japão, também decorrente da pandemia; (iii) monitoramento de grandes eventos (Reino Unido) para identificar pessoas procuradas pela polícia. Nos EUA temos notícias de proposta de lei federal (2023) que quer regulamentar a matéria (*Facial Recognition Act*), restringindo o emprego do reconhecimento facial biométrico (Disponível em: <https://www.congress.gov/bill/117th-congress/house-bill/9061/text?s=1&r=7>. Acesso em: 29 abr. 2024).

<sup>50</sup> Dentre os movimentos que deram força no combate à plataforma, está a campanha *Tire meu rosto da sua mira*, feita por mais de 50 entidades da sociedade civil e que tem como objetivo solicitar o banimento do uso das câmeras para segurança pública (Disponível em: <https://tiremeurostodasuamira.org.br>. Acesso em: 22 abr. 2024).

<sup>51</sup> Notícia veiculada pelo sítio jurídico do *Conjur*, em 17.5.2024, dá conta de que quatro estados brasileiros já prenderam mais de 1,7 mil pessoas utilizando o reconhecimento facial sem regulamentação adequada para tanto. Ver matéria completa no *site*: <https://www.conjur.com.br/2024-mai-17/sem-regulacao-estados-prendem-centenas-utilizando-reconhecimento-facial/>. Acesso em: 18 mai. 2024.

<sup>52</sup> Informa o *site* do projeto que: "A nova plataforma ainda facilita a integração de diversos serviços municipais, como CET, SAMU, Defesa Civil e GCM, em uma única plataforma por meio da criação de uma moderna

- (i) Decreto nº 10.882/2021, criando o Plano Nacional de Segurança Pública – 2021/2030, e visando, dentre outras metas, promover a *expansão tecnológica* na promoção de políticas de segurança pública, utilizando-se, para tanto, de padronização, integração e interoperabilidade dos dados sobre segurança pública entre União, estados, Distrito Federal e municípios (estratégia nº 7);<sup>53</sup>
- (ii) também em 2021 foi instituída a política de *adoção de câmeras corporais nos uniformes dos policiais (body-worn)*, instaladas na farda, capacete ou óculos dos policiais, com capacidade de captar e gravar, vídeo e áudio das atividades desenvolvidas pelos agentes em sua rotina policial, a exemplo de gravações de trânsito, detenções, revistas, interrogatórios.<sup>54</sup>

O problema é que, modo geral, estas políticas de segurança pública virtuais estão estruturadas a partir de ferramentas tecnológicas de *software* fechado, o que tem aumentado em nível global as pressões sociais e políticas à regulamentação das *big tech*, assim como se amplia o uso de sistemas de fonte aberta, já tendo algumas que fazem parte da *Software Choice Initiative*, avançado neste sentido, dentre as quais: Intel (EUA), Linux (EUA), Open Solutions (Argentina), Paradigma (Brasil), Associação Peruana de Software (Peru), Siam Commercial Bank (Tailândia), VSI (Alemanha).<sup>55</sup> E estes modelos abertos ao menos dariam maiores garantias

---

Central de Monitoramento Integrada. Além disso, com as novas câmeras, os órgãos de segurança terão como monitorar escolas, UBS e demais equipamentos públicos, aumentando significativamente a segurança nesses locais. As câmeras técnicas contarão ainda com monitoramento de calor, facilitando a supervisão em praças e parques, que normalmente possuem árvores e áreas verdes que podem prejudicar uma vigilância mais precisa” (Disponível em: <https://participemais.prefeitura.sp.gov.br/legislation/processes/209>. Acesso em: 22 abr. 2024).

<sup>53</sup> Disponível em: [https://www.gov.br/mj/pt-br/centrais-de-conteudo/publicacoes/categorias-de-publicacoes/planos/plano\\_nac\\_de\\_seguranca\\_publica\\_e\\_def\\_soc\\_2021\\_\\_2030.pdf](https://www.gov.br/mj/pt-br/centrais-de-conteudo/publicacoes/categorias-de-publicacoes/planos/plano_nac_de_seguranca_publica_e_def_soc_2021__2030.pdf). Acesso em: 29 abr. 2024.

<sup>54</sup> O Estado de São Paulo foi pioneiro na adoção da prática, sendo replicada em outros estados como o Rio de Janeiro, Minas Gerais, Pará, Santa Catarina e Rio Grande do Sul. Ver a matéria do Núcleo de Estudos da Violência, da Universidade de São Paulo, no *site*: <https://nev.prp.usp.br/projetos/pesquisa-uso-cameras-corporais-pela-policia-militar-de-sp/>. Acesso em: 29 abr. 2024. O *site* dá conta de que, no Estado de São Paulo: “Estudo realizado pelo Fórum Brasileiro de Segurança Pública indicou uma queda geral de 62,7% na letalidade policial, entre 2019 e 2022, com especial ênfase nas unidades já equipadas com as COPS. Análise realizada pelo CCAS/FGV, com colaboração da PMESP, indica que as câmeras foram responsáveis diretamente por 57% de redução no número de mortes decorrentes de intervenção policial e queda 63% nas lesões corporais causadas por policiais militares. Estudo recente do Instituto Sou da Paz revela que os casos de mortes de jovens (entre 15 e 24 anos) caíram 46% após a implementação das câmeras”.

<sup>55</sup> Ver o *site*: <https://web.archive.org/web/20061107202717/http://www.softwarechoice.org/>. Acesso em: 29 abr. 2024. No Reino Unido, em 15.7.2002, o *Commerce Office* lançou o projeto de *software* de código aberto. Esta iniciativa afirma que um *software* de código aberto bem configurado pode ser tão seguro quanto sistemas proprietários e está atualmente sujeito a menos ataques pela internet. Por esta razão devem se estabelecer equilíbrios entre a disponibilidade de competências de administração e segurança e as vantagens que diferentes sistemas podem proporcionar. Ver as informações no *site*: [https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://assets.publishing.service.gov.uk/media/5a79cceed915d042206b200/All\\_About\\_Open\\_Source\\_v2\\_0.doc&ved=2ahUKEwY6LC4vueFAxVqrpUCHVqmDL8QFnoECCDAQ&usq=A0vVaw1q\\_eK5Ym0tvDSO4c8dUjw2](https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://assets.publishing.service.gov.uk/media/5a79cceed915d042206b200/All_About_Open_Source_v2_0.doc&ved=2ahUKEwY6LC4vueFAxVqrpUCHVqmDL8QFnoECCDAQ&usq=A0vVaw1q_eK5Ym0tvDSO4c8dUjw2). Acesso em: 29 abr. 2024.

técnicas de monitoramento e visibilidade dos processos de acesso e gestão de dados, tanto às pessoas como ao Estado.<sup>56</sup>

Em nível de judicialização destas discussões, vale lembrar as decisões do Supremo Tribunal Federal – STF, na Ação Declaratória de Inconstitucionalidade nº 6.649, e na Ação de Descumprimento de Preceito Fundamental nº 695, entendendo que o compartilhamento de dados pessoais entre órgãos públicos – mesmo para fins de segurança pública – pressupõe propósitos legítimos e específicos,<sup>57</sup> e o procedimento deve cumprir todos os requisitos da Lei Geral de Proteção de Dados (Lei nº 13.709/2018).<sup>58</sup> Se forem desobedecidas as diretrizes da LGPD, o Estado responderá objetivamente pelos danos causados às pessoas. E o funcionário que dolosamente violar o dever de publicidade estabelecido no art. 23, I, da LGPD responderá por ato de improbidade administrativa.<sup>59</sup>

De igual sorte, no Tema nº 977,<sup>60</sup> o STF está enfrentando o tormentoso tema de se o acesso a registro telefônico, agenda de contatos e demais dados contidos em aparelhos celulares apreendidos no local do crime atribuído ao acusado depende de prévia decisão judicial que justifique, com base em elementos concretos, a necessidade e a adequação da medida, e delimite a sua abrangência à luz dos direitos fundamentais à intimidade, à privacidade<sup>61</sup> e ao sigilo das comunicações e dados dos indivíduos.

## 4 Notas conclusivas

Temos, pois, como conclusão destas reflexões, que algumas premissas se fazem importantes para viabilizar políticas de segurança pública democráticas com o uso de tecnologias virtuais, a saber:

<sup>56</sup> Acerca do direito fundamental à proteção de dados, ver: ARAÚJO, Valter Shuenquener de; PERIM, Maria Clara Mendonça; RIBEIRO, Koryander Figueirêdo. As assimetrias da regulação estatal para a proteção de dados pessoais e a afirmação dos direitos fundamentais de primeira dimensão. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 22, n. 87, p. 267-296, jan./mar. 2022. DOI: 10.21056/aec.v22i87.1453; SÁNCHEZ DÍAZ, María Fernanda. El derecho a la protección de datos personales en la era digital. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 10, n. 1, e235, ene./jun. 2023. DOI: 10.14409/redoeda.v10i1.12626.

<sup>57</sup> Sobre a jurisprudência do Supremo Tribunal Federal em matéria de comunicação de dados: ABREU, Jacqueline de Souza. Comunicação de dados, não dados em si: origens e problemas do atual paradigma de proteção constitucional do sigilo de dados. *Revista de Investigações Constitucionais*, Curitiba, v. 11, n. 1, e256, jan./abr. 2024. DOI: 10.5380/rinc.v11i1.89280.

<sup>58</sup> MARTINS, Ricardo Marcondes. Proteção de dados, competências dos entes federativos e a Emenda Constitucional n. 115/22. *Revista de Investigações Constitucionais*, Curitiba, v. 9, n. 3, p. 645-658, set./dez. 2022. DOI: 10.5380/rinc.v9i3.87107.

<sup>59</sup> Conforme decisão publicada no site do STF: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238>. Acesso em: 30 abr. 2024.

<sup>60</sup> Conforme site do STF: [https://jurisprudencia.stf.jus.br/pages/search?classeNumerolIncidente=%22ARE%201042075%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=\\_score&sortBy=desc&isAdvanced=true](https://jurisprudencia.stf.jus.br/pages/search?classeNumerolIncidente=%22ARE%201042075%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true). Acesso em: 30 abr. 2024.

<sup>61</sup> ROBLES OSOLLO, Ana Gloria. El derecho a la privacidad y la protección de datos personales transfronterizos. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 8, n. 1, p. 35-60, ene. /jun. 2021. DOI 10.14409/redoeda.v8i1.9543.

- a) quadros legais e regulamentares: com a aplicação e harmonização dos quadros jurídicos e regulamentares atuais para promover um ambiente de certeza e confiança na adoção, utilização e promoção das tecnologias;
- b) interoperabilidade: em torno das capacidades estruturais, técnicas, organizacionais e de governança necessárias para compartilhar informações e gerar conhecimento, com transparência e prestação de contas públicas;
- c) dados abertos: disponibilização de informação governamental em formatos úteis e reutilizáveis por diferentes entidades governamentais, população, organizações da sociedade civil, cooperadores e universidades, entre outros, para promover o empreendedorismo e a governação a partir da ideia de segurança cidadã;
- d) conectividade e ferramentas digitais adequadas: fortalecimento e desenvolvimento das redes (governamentais e cidadãos), expansão de melhores infraestruturas nos territórios e da capacidade das redes existentes, e o desenvolvimento de (i) competências no setor das tecnologias para estimular aplicações principalmente em redes celulares massivas, e (ii) ferramentas virtuais que viabilizem aplicações para denúncias/demandas/respostas em múltiplas plataformas;<sup>62</sup>
- e) participação cidadã e competências digitais: desenvolvimento equitativo de competências para desenvolver e operar tecnologias e serviços digitais, contemplando a cobertura social e o desenvolvimento de competências em sistemas comunitários;
- f) comunicação digital e redes sociais: como instrumento de capacitação e consciência social para apoiar estratégias digitais, comunicação digital focada nos cidadãos e nas suas necessidades como demandantes de segurança e convivência, prestando serviços baseados na gestão do conhecimento, e não apenas na informação.

Nomeadamente no Brasil estes elementos não se fazem ainda exaustivamente presentes, o que nos vai demandar ainda muito tempo.

## Referências

ABREU, Jacqueline de Souza. Comunicação de dados, não dados em si: origens e problemas do atual paradigma de proteção constitucional do sigilo de dados. *Revista de Investigações Constitucionais*, Curitiba, v. 11, n. 1, e256, jan./abr. 2024. DOI: 10.5380/rinc.v11i1.89280.

<sup>62</sup> A Venezuela tem um aplicativo chamado *Patrulha Inteligente*, que detecta o quadrante de segurança correspondente à localização do usuário, fornecido pelo GPS do seu celular, ou por meio do seu provedor de rede, e fornece as informações para que possa entrar em contato com o número de telefone de emergência associado. Os cidadãos podem ligar para as autoridades policiais e militares mais próximas da sua área e fazer as suas queixas de forma anônima. Mais informações no site: <https://consejogeneraldepolicia.org/opinion/patrullaje-inteligente/>. Acesso em: 29 abr. 2024.

- ARAÚJO, Valter Shuenquener de; PERIM, Maria Clara Mendonça; RIBEIRO, Koryander Figueirêdo. As assimetrias da regulação estatal para a proteção de dados pessoais e a afirmação dos direitos fundamentais de primeira dimensão. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 22, n. 87, p. 267-296, jan./mar. 2022. DOI: 10.21056/aec.v22i87.1453.
- BAMFORD, James. The shadow factory: the ultra-secrets NSA from 9/11 to the eavesdropping on America. *Democracy Now*, 14 out. 2008. Disponível em: [https://www.democracynow.org/2008/10/14/james\\_bamford\\_the\\_shadow\\_factory\\_the](https://www.democracynow.org/2008/10/14/james_bamford_the_shadow_factory_the). Acesso em: 29 abr. 2024.
- BITENCOURT, Caroline Müller; MARTINS, Luisa Helena Nicknig. A inteligência artificial nos órgãos constitucionais de controle de contas da administração pública brasileira. *Revista de Investigações Constitucionais*, Curitiba, v. 10, n. 3, e253, set./dez. 2023. DOI: 10.5380/rinc.v10i3.93650.
- BLANCHET, Luiz Alberto; TRENTO, Melissa. A inteligência artificial como diretriz propulsora ao desenvolvimento e à eficiência administrativa. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 23, n. 93, p. 153-172, jul./set. 2023. DOI: 10.21056/aec.v23i93.1733.
- BOMTEMPO, Eugênio Moraes; CARMONA, Paulo Cavichioli. A solidariedade social na pandemia de Covid-19. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 22, n. 89, p. 251-276, jul./set. 2022. DOI: 10.21056/aec.v22i89.1662.
- CASTELS, Manuel. *La sociedad en red – La era de la información. Economía, sociedad y cultura*. Madrid: Alianza Editorial, 1997. v. 1.
- CASTILLO ARJONA, Mónica. El fenómeno de la Covid-19 y sus efectos sociales en el derecho administrativo del siglo XXI. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 8, n. 1, p. 173-187, ene./jun. 2021. DOI: 10.14409/redoeda.v8i1.9548.
- CERI, Paolo. *La società vulnerabile – Quale sicurezza, quale libertà*. Roma/Bari: Laterza, 2003.
- COLE, David. *Enemy Aliens – double standards and constitutional freedoms in the war on terrorism*. New York: The New Press, 2003.
- D'AGOSTINI, Franca; FERRERA, Maurizio. *Le verità del potere – Sei diritto aleatici*. Roma: Einaudi, 2019.
- DAVARRA RODRIGUEZ, Miguel Angel. *De las autopistas de la información a la sociedad virtual*. Madri: Aranzadi Editorial, 2008.
- DOMINICI, Piero. *La società dell'irresponsabilità*. Milano: Franco Angeli, 2015.
- FELICE, Emanuele. *Dubai – L'ultima utopia*. Roma: Il Mulino, 2020.
- FERRAJOLI, Luigi. *La democrazia attraverso i diritti*. Roma: Laterza, 2013.
- FOUCAULT, Michel. *Vigilar y castigar*. Nascimento de la prisión. México: Siglo XXI, 1983.
- GRECO, Rogério. *Direitos humanos, sistema prisional e alternativas à privação de liberdade*. São Paulo: Saraiva, 2011.
- HARARI, Yuval Noah. *Homo Deus*. Uma breve história do amanhã. São Paulo: Companhia das Letras, 2016.
- HERNANDES, Luiz Eduardo Camargo Outeiro; PIOVESAN, Flávia. Desafios judiciais em tempos de pandemia: fortalecendo o diálogo entre a Comissão Interamericana de Direitos Humanos e o Supremo Tribunal Brasileiro para a proteção dos direitos humanos. *Revista de Investigações Constitucionais*, Curitiba, v. 9, n. 2, p. 371-388, maio/ago. 2022. DOI: 10.5380/rinc.v9i2.86138.
- KUKSO, Federico. *Una historia de control*. Buenos Aires: Capital Intelectual, 2019.
- LEAL, Rogerio Gesta. *Segurança pública no Estado democrático de direito – Avanços e recuos*. São Paulo: Tirant lo Blanch, 2023.

LEAL, Rogerio Gesta; SILVA, Ricardo Machado da. *O direito fundamental social à segurança pública no Estado democrático de direito* – Parâmetros para políticas públicas de implementação. Cruz Alta: Ilustração, 2023.

MARTINS, Ricardo Marcondes. Proteção de dados, competências dos entes federativos e a Emenda Constitucional n. 115/22. *Revista de Investigações Constitucionais*, Curitiba, v. 9, n. 3, p. 645-658, set./dez. 2022. DOI: 10.5380/rinc.v9i3.87107.

MARTNEZ GARBIRAS, María Margarita; SÁNCHEZ-HUERTAS, Luis Fernando. Los atajos de la Cuarta Revolución Industrial a la democracia: una reflexión de lecciones aprendidas en clave de Lafont y Berlin. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 23, n. 94, p. 43-62, out./dez. 2023. DOI: 10.21056/aec.v23i94.1725.

MCNEALY, Scott. Private Lives? Not ours! *PC World*. Disponível em: [https://www.pcworld.com/article/16331/private\\_lives\\_not\\_ours.html](https://www.pcworld.com/article/16331/private_lives_not_ours.html). Acesso em: 23 maio 2022.

MIRANZO DÍAZ, Javier. El Reglamento de Inteligencia Artificial de la Unión Europea: regulación de riesgos y sistemas de estandarización. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 24, n. 96, p. 43-78, abr./jun. 2024. DOI: 10.21056/aec.v24i96.1932.

MONGARDINI, Carlo. *Le dimensioni sociali della paura*. Milano: Franco Angeli, 2010.

MOROZOV, Evgeny. *The net delusion: the dark side of internet freedom*. New York: Public Affairs, 2019.

NÓBREGA, Marcos; HEINEN, Juliano. As forças que mudarão a Administração Pública pós-Covid: transparência 2.0, blockchain e smart contracts. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 21, n. 85, p. 217-230, jul./set. 2021. DOI: 10.21056/aec.v21i85.1405.

PHILIPPI, Juliana Horn Machado. Transformação digital e urgência da cultura de dados na Administração Pública brasileira. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 10, n. 1, e232, ene./jun. 2023. DOI: 10.14409/redoeda.v10i1.12401.

PUSCHEL, André Felipe Silva; RODRIGUES, Roberto Tassis; VALLE, Vivian Cristina Lima López. O dilema ético da decisão algorítmica na administração pública. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 22, n. 90, p. 207-226, out./dez. 2022. DOI: 10.21056/aec.v22i90.1737.

RODRÍGUEZ-ARANA MUÑOZ, Jaime. Administrative Law and human dignity (on the post-pandemic reconstruction of Administrative Law). *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 22, n. 88, p. 11-33, abr./jun. 2022. DOI: 10.21056/aec.v22i88.1646.

SÁNCHEZ DÍAZ, María Fernanda. El derecho a la protección de datos personales en la era digital. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 10, n. 1, e235, ene./jun. 2023. DOI: 10.14409/redoeda.v10i1.12626.

SÁNCHEZ DÍAZ, María Fernanda. El impacto de la inteligencia artificial generativa en los derechos humanos. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 11, n. 1, e252, ene./jun. 2024. DOI: 10.14409/redoeda.v11i1.13612.

SÁNCHEZ DIAZ, Maria Fernanda; ROMERO TELLO, Ana Guadalupe. Covid-19, Derechos Humanos y Estado frente al manejo de la Pandemia. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 8, n. 1, p. 233-254, ene. /jun. 2021. DOI 10.14409/redoeda.v8i1.9525.

SAUER, Moritz. *Weblogs, Podcasting & Online-journalism*. Cambridge: O'Reilly Verlag GmbH & Co., 2017.

SIERRA CADENA, Grenfieth de Jesus. Implementación de la Inteligencia Artificial en las Altas Cortes de Colombia: los casos de la Corte Constitucional y el Consejo de Estado. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 11, n. 1, e253, ene./jul. 2024. DOI 10.14409/redoeda.v11i1.13824.

TOFFLER, Alvim. *La tercera ola*. México: Edivisión, 1981.

TOLEDO, Claudia; PESSOA, Daniel. O uso de inteligência artificial na tomada de decisão judicial. *Revista de Investigações Constitucionais*, Curitiba, v. 10, n. 1, e237, jan./abr. 2023. DOI: 10.5380/rinc.v10i1.86319.

VALLE, Vivian Cristina Lima López; RUIZ, Maria Guadalupe Fernandes; BÜTTNER, Marcielly. Fake news, influência na formação da opinião pública e impactos sobre a legitimidade da decisão pública. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 24, n. 95, p. 73-97, jan./mar. 2024. DOI: 10.21056/aec.v24i95.1898.

VALLE, Vivian Lima López; FUENTES I GASÓ, Josep Ramón; AJUS, Atílio Martins. Decisão judicial assistida por inteligência artificial e o Sistema Victor do Supremo Tribunal Federal. *Revista de Investigações Constitucionais*, Curitiba, v. 10, n. 2, e252, maio/ago. 2023. DOI: 10.5380/rinc.v10i2.92598.

VAROUFAKIS, Yanis. *Technofeudalism*. London: Bodley Head, 2023.

VATTIMO, Gianni. *La società trasparente*. Roma: Garzanti, 2000.

VERHOEVEN, Charles Leben. *Le principe de précaution – Aspects de droit international et communautaire*. Paris: Éditions Panthéon-Assas, 2022.

WALZER, Michael. *La libertà e i suoi nemici nell'età della guerra al terrorismo*. Roma/Bari: Laterza, 2010.

ZOLO, Danilo. *Sula paura – Fragilità, aggressività, potere*. Milano: Feltrinelli Editore, 2011.

ZUBOFF, Shoshana. *The age of surveillance capitalism*. New York: Perseus Books, 2019.

---

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

LEAL, Rogério Gesta. Segurança pública e inteligência artificial – Novos paradigmas. *International Journal of Digital Law*, Belo Horizonte, ano 5, n. 2, p. 81-99, maio/ago. 2024. DOI: 10.47975/digital.law.vol.5.n.2.leal.

---

### Informações adicionais

#### Additional information

Editores responsáveis	
<b>Editor-Chefe</b>	Emerson Gabardo
<b>Editor-Adjunto</b>	Lucas Bossoni Saikali