A SOCIEDADE DO CONTROLE DIGITAL E A SEGURANÇA PÚBLICA BRASILEIRA

Érica Nascimento Pinheiro Vargas[1]
Mônica Matos Ribeiro[2]

RESUMO

A sociedade hodierna se destaca pelo avanço da tecnologia e mudanças na forma da inter-relação homem/máquina, principalmente, após a criação da inteligência artificial e sua aplicação em diversos setores da sociedade, com destaque, para a sua utilização na política de segurança pública no Brasil. Nesse sentido, o objetivo deste artigo foi analisar a inserção das tecnologias de informação e comunicação (TICs) para o controle digital por parte das políticas de segurança pública implementadas no Brasil nos anos recentes, contribuindo para o debate acerca de como o controle digital tem avançado na elaboração de tais políticas, e da necessária reflexão acerca dos cuidados que emergem da sua implementação. Essa análise ganha relevância em um contexto no qual as políticas de segurança pública no Brasil tem ampliado o uso das TICs como solução para diminuição dos índices de criminalidade e violência. Foi utilizado o método qualitativo para o alcance do objetivo proposto, valendo-se da revisão bibliográfica e documental. Como resultado destaca-se a ampliação sistemática do uso das TICs como solução para diminuição dos índices de criminalidade e violência no Brasil. Entretanto, deve-se atentar que a construção de perfis das pessoas, através da exploração do corpo humano em sua forma de extração de dados biométricos e análise comportamental ou de emoções para personalizar seus produtos e serviços, pode implicar, se essa prática for realizada de forma reiterada e indiscriminada, e não havendo controle efetivo da sua utilização, em uma sociedade da vigilância, marcada pelo panoptismo digital.

Palavras-chave: Controle Digital. Política Pública. Segurança Pública. Penoptismo Digital.

ABSTRACT

Modern society stands out for the advancement of technology and changes in the form of man/machine interrelationship, mainly after the creation of artificial intelligence and its application in various sectors of society, with emphasis on its use in public security policy in Brazil. In this sense, the objective of this article was to analyze the insertion of information and communication technologies (ICTs) for digital control by the public security policies implemented in Brazil in recent years, contributing to the debate about how digital control has advanced in the elaboration of such policies, and the necessary reflection about the care that emerges from its implementation. This analysis gains relevance in a context in which public security policies in Brazil have expanded the use of ICTs as a solution to reduce crime and violence rates. The qualitative method was used to reach the proposed objective, making use of

[1] Advogada e Professora de Direito Digital. Mestre em Direito, Governança e Políticas Públicas – Universidade Salvador (Unifacs). Especialista em Direito, Governança e Políticas Públicas pela Universidade Salvador (Unifacs). Especialista em Direito Empresarial pela Universidade Salvador (Unifacs). Especialista em Direito Processual Civil pela Universidade Federal da Bahia (UFBA). Especializanda em Direito Digital pela Escola Brasileira de Direito. Membro da Comissão de Arbitragem da Ordem dos Advogados do Brasil – Seção Bahia 2019/2020. E-mail: ericapinheiroadv@hotmail.com

[2] Doutora em Administração pela Universidade Federal da Bahia (UFBA) é professora da Universidade do Estado da Bahia (UNEB) e do Mestrado Profissional em Direito, Governança e Políticas Públicas da Universidade Salvador (UNIFACS). E-mail: monica.matos@animaeducacao.com.br

the bibliographical and documental review. As a result, the systematic expansion of the use of ICTs as a solution to reduce crime and violence rates in Brazil stands out. However, it should be noted that the construction of people's profiles, through the exploration of the human body in its form of extraction of biometric data and behavioral or emotional analysis to customize its products and services, may imply, if this practice is carried out in a repeatedly and indiscriminately, and with no effective control over its use, in a surveillance society marked by digital panopticism.

Keywords: Digital Control. Public policy. Public security. Digital Penoptism.

1. INTRODUÇÃO

A sociedade hodierna se destaca pelo avanço da tecnologia e mudanças na forma da inter-relação homem/máquina, principalmente, após a criação da inteligência artificial (IA) e sua aplicação em diversos setores da sociedade, com destaque, para a sua utilização nas políticas de segurança pública. As revoluções industriais que resultaram na sociedade atual demonstraram a importância do desenvolvimento da tecnologia, especialmente, a partir da Terceira Revolução Industrial, com o desenvolvimento das Tecnologias de Informação e Comunicação (TICs) (CASTELLS, 1999).

As TICs moldaram a nova forma de relacionamento entre economia, Estado e Sociedade e contribuíram para a formação de uma sociedade globalizada (CASTELLS, 2004), mediante a modificação da lógica gerencial produtiva, antes constituída de tarefas repetitivas – fordismo – para uma cadeia produtiva com incentivo a ampliação de trabalhos intelectuais e das forças microeletrônicas de comunicação, inclusive pelo Estado, na condição de líder ou mediador desse movimento (LOPES, 2008).

A informação começa a ser alçada a um ativo valioso, impulsionada pela criação da IA em 1960, e da internet em 1969, e embalada pela forma de expansão do capitalismo, a partir da década de 1980, cujo destaque se deu com a expansão global da internet comercial, em 1987. Nesse esteio, todos esses acontecimentos contribuíram para a formação da chamada Sociedade da Informação (CASTELLS, 1999) e a criação da Sociedade em Rede (LEVY, 2011).

A partir de 2016 Schwab (2016) cunhou o termo Quarta Revolução Industrial, uma vez que considerou ser um novo paradigma social o avanço da criação de novas tecnologias, como uma fusão em seus domínios físicos, digitais e biológicos que impactam na inter-relação entre o homem e máquina e se aplicam a todos os setores sociais, inclusive para promoção de políticas públicas. São destaques a biotecnologia, IA, robôs, *Internet of Things* (IOT) e a extração e análise de dados – *Big Data*.

A fusão digital homem/máquina, em sua análise sob a ótica do *Big Data,* se perfaz na ideia de utilização dos dados pessoais como matéria-prima, para que, através de análises algoritmas, as empresas de tecnologia possam construir perfis personalizados dos gostos e preferências das pessoas para o oferecimento de seus produtos e/ou serviços, tornando-os mais atrativos e acessíveis (PINHEIRO; FERRAZ, 2021).

O corpo humano passa a ter relevância na criação dos perfis acima mencionados, visto que o perfilamento é realizado por algoritmos que fazem análises biométricas, das emoções e comportamentos. O perfilhamento algoritmo das pessoas, inclusive, é aplicado às relações de

trabalho e a cultura da digitalização dos serviços, a exemplo da escolha automatizada de candidatos a vagas de emprego, via IA, aplicações de saúde e telemedicina e aplicativos de prevenção de fraudes via reconhecimento facial.

O poder público também se utiliza da tecnologia de captação dos dados pessoais, via *Big Data*, para a promoção de políticas públicas, com o escopo de perfilar produtos e serviços oferecidos à população, objetivando conferir mais eficiência nos recursos públicos e amplitude da política. Nesse esteio se destacam a promoção de aplicações com bases de dados integradas e interoperáveis, como a plataforma Gov.br (BRASIL, 2022) para acesso a diversos serviços públicos no Brasil, desenvolvimento de aplicativos para identificação de pessoas que gozariam do direito a benefícios sociais, a exemplo do Auxílio Emergencial e Auxílio Brasil, e ainda, para ações no campo da segurança pública, destaque para o reconhecimento de pessoas foragidas da justiça ou com mandados de prisão em aberto.

Mister ressalvar, entretanto, que um outro efeito secundário e importante é que a captação massiva dos dados pessoais biométricos pode ensejar a realização de grandes bases de dados pessoais para fins que vão além do consumo e personalização de serviços públicos, mas para o exercício do controle e vigilância pelo Estado e pelas empresas que detêm o conhecimento da tecnologia (WERTHEIN, 2000). Com o desenvolvimento da tecnologia, a vigilância que antes era realizada em espaços fechados e físicos passa a ser realizada, também, de forma virtual, em um clique, um *cookie*, câmera de videomonitoramento em locais públicos, muitas vezes, sendo realizada de forma indiscriminada (OLIVEIRA, 2021).

Essa vigilância ostensiva digital é denominada de panóptico digital (HAN, 2018), conceito de vigilância baseado no panóptico de Benthan e que causa preocupações quando há controle excessivo e manipulação de massas quando da implementação de políticas públicas, sobretudo, as de segurança.

A promoção de políticas públicas de segurança envolvendo as TICs se difundiu no Brasil a partir dos anos 2000, mediante estímulo à inovação tecnológica previsto no Plano Nacional de Segurança Pública (PNS) e a necessidade do Estado brasileiro de desenvolver novas ações preventivas e de combate à criminalidade (BRASIL, 2000). Para Alcadipani (2020), a utilização da tecnologia nas ações pelo Estado decorre da tentativa de desenvolver mais ações de inteligência, com menos letalidade e da necessidade do Estado controlar o exponencial crescimento da violência no país.

Nessa perspectiva, como forma de combate à criminalidade, foram adotadas diversas políticas públicas envolvendo a tecnologia ao longo dos anos no Brasil, com destaque para a área de segurança, do estímulo à utilização da IA, instituído pela Política Nacional de Segurança Pública, no ano de 2018, que trouxe, especificamente, a possibilidade de utilização do reconhecimento facial automatizado para fins de fiscalização de fronteiras, portos, aeroportos e rodovias (BRASIL, 2018).

Entretanto, o controle do Estado e das grandes empresas que detém a tecnologia, sem discutir questões éticas e de transparência, sem a oposição das pessoas, se assemelharia a um panóptico digital, favorecendo estados totalitários (HAN, 2018). Nesse esteio, salienta-se, conforme destacado por Norris e Armstrong (1999, p. 113), que "os riscos da sociedade de vigilância ligam-se tradicionalmente ao uso político de informações para controlar os cidadãos" e, quando afirma Rodotá (2008), que as tecnologias de comunicação e informação entram em conflito

com o direito à vida privada das pessoas em razão do direito à autodeterminação informativa, aproximando-se da ideia do panóptico digital.

Em razão da sensibilidade e relevância do tema, o objetivo deste artigo é analisar a inserção das TICs para o controle digital por parte das políticas de segurança pública implementadas no Brasil nos anos recentes, contribuindo para o debate acerca de como o controle digital tem avançado na elaboração de tais políticas, e da necessária reflexão acerca dos cuidados que emergem da sua implementação. Essa análise ganha relevância em um contexto no qual as políticas de segurança pública no Brasil tem ampliado o uso das TICs como solução para diminuição dos índices de criminalidade e violência.

Em termos metodológicos, foi utilizado o método qualitativo para o alcance do objetivo proposto, utilizando-se da revisão bibliográfica e documental. O artigo foi estruturado em quatro seções, incluindo essa introdução. A primeira seção é dedicada ao estudo da evolução das TICs. Na segunda seção é abordado o impacto da quarta revolução industrial, com ênfase no desenvolvimento da tecnologia na vida das pessoas e as relações homem-máquina. Na terceira seção é exposta a evolução da sociedade disciplinar até a sociedade do controle, marcada atualmente pela vigilância e desenvolvimento de um controle do Estado e das grandes empresas de tecnologia (HAN, 2018). Para, na quarta seção, ser analisado o uso da tecnologia da informação e comunicação nas políticas de segurança pública no Brasil, nos anos recentes. Ao final, são apontadas algumas considerações finais que assinalam possibilidades de novos estudos.

2. REVOLUÇÃO INDUSTRIAL E O SURGIMENTO DAS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO

Alguns autores analisam a evolução da sociedade pela perspectiva de ondas, as quais impulsionaram as transformações sociais, econômicas, políticas e culturais em cada sociedade. Essas mudanças foram particularmente impulsionadas pelas revoluções industriais. Segundo Peck (2019), a primeira onda foi a Era Agrícola na qual a propriedade era sinônimo de poder e riqueza.

A segunda onda foi iniciada com a Primeira Revolução Industrial, no século XVIII, e foi marcada pelo surgimento da máquina a vapor e da transição da manufatura para a produção em grande escala (SCHWAB, 2016). Com essa revolução, a noção de riqueza passa a ser a junção de propriedade, trabalho e capital (PECK, 2019).

A terceira onda, chamada de Era da Informação, foi iniciada a partir da Segunda Revolução Industrial e algumas das suas características permanecem até os dias atuais. A Segunda Revolução Industrial teve início na segunda metade do século XIX, sendo marcada por importantes transformações sociais, estimuladas através da invenção da energia elétrica, da utilização do petróleo em substituição ao carvão, bem como da fabricação dos motores de explosão e do desenvolvimento dos meios de comunicação, como o telefone e telégrafo (MENEZES, 2022). No contexto dessas mudanças, a invenção dos meios de comunicação apresentou-se como condição fundamental para as transformações que viriam a seguir, sendo caracterizada como a “produção em grande escala, de massificação, centralização de poder e estandardização ditado pela Era Industrial” (PECK, 2019, p. 52). Nesse esteio, surge a tecnologia digital.

Já a Terceira Revolução Industrial foi iniciada com o fim da Segunda Guerra Mundial e é caracterizada pela revolução digital e pelas TICs (MENEZES, 2022). A informação, segundo o artigo 4º, inciso I, da Lei de Acesso à Informação (LAI), Lei nº 12.257/2011 (BRASIL, 2011), são dados "processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato". A informação aliada à tecnologia passa a ser um ativo importante para a sociedade.

As TICs, segundo Castells (1999, p. 67), podem ser definidas como o "uso de conhecimentos científicos para especificar as vias de se fazerem as coisas de uma maneira reproduzível". Destacam-se o desenvolvimento de software, hardware, telecomunicações, radiodifusão, optoeletrônica e engenharia genética.

Para Rodrigues (2016, p. 15), as TICs "podem ser definidas como o conjunto total de tecnologias que permitem a produção, o acesso e a propagação de informações, assim como tecnologias que permitem a comunicação entre pessoas". Nesse sentido, a partir de 1950 o desenvolvimento tecnológico teve um papel fundamental na mudança econômico e social da época, haja vista que possibilitou o aumento da produção além da demanda e a consequente expansão do mercado.

A revolução tecnológica concentrada nas TICs modificou a base da sociedade, de forma a proporcionar uma interdependência global, através de nova forma de relacionamento entre economia, o Estado e a sociedade (CASTELLS, 2004), passando dos "insumos baratos de energia como na revolução industrial", para os "insumos baratos de informação propiciados pelo avanço na microeletrônica e telecomunicações" (WERTHEIN, 2000, p. 1).

Em 1969, na Terceira Revolução Industrial, foi criada a internet para fins militares na Guerra Fria que, inicialmente, foi denominada de *Advanced Research Projects Agency Network* (ARPANET). A internet foi expandida para utilização comercial quando da criação, por Tim Berners-Lee, em 1987, da *Word Wide Web*, conhecida por www, que é um sistema de documentos armazenados na internet que permite aos usuários acessarem textos em formato digital (AUGUSTO, 2019).

A internet, quando do surgimento, foi considerada uma tecnologia restrita, limitada. Em 1993, a *Word Wide Web* foi lançada em domínio público, gratuita e com liberação de suas ferramentas, a abertura do software-base permitiu a expansão e democratização da utilização da internet (AUGUSTO, 2019), mediante a ampliação da comunicação entre as pessoas com a consequente expansão global das informações, de forma que as telecomunicações e a informática se tornaram mais acessíveis a todos (LEVY, 1999). A rápida expansão da internet fez com que ela se tornasse "o meio indispensável e a força propulsora na formação da nova economia, erigidas em torno de normas e processos novos de produção, administração e cálculo econômico" (CASTELLS, 2004, p. 72).

Com a disseminação global da internet e da informação surge a denominada Sociedade da Informação ou Sociedade Informacional, nomenclatura criada por Castells (1999), que representou a forma como o sistema capitalista de produção passou a se reestruturar a partir da década de 1980. O avanço tecnológico como um novo paradigma resultou em grande parte de ação do Estado como líder ou mediador, que permitiu revelar uma restruturação do capitalismo muito motivado pelo avanço das tecnologias e sua interação com os sindicatos locais, o que gerou um processo de transformação social (GUEVADA, 2000 *apud* WERTHEIN, 2000), "que teria no trabalho criativo e cultura da inovação fontes de produtividade e valorização

econômica" (LOPES, 2008, p. 4) mais humanitária porque substitui os trabalhadores do fordismo e as tarefas repetitivas pelo trabalhador autônomo e mais instruído (CASTELLS, 1999).

Como características do paradigma tecnológico, a informação passa a ter uma importância singular, haja vista que passa a ser a matéria-prima da atuação do ser humano na informação propriamente dita e não apenas como meio de ser dominado para ampliar o uso da tecnologia. Importante mencionar a flexibilidade como outra característica desse paradigma tecnológico da Sociedade da Informação, visto a capacidade de reconfiguração em uma sociedade marcada pela mudança e fluidez organizacional (CASTELLS, 1999; WERTHEIN, 2000).

Ainda destacam-se a penetrabilidade, uma vez que como a informação é parte da atividade humana, os processos da existência individual ou coletiva de todos acabam sendo afetados pela nova tecnologia e lógica das redes: quando as redes se difundem, o crescimento tecnológico é exponencial, dessa forma a difusão da informação em rede amplia a sua importância e implementação em qualquer tipo de processo e crescente convergência das tecnologias, através da interligação das áreas de saber que se utilizam da tecnologia (CASTELLS, 1999; WERTHEIN, 2000).

No que tange a centralidade que as TICs conquistaram na contemporaneidade, com base no desenvolvimento da internet, é importante ressalvar dois posicionamentos: o primeiro, se refere ao impacto social, na esfera produtiva que emerge um novo regime de acumulação (LOPES, 2008); o segundo, a defesa de que as TICs podem ajudar a reparar mazelas sociais pelo seu caráter democratizante (CASTELLS, 1999).

Lopes (2008) se posiciona no sentido de que o fundamento do caráter eminentemente democrático e socializante das TICs, que diminuiria assimetrias no sistema, defendido por Castells (2004), decorre de uma leitura distorcida das macromudanças econômico-sociais e justifica posicionamento no sentido de que estar diante de uma rede com conectividade mundial, com convergência em diversas mídias e com produtos intangíveis, como a informação, seria uma espécie de capitalismo da informação.

As TICs modificam os modos de produção mudando "profundamente a lógica reprodutiva e o sistema gerencial a partir da ampliação das forças produtivas microeletrônicas, da comunicação e do trabalho intelectual" (LOPES, 2008, p. 1). Há a intelectualização de forma geral quanto aos processos de trabalho e de consumo, bem como exigências de novas habilidades para se alcançar o sucesso competitivo, mas, segundo Lopes, (2008), seria um equívoco eleger a tecnologia como um paradigma de mudança.

> [...] pois a centralidade econômica das TICs, da informação e do conhecimento nos dias atuais é reconhecer que o capitalismo – movido por suas próprias crises e conflitos entre o capital e o trabalho e não podendo mais valorizar-se, como antes, na esfera da indústria propriamente dita – foi obrigado a espraiar-se para áreas mais **imateriais** como a cultura e os serviços, ou a ver na financeirização uma excelente oportunidade, ainda que episódica, de ganhos fáceis (LOPES, 2008, p. 1, grifo do autor).

Para Vidal (2014), a internet e seus espaços mediáticos – ciberespaços – se estabeleceram como "ontológica categoria central da contemporaneidade", digitalizada, interativa e comutável, com matriz na rede global de computadores, e mudaram a interação social com a tecnologia

mediante a utilização de artefatos tecnológicos nas interações humanas culturais, impactando na análise quanto a essas novas relações com o poder, sendo uma utopia o aspecto democratizante de que não há hierarquia de poder.

No final da década de 1990, o poder de comunicação da internet provocou uma nova mudança tecnológica, a dos microcomputadores, descentralizados, autônomos por meio de dispositivos de processamento de dados distribuídos ao redor de servidores da web (CASTELLS, 1999 p. 89), o que contribuiu para a organização da sociedade em rede.

Levy (2011) apresenta o termo 'rede' como 'ciberespaço', que seria um novo meio de comunicação originada da interconexão mundial de computadores, em que as pessoas navegam na internet, adquirem e compartilham novos conhecimentos. Para Levy (2011, p. 7):

> [...] novas maneiras de pensar e de conviver estão sendo elaboradas no mundo das telecomunicações e da informática. As relações entre os homens, o trabalho, a própria inteligência dependem, na verdade, da metamorfose incessante de dispositivos informacionais de todos os tipos. Escrita, leitura, visão, audição, criação, aprendizagem são capturadas por uma informática cada vez mais avançada.

Com a criação e desenvolvimento do ciberespaço e as novas formas de pensar e conviver desenvolvidas pela interação entre os homens e a informática se perfez no desenvolvimento de uma cibercultura, que seria o conjunto de técnicas materiais e intelectuais de práticas, modos de pensamento e de valores que surgem ou evoluem em razão da relação das pessoas com o ciberpespaço (LEVY, 2011, p. 17).

A interação cada vez mais imponente entre os homens e a informática, deu origem ao surgimento de novas tecnologias que provocaram não somente impactos relacionados à cultura ou a objetivos sociais e econômicos, mas até mesmo impactos biológicos na humanidade. Para Schwab (2016), essa nova forma de interação e desenvolvimento tecnológico significou que a humanidade adentrou na Quarta Revolução Industrial[3].

3. QUARTA REVOLUÇÃO INDUSTRIAL: AVANÇOS TECNOLÓGICOS, *BIG DATA* E INTERAÇÃO HOMEM-MÁQUINA

A Quarta Revolução Industrial trouxe transformações em toda a sociedade e alterou a maneira como as pessoas vivem, trabalham e se relacionam. Há uma mudança de paradigma em curso no modo de se relacionar das pessoas com o trabalho, diversão e existência social, marcada pela "fusão dessas tecnologias e a interação entre os domínios físicos, digitais e biológicos" (SCHWAB, 2016, p. 17).

Schwab (2016) justifica a Quarta Revolução Industrial mediante as novas tecnologias e apresenta três razões: 1) velocidade da difusão da tecnologia; 2) profundidade e 3) impacto no sistema entre países – interno e externamente, atingindo socialmente a economia, política e forma de novos negócios. Nesse esteio, destacam-se os avanços tecnológicos de desenvolvimento da biotecnologia, IA, robótica, IOT, veículos autônomos, impressões em terceira dimensão (3D), computação quântica, bitcoins, economia compartilhada, blockchain,

[3] Termo cunhado por Klaus Schwab, em 2016, no Fórum Econômico de Davos (Suiça).

sistemas em nuvens, dentre outros que redefinem o ser humano ampliando sua longevidade, saúde e cognição (SCHWAB, 2016; ZUBOFF, 2018).

Para Schwab (2016) é importante aplicar quatro tipos de inteligência na criação dessas tecnologias, quais sejam: contextual, emocional, inspirada e física, que seriam estruturadas pelo aumento da conscientização dos diversos setores sociais, mediante o desenvolvimento de proposições éticas e a restruturação dos sistemas políticos, econômicos e sociais. Para Schwab (2016), a sociedade deve assumir a responsabilidade coletiva por um futuro em que a inovação e tecnologia sejam sustentáveis e sirvam ao interesse público.

Se por um lado há incerteza no desenvolvimento tecnológico nos desdobramentos gerados pela Quarta Revolução Industrial, uma vez que a Sociedade da Informação ainda tem que lidar com muitos desafios de caráter técnico, econômico e até mesmo legal, a exemplo da automação dos processos e produtos e o consequente desemprego provocado pela falta de qualificação para operacionalização das novas tecnologias e ainda a invasão de privacidade do indivíduo, por outro lado a própria evolução do paradigma já faz com os desafios acima sejam reduzidos, por exemplo, uma restruturação do emprego e qualificação dos trabalhadores e o desenvolvimento social (LEAL, 1996 *apud* WERTHEIN, 2000).

Hodiernamente a contribuição das TICs para a melhoria de alguns campos na sociedade é explícito, principalmente pela necessidade de rápida adaptação pela qual a humanidade foi obrigada a assumir em razão da pandemia de Covid-19, iniciada em 2020 e que permanece até os dias atuais. O isolamento social necessário à contenção do avanço da pandemia foi um verdadeiro estopim para a digitalização de serviços e produtos. No âmbito da saúde se destacam, dentre outros, a regulação das consultas por teleconferências, os aplicativos com orientações de saúde; no campo da educação, o desenvolvimento de aulas on-line e no campo econômico o desenvolvimento de aplicativos para cadastramento de usuários beneficiários de políticas públicas, visando ampliar o acesso das pessoas aos seus direitos.

Um aspecto importante para o desenvolvimento dessas novas tecnologias é justamente a extração e análise de dados, processos importantes para compreender o *Big Data*. Os dados passam a ser a matéria-prima, fonte de riqueza de um capitalismo, definido por Zuboff (2018) como capitalismo da vigilância, que seria uma "nova forma de capitalismo da informação que procura prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado" (ZUBOFF, 2018, p. 18).

Para Zuboff (2018) são fontes de dados: dados derivados de transações econômicas mediadas por computadores; dados mediados por computador de modo exponencial, que se utilizam de uma estrutura integrativa entre corpos e lugares conectados à internet, como a IOT, drones, carros automatizadas, IA, bancos de dados governamentais e corporativos, "câmeras de vigilância públicas e privadas, smartphones, satélites, curtidas do Facebook" (SAMPAIO e outros, 2021, p. 5), buscas no Google, e-mails, localizações e compras. O Quadro 1 demostra de forma resumida quais as áreas, fontes de dados e as técnicas que são utilizadas para o tratamento de dados, de forma a extrair perfilamento e valor comercial aos dados.

Quadro 1 – Técnicas de *Big Data Analysis*

Área	**Fontes de dados**	**Técnicas**
Análise/mineração de textos, *Information extraction.*	Redes sociais, e-mails, blogs, fóruns on-line, questionários,	*Text summarization, question answering, sentiment analysis.*

	relatórios, notícias, registros de *call centers.*	
Análise de áudio.	Dados de *call centers*, área da saúde.	*Automatic-speech recognition, phonetic-indexing, search.*
Análise de conteúdo de vídeo.	Vídeos de segurança – circuitos internos; geração descentralizada de vídeos – YouTube.	*Server-based/edge-based architecture.*
Análise de redes sociais.	Redes sociais, blogs, microblogs, social, compartilhamento de mídias, sites de respostas/perguntas, wikis.	*Content-based analytics, structure-based analytics – community detection, social influence analysis, link prediction.*

Fonte: Neto, Bonacelli e Pacheco (2020).

Ressalva-se que o rápido desenvolvimento dessas tecnologias, principalmente mais preditivas, provocadas pela acumulação, extração e análise de dados – *Big Data*, uma vez integrada e interconectadas com as pessoas, como a IA e a IOT, causam imensas inquietações sob os efeitos destas no futuro da humanidade pelo seu potencial de modificação das relações homem/natureza para homem/máquina. Os dados de análises comerciais são extraídos dos seres humanos através da análise de sua biometria, do estudo do seu corpo, seu comportamento e emoções.

O corpo humano interconectado à tecnologia começa a ser um fator de preocupação quanto aos possíveis efeitos dessa relação (ZUBOFF, 2018; SIQUEIRA; LARA, 2020; WERTHEIN, 2000), sob a ótica da vigilância ostensiva e do controle, principalmente no que tange a utilização deste como forma de expansão de um capitalismo da vigilância (ZUBOFF, 2018), em que o poder é concentrado e exercido pelo Estado e empresas de tecnologia sem que muitas vezes as pessoas percebam que estão sendo controladas.

Para Werthein (2000), os avanços tecnológicos e as melhorias no desenvolvimento social provocados pela aplicação da tecnologia na vida das pessoas superam os possíveis desafios dessa aplicação e interconexão entre tecnologia e ser humano, contudo, é feito uma ressalva de que o sentimento de perda de controle das pessoas sobre sua vida e a perda de identidade é um desafio preocupante e carecem de estratégias eficientes de intervenção para sua minimização.

A relação de utilização do corpo humano passa a ter primordial relação com o avanço das novas tecnologias de informação e controle social, contudo, a importância do corpo humano como forma de controle e poder não é algo novo, por isso para se entender o atual fenômeno de integração digital, se faz necessário dispor sobre a ideia do panóptico de Bentham e a origem da sociedade da disciplina de Foucault (1999) que evoluiu e chegou até os dias atuais de integração tecnologia/humano para a formação da sociedade da vigilância e controle digital, o panoptismo digital (HAN, 2018).

4. O CORPO HUMANO COMO FORMA DE EXERCÍCIO DA VIGILÂNCIA E CONTROLE: DA SOCIEDADE DISCIPLINAR À SOCIEDADE DO CONTROLE DIGITAL

A sociedade perpassou por uma evolução quanto à forma de controle do Estado na vida das pessoas, mediante a qual se traz à baila, inicialmente as questões relativas ao sistema penal. Atualmente com a influência da tecnologia, o Estado conseguiu ampliar o seu poder, agora se utilizando da vigilância e do controle em outros setores da vida, tais como economia, educação, com destaque para a segurança pública.

O sistema penal, em seus primórdios, contava com o imperativo da vingança privada, mediante o qual cada pessoa estava autorizada pelo Estado para reprimir violações do direito da forma que lhe conviesse, com estudos remotos ao século XIII. Posteriormente, surge a fase da vingança divina, em que o sacerdote é que se torna o responsável pela aplicação das penas e definições sobre o futuro dos infratores, em seguida o sacerdote perde poder dentro da sociedade e este poder punitivo é transferido para o monarca, nasce assim o poder punitivo estatal, também chamado de vingança pública (VIDAL, 2014, p. 19-20).

No final do século XVIII, o corpo humano passa a ser considerado como uma máquina que se pode controlar, nascendo uma mecânica do poder "através da qual se pode ter o domínio dos indivíduos para que façam o que quer o Estado e, sobretudo, operem com as técnicas, rapidez e eficácia exigidas" (VIDAL, 2014, p. 23), contexto este aplicado principalmente quanto ao tratamento dado aos prisioneiros.

Em 1794, Jeremy Bentham concebeu a ideia de projetar um prédio prisional, com uma arquitetura que permitisse o máximo controle das pessoas (OLIVEIRA, 2021) nos planos físico e estrutural, controle este exercido pela vigilância, o Panóptico. Vigiar consiste em "assistir, ouvir ou registrar as atividades de um indivíduo" (SOLOVE, 2008, p. 154), "monitorar, ouvir, interceptar" (VIDAL, 2014, p. 40).

Ao analisar o Panóptico de Bentham, Foucault (1999) vai além do pensamento do controle por vigilância e começa a aplicar uma técnica de controle dos corpos, através da análise da utilidade e docilidade destes, comumente chamada de disciplina. Nesse diapasão, outras instituições da sociedade, como escolas, igrejas, hospitais, quarteis, etc. também começam a se valer da sujeição de aptidões e forças como forma de controle através da disciplina (FOUCAULT, 1999; VIDAL, 2014).

Segundo Vidal (2014), para Foucault, o controle na sociedade disciplinar se daria mediante o quadriculamento dos indivíduos, separação dos corpos em celas, com lugares determinados para otimizar a vigilância e controle estatal, assim já se percebe a ideia do controle estatal absoluto e não apenas dos indivíduos que cometeram crimes.

A arquitetura estrutural do panóptico privilegia o fato de que haja poucos observadores para supervisionar muitas pessoas. O objetivo do panóptico, segundo Foucault (1999, p. 240), é "fazer com que a vigilância seja permanente em seus efeitos, mesmo se é descontinua em suas ações, que a perfeição do poder tenda a tornar inútil a atualidade de seu exercício". A ideia de vigilância incessante proporciona um aspecto subjetivo do efeito da disciplina, uma sujeição fictícia.

Assim, as pessoas se autodisciplinam com a ideia do olhar onipresente, com a invisibilidade do poder disciplinar, que tem um efeito de "se apropriar e retirar, tem como função maior adestrar para retirar e se apropriar ainda mais e melhor" (FOUCAULT, 1999, p. 43). A vigilância é a principal engrenagem do poder disciplinar. Ela contribui para individualizar os sujeitos a ela submetidos e generaliza a disciplina. Para Foucault (1999, p. 239), a vigilância assegura uma "distribuição infinitesimal do poder".

Segundo Schneider e Miranda (2020, p. 3), o pensamento de Foucault concretizou a análise da transição da estrutura física do panoptismo para uma tecnologia de poder "utilizada com a finalidade de obter o máximo de proveito e domínio sobre os indivíduos (homem-corpo),

sempre conectada a um capitalismo liberal em ascensão, de modo a torná-lo o mais eficaz possível".

A vigilância ostensiva se baseia na disciplina e mobiliza as forças sociais, levando ao aumento da produção e da economia, fabricando indivíduos úteis, mais dóceis e menos custosos econômica ou politicamente (FOUCAULT, 1999; POGREBINSCHI, 2004), pelo que pode ser constatado a Sociedade Disciplinar.

> O momento histórico das disciplinas é o momento em que nasce uma arte do corpo humano, que visa não unicamente o aumento das suas habilidades, nem tampouco aprofundar sua sujeição, mas a formação de uma relação que no mesmo mecanismo o torna tanto mais obediente quanto é mais útil, e inversamente. Forma-se então, uma política das coerções que são um trabalho sobre o corpo, uma manipulação calculada dos seus elementos, de seus gestos, de seus comportamentos (FOUCAULT, 1999, p. 119).

Foucault (2011) analisa o corpo humano de forma que possa ser manipulado em seus comportamentos como um mecanismo de poder para se alcançar a disciplina, quanto mais informações sobre as pessoas, maior o poder de controle. Nesse esteio surge a biopolítica, de forma que o poder passa a ser exercido sobre populações, através do foco em corpos coletivos, sob o espeque de preservação da vida através da extinção de possíveis ameaças ao bem-estar social com base em ideais econômicos liberais (SCHNEIDER; MIRANDA, 2020).

Com o avanço tecnológico, o Estado e a iniciativa privada começam a se utilizar das TICs como forma de controle e vigilância, a exemplo do desenvolvimento de *softwares* e outras tecnologias mais potentes, como a IA, para promoção de políticas públicas, inclusive de segurança, sob o argumento de políticas públicas mais modernas, eficientes e menos letais que fazem parte da sociedade digital (OLIVEIRA, 2021).

Uma vigilância que se aplica a contextos, lugares, períodos de tempo, de forma geral e não específica a uma pessoa, mas a categorias de pessoas, uma vigilância generalizada (NORRIS; ARMSTRONG, 1999). A vigilância é exercida a cada *click* na web, seja em um site ou em uma rede social, através de um *cookie*[4], ou de um pixel, ou ainda em situações corriqueiras da vida, principalmente nos centros urbanos, como a vigilância realizada pelas câmeras de vídeo em locais públicos que estão sendo usadas de maneira generalizada tanto pela iniciativa privada quanto pela administração pública. Assim, Han (2018) apresenta essa nova forma de vigilância e controle como uma nova forma de panóptico, a qual denomina panóptico digital.

O centro do poder do panóptico digital não se encontra totalmente atrelado ao Estado, ou ao poder familiar, ou de instituições, esse poder passa a ser também das grandes corporações que controlam as tecnologias, mediante a coleta, armazenamento e processamento de dados pessoais (OLIVEIRA, 2021, p. 93), inclusive fornecidos pelas próprias pessoas, através de autoexposição (HAN, 2018), gerando assim um controle geral e multilateral (VIDAL, 2014).

A diferença entre o panóptico de Benthan e o panoptico digital está que, no primeiro, o isolamento social é condição de aplicação da vigilância ostensiva, ao passo que, no panóptico

[4] *Cookie* são "pequenos arquivos de texto que contêm várias informações sobre os visitantes de um website. A principal função do *cookie* é identificar e armazenar informações desses usuários" (DONDA, 2020, p. 50)

digital, a vigilância pressupõe a conexão e comunicação intensa de seus habitantes (HAN, 2018). No lugar do *Big Brother*[5], entra o *Big Data* (HAN, 2018, p. 122).

Segundo Zuboff (2018), o Estado e as grandes corporações detentoras das tecnologias de reconhecimento de pessoas, ao se tornarem onipresentes e vigilantes, representam um risco para a sociedade, no que tange a possibilidade da utilização abusiva das informações biométricas das pessoas, seus gostos, seus passos, sua liberdade em detrimento de fins econômicos ou políticos escusos, que é uma consequência do capitalismo da vigilância.

Assim, a expansão dessas tecnologias de identificação e comunicação, catalogação e controle de pessoas mediante o compartilhamento intenso de dados, se torna ainda mais arriscada pela potencial nocividade de controle e manipulação das massas, seja pelas limitações relacionadas a possíveis falhas da aplicação da tecnologia, ou ainda a utilização desta por estados totalitários, tecnoautoritarismo, que violariam o direito à privacidade das pessoas. Segundo Barbosa (2012), o tecnoautoritarismo são ferramentas do Estado baseado em tecnologias que promovem coleta massiva e indiscriminada de dados pessoais e o uso dos dados como ferramenta de controle.

Para Solove (2008), o excesso de vigilância e controle pode ser nocivo à democracia, porque pode afetar negativamente a liberdade, a criatividade e o autodesenvolvimento das pessoas. Por outro lado, Koerner (2021, p. 4) apresenta o posicionamento de que a vigilância seria algo inerente à lógica de exploração dos dados "pois só se usam metadados, e o objetivo da elaboração de perfis individuais seria a melhoria dos serviços". Koerner (2021), também defende a restrição de controle e regulação das TICs e autorregulação pelas empresas de suas tecnologias:

> a vigilância para extração de dados é inerente à sua lógica e não será controlada ou eliminada por restrições legais ou regulações. A tendência não seria um poder instrumentário global, mas batalhas por monetização e controle. As empresas viriam a criar ambientes fechados, com maior respeito à privacidade, mas com identificação constante dos usuários [...] (KOERNER, 2021, p. 4).

O autor conclui informando que a privacidade seria um direito subjetivo mercantilizável pelo seu titular, cuja liberdade de escolha se exerceria ao contratar os termos de uso para a extração dos dados realizada pelas empresas. Nesse diapasão, Batkins (2019) afirma que o aspecto da vigilância não seria um desafio ao desenvolvimento das TICs, conforme defende Zuboff (2018), pois seria inerente ao desenvolvimento da tecnologia.

A aplicação das TICs pelo Estado na promoção de políticas públicas, principalmente no âmbito da segurança pública é algo não pacificado, haja vista possíveis conflitos entre a utilização da tecnologia e as dicotomias entre controle e vigilância versus direitos fundamentais das pessoas, nesse sentido, na próxima seção serão apresentados as aplicações das tecnologias na segurança pública brasileira, como reflexões inicias acerca dessas complexas relações.

5. O USO DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO COMO POLÍTICA DE SEGURANÇA PÚBLICA NO BRASIL

[5] O *Big Brother* é um grande irmão que, dentro das ideias de George Orwell, no livro 1984, atua como um poder dentro de uma sociedade fictícia em que tudo vê e controla todos.

A segurança pública pode ser definida como

> um conjunto integrado e otimizado envolvendo instrumentos de coação, justiça, defesa dos direitos, saúde e social. Portanto, a segurança pública se inicia com prevenção e se finda na reparação do dano, no tratamento das causas e na reinclusão na sociedade do autor do ilícito (LIMA; OLIVEIRA; COSTA, 2021, p. 106).

Nesse sentido, a evolução da sociedade e aplicação das TICs se perfizeram como um mecanismo de utilização da tecnologia para prevenção e repressão de crimes, contribuindo para o desenvolvimento de políticas de segurança pública no Brasil menos letais e mais eficientes (ALCADIPANI, 2020).

Historicamente, na época colonial brasileira, os crimes atentavam contra a vontade do Soberano e eram tratados como faltas morais ou religiosas. As atribuições policiais e judiciais eram exercidas por poucos cargos dentro da hierarquia de poder e as práticas de punição aos infratores eram realizadas mediante degredo, para pessoas mais abastadas, e de açoite, para os escravos. As práticas de investigação eram feitas por suspeitas sobre o indivíduo e as provas colhidas mediante tortura judicial (OBSERVATÓRIO DE SEGURANÇA, 2020).

A segurança pública sob o aspecto estatal remonta a 1808, com a criação da Intendência Geral de Polícia e Corte do Estado do Brasil, na cidade do Rio de Janeiro, que tinha como função delegar e desempenhar funções de polícia judiciária, com o estabelecimento de poderes de fiscalização e aplicação de punições (MARCINEIRO; GIOVANNI, 2005). Em 1824, o Brasil promulgou sua Constituição, um Código Criminal, em 1830, e um Código de Processo Criminal, em 1832. A lei penal começou a entender o crime como infração penal e o sofrimento físico passou a dar lugar a penas como o degredo e a privação de liberdade (OBSERVATÓRIO DE SEGURANÇA, 2020).

Com o advento das Constituições de 1934, 1937 e 1946 e ainda com o Código Penal de 1940 e o Código de Processo Penal de 1941 ocorreram diversas mudanças pelos entes integrantes da segurança pública[6] quanto ao estabelecimento de normas relativas ao processamento de crimes através de uma centralização e racionalização da administração pública, todavia, com a Ditadura Militar, os direitos constitucionais dos investigados e capturados pelas polícias e para os que estavam internados em manicômios foram relegados, mediante a adoção de torturas e degradações, segundo notícias da imprensa à época (OBSERVATÓRIO DE SEGURANÇA, 2020).

A democratização do Brasil iniciou em 1985 e foi consagrada com a Constituição Federal de 1988, que, em seu artigo 5º, *caput*, então vigente, veio a disciplinar a segurança pública como um direito fundamental, como dever do Estado, direito e responsabilidade de todos a ser exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio (artigo 144).

Ainda, a Constituição de 1988 descentralizou a segurança pública mediante atribuições e responsabilidades atribuídas às policias federal, polícia rodoviária federal; polícia ferroviária federal; polícias civis; polícias militares e corpos de bombeiros militares e polícias penais federal, estaduais e distrital.

[6] Ministério Público, Polícias, Magistrados e Júri.

Apesar da nova configuração político-institucional após a Constituição Federal de 1988, baseada na instituição da defesa dos direitos humanos, os institutos jurídicos tradicionais do Brasil não promoveram a integração dos direitos definidos pela Constituição com as práticas das polícias e do judiciário nas aplicações punitivas, aliado a isso, houve um exponencial crescimento da violência e criminalidade e cada vez mais a segregação da iniciativa privada, vide as iniciativas de condomínios fechados, gradeamento de casas, adoção de equipamentos de segurança e contratação de segurança privada (OBSERVATÓRIO DE SEGURANÇA, 2020).

Para tentar se proteger da violência crescente, o Estado passou a investir mais em armas e equipamentos, e a iniciativa privada em grades, muros e dispositivos eletrônicos (OBSERVATÓRIO DE SEGURANÇA, 2020). O sentimento de insegurança e a cultura do medo inundaram a sociedade, sobretudo nos grandes centros urbanos e diante dessa nova problemática, segundo Barbosa e Santos (2009), não há a possibilidade da resolução da violência somente com ações e políticas repressivas.

Segundo a Política Nacional de Segurança Pública e Defesa Social (PNSPDS) de 2018-2028, o Brasil, em 2013, concentrava 11% dos homicídios do planeta[7], e afirma: "Os dados do Ministério da Saúde indicam que o Brasil passou de 11,7 homicídios por 100 mil habitantes em 1980 para 30,3 em 2016, o que resultou na morte de 1,4 milhões de pessoas em território nacional no período" (BRASIL, 2018).

Ademais, o crime organizado está cada vez mais munido de armas de grosso calibre e se valendo de novas tecnologias e estratégias em ações que dificultam as ações de segurança pública e a mentalidade de apenas utilização da força bruta estatal. Assim, o Estado tem que investir em agentes de segurança pública, de forma a ampliar os conhecimentos científicos, se aprimorar e utilizar as tecnologias a seu favor, visto que a cada vez mais "há uma possibilidade real de que com o uso das tecnologias por parte dos criminosos precisamos ter mais policiais que dominem a lógica das tecnologias digitais" (ALCADIPANI, 2020, p. 1).

Diante do cenário da necessidade de expansão do uso das TICs nas políticas públicas, o Estado, através do Governo Federal, desenvolveu planos de desenvolvimento das políticas de segurança pública, com a previsão de "melhorar a governança do setor público, aumentando a eficiência e eficácia das ações de governo" (BRASIL, 2018, p. 20) se utilizando das tecnologias no combate à criminalidade como mais uma tentativa de melhorar a qualidade da segurança pública no Brasil.

Nesse sentido, o PNS de 2000 (BRASIL, 2000) é considerado a primeira política de segurança pública brasileira focada no estímulo à inovação tecnológica. O PNS de 2000 previu a integração de políticas de segurança, sociais e ações comunitárias como medida importante para o aperfeiçoamento da segurança pública no Estado democrático de direito (LOPES, 2009), bem como o objetivo de reprimir e prevenir a criminalidade no Brasil.

[7] "O documento que analisou a taxa de violência letal em 121 países no ano de 2013 registra que o Brasil, com 2,8% da população mundial, concentra 11% dos homicídios do planeta, realidade que, infelizmente, mostra tendência no sentido de agravar-se a cada ano" (BRASIL, 2018, f. 23).

De 2003 a 2017 foram instituídos outros programas[8] e políticas de segurança pública, com o escopo de articular ações policiais e da justiça criminal, restaurar a ordem pública e a incolumidade física e patrimonial das pessoas, a exemplo da criação da Força Nacional, em 2004, e o estimulo de que financiadoras de projetos de inovação incentivassem a pesquisa de projetos relativos à aplicação da tecnologia à segurança pública.

Importante trazer à baila que, entre 2002 e 2010, a Financiadora de Estudos e Projetos (FINEP), principal agência de apoio a projetos de inovação no Brasil, financiou 53 projetos relativos ao desenvolvimento da segurança pública, dos quais 34 se referiram ao desenvolvimento de TICs, predominando o desenvolvimento de softwares para treinamento e identificação, radares e antenas (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2013).

Dentro do estímulo à inovação foi publicada a Lei nº 12.258/2010 que modificou a Lei de Execuções Penais e promoveu 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. Em 2011, foi publicada a Lei nº 12.403, que modificou o Código de Processo Penal e instituiu o monitoramento eletrônico como medida cautelar no art. 319, inciso IX (VIDAL, 2014). O monitoramento eletrônico consiste em condutas rastreadas via satélite que utiliza a radiofrequência e informações com criptografia de dados sobre o local onde se encontra o monitorado:

> No monitoramento eletrônico de condutas, o usuário é rastreado via satélite através de um aparelho chamado Sistema de Acompanhamento de Custódia 24 horas - SAC 24, que funciona através de rádio frequência e informações criptografadas dos dados sobre a posição em que se encontra o usuário. Os dados colhidos pelo sistema são enviados a um servidor e podem ser acessados por um terminal conectado à *internet*. O controle pode ser realizado através do uso de um bracelete, pulseira ou tornozeleira. O dispositivo utilizado pelo usuário possui um sensor antifraude e ruptura e possui uma bateria que dura em média 12 horas. Existe uma outra forma de monitoramento através de um *microchip* desenvolvido por nanotecnologia e que seria inserido no corpo do apenado, sendo os dados deste *chip* transmitidos via satélite, para que se saiba sua localização exata (VIDAL, 2014, p. 49, grifo do autor).

Para os defensores do monitoramento eletrônico, a tecnologia se apresenta como fator importante para a redução da população carcerária, diminuição dos gastos públicos com presos e reinserção no convívio social (GRECO, 2011; VIDAL, 2014). O Superior Tribunal de Justiça (STJ), em decisão de 2011, se manifestou favorável quanto à legalidade do monitoramento eletrônico e ainda decidiu a vantagem do equipamento – tornozeleira ou pulseira eletrônica – substituir a vigilância policial. Por outro lado, há argumentos contra o monitoramento eletrônico, tais como possibilidade de retorno a um Estado totalitário, em que a sociedade seria a própria prisão, bem como estigmatização social da pessoa em razão da utilização do equipamento de monitoramento em público e ainda violação ao direito a intimidade e privacidade (KARAN, 2007).

[8] Em 2004 ocorreu a criação da Força Nacional de Segurança Pública; em 2007 foi criado o Programa Nacional de Segurança com Cidadania (PRONASCI) com o objetivo de promover o financiamento de ações de prevenção à violência; em 2012 foi lançado o Plano Brasil Mais Seguro, que apresentou como objetivo a redução da criminalidade violenta no país; em 2015 foi anunciado o Plano Nacional para Redução de Homicídios (PNRH). (BRASIL, 2018, p. 34).

Em 2012, foi publicada a Lei nº 12.681, que criou o Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Drogas (SINESP), um sistema de TICs que se utiliza de uma plataforma de informações integradas das bases de dados do Governo Federal e dos estados, com o escopo de criar uma estrutura de gestão de informações em nível nacional, com a finalidade de produzir, coletar, sistematizar e disponibilizar informações para a segurança pública (SANTOS; LIMA; SOUZA, 2020).

Uma crítica ao SINESP é abordada por Santos, Lima e Souza (2020, p. 17) quando afirmam que "a construção de um sistema que, por disposição legal, necessita da participação ativa de todas as unidades da Federação encontra de pronto um grande obstáculo inicial: diferentes realidades culturais, técnicas, metodológicas e orçamentárias" e recomendam em seu trabalho a sistematização da base de dados de forma mais integrativa e interoperável, se utilizando de inteligência operacional.

Ainda, em 2012, o Ministério da Justiça, com o objetivo de otimizar recursos públicos, de forma a desenvolver ações de fomento para ações de segurança pública, publicou o Edital Público 2012 e forneceu um guia de apresentação de propostas para o desenvolvimento de convênios do governo federal com os estados e municípios. No guia continha informações de como captar recursos do Fundo Nacional de Segurança Pública, nas ações de prevenção da criminalidade, com destaque para implantação ou expansão do videomonitoramento no país. Esse guia se transformou em um marco para o desenvolvimento do videomonitoramento no Brasil, visto que passou a destinar recursos para tal finalidade (FREITAS FILHO, 2018).

Em 2018 foi publicado o Plano Nacional de Segurança Pública de Desenvolvimento Social (PNSP) 2018-2028 (BRASIL, 2018), criado pela Lei nº 13.675/2018, regulamentada pelo Decreto nº 9.489/2018, e que teve como escopo criar o Sistema Único de Segurança Pública (SUSP) para desenvolvimento de governança, "através da padronização de dados, integração tecnológica, de inteligência e operacional" (BRASIL, 2018, p. 8), um marco no desenvolvimento e estímulo tecnológico. Os objetivos previstos no SUSP foram o estabelecimento de princípios e estratégias da atuação do Estado na segurança pública com controle, transparência e prestação de contas. Uma importante previsão, visto a necessidade de *accountabilit*, das ações do poder público (BRASIL, 2018).

Ainda em 2018, o Conselho Nacional de Justiça (CNJ) criou o Banco Nacional de Monitoramento de Prisões (BNMP), base de dados 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 (SANTOS; LIMA; SOUZA, 2020). O BNMP 2.0 "é um sistema eletrônico que auxilia 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" (SANTOS; LIMA; SOUZA, 2020, p. 10).

Em setembro de 2021, através do Decreto nº 10.882/2021, foi publicado o PNSP 2021-2030 (BRASIL, 2021). Esse plano é constituído de objetivos, ações estratégicas, metas, sistema de governança e orientações aos entes federativos (artigo 1º, §2º). São objetivos do PNSP 2021-2030: definir ações estratégicas, metas e indicadores para a efetivação do plano; determinar ciclos para implementação, monitoramento e avaliação da política; estabelecer estratégias de governança e de gerenciamento de riscos e ter papel de orientação aos demais entes

federativos[9]. Dentre as ações estratégicas do PNSP 2021-2030, percebe-se o intuito do legislador em promover a expansão tecnológica na promoção de políticas de segurança pública, deixando claro a estratégia de padronização, integração e interoperabilidade dos dados sobre segurança pública entre União, estados, Distrito Federal e municípios. Destaca-se que o PNSP 2021-2030 apresentou os requisitos necessários para se concretizar a estratégia nº 7:

> a) Padronizar, integrar, coletar e consolidar dados e informações de interesse da segurança pública e defesa social, para o tratamento, a análise e a divulgação estatística; b) Promover a modernização e a interoperabilidade dos sistemas de interesse da segurança pública e defesa social com vistas à integração, à gestão, à análise e ao compartilhamento de dados e informações; c) Integrar e aprimorar a base de dados entre os órgãos integrantes do SNT e os demais órgãos de segurança Pública e defesa social; e d) Ampliar os mecanismos de proteção e segurança de dados (BRASIL, 2021).

De igual modo, a estratégia nº 8 do PNSP 2021-2030 também prevê o fomento ao fortalecimento das atividades de inteligência nas instituições de segurança pública e defesa social, por meio de atuação do SUSP, com o objetivo de analisar, gerir e compartilhar dados e informações:

> a) Promover ações com o objetivo de dotar as instituições de segurança pública com ferramentas de inteligência modernas, padronizadas e integradas para a produção de conhecimento, em conformidade com a legislação aplicável; b) Atuar na estruturação e no aperfeiçoamento das atividades de inteligência penitenciária; c) Estimular a cooperação e o intercâmbio de informações de inteligência de segurança pública com instituições estrangeiras congêneres; d) Promover a criação e a estruturação da atividade de inteligência de trânsito; e) Integrar os sistemas e os subsistemas de inteligência de segurança pública e promover o compartilhamento de tecnologias interagências; e f) Estimular a articulação e a cooperação entre o sistema de inteligência de segurança pública com setores de inteligência da iniciativa privada, em conformidade com a legislação aplicável à proteção de dados (BRASIL, 2021).

Em 2021, ganhou destaque a adoção de câmeras corporais nos uniformes dos policiais, como política de segurança pública, também chamada de câmeras *body-worn*, que são como pequenas câmeras de vídeo, instaladas na farda, capacete ou óculos dos policiais, que tem a capacidade de captar e gravar, do ponto de vista dos policiais, vídeo e áudio das atividades desenvolvidas por eles em sua rotina policial, a exemplo de gravações de trânsito, detenções, revistas, interrogatórios, tanto no uso da força quanto na redução de queixas externas a atuação dos agentes (ALBARDEIRO, 2020).

O estado de São Paulo foi pioneiro na adoção da prática, sendo replicada em outros estados como o Rio de Janeiro e Santa Catarina. Sob a ótica da sociedade civil, as imagens podem servir para garantir a disciplina e evitar o abuso de autoridade e os oficiais que defendem o projeto afirmam que as câmeras proporcionam segurança aos agentes (DUARTE, 2022). O dispositivo eletrônico acoplado as fardas funcionam da seguinte forma:

> O dispositivo é designado a um só agente, que precisa desbloqueá-lo com reconhecimento facial; O sistema reconhece o policial e solta a câmera, que já começa a gravar e a transmitir para o Centro de Comando e Controle; A autonomia do aparelho é de 12 horas; Por padrão, o aparelho grava em média

[9] Artigo 2º e incisos do Decreto 10.882/2021 que instituiu o PNSP 2021-2030.

> resolução, e as imagens ficam armazenadas por 60 dias; Há a possibilidade, porém, de ativar o modo HD: nesse caso, as imagens são registradas em alta definição e ficam salvas em uma nuvem por até um ano; Tanto o policial em ação quanto o agente que estiver acompanhando do Centro podem acionar o HD; Os órgãos de controle, como as corregedorias, a Defensoria e o Ministério Público, poderão pedir as imagens (G1 RIO, 2022).

Alcadipani, Bueno e Lima (2021), quando questionados sobre o uso das câmeras nas fardas dos policiais, afirmaram que os resultados são positivos para a profissionalização da polícia, corroborando com a redução da letalidade e preservação de provas nas ações policiais. Ainda se destaca um estudo realizado na análise da Polícia Militar de São Paulo que constatou que com a utilização das câmeras acopladas a farda dos policiais chegou a zero os homicídios nas áreas pesquisadas e foram aferidos baixos índices de lesão corporal (PAGNAN, 2021). Ainda os defensores dessa política se baseiam entre outros argumentos, no aumento da transparência e da legitimidade policial, coleta de provas, formação dos policiais, resolução célere de queixas (ALBARDEIRO, 2020).

Por outro lado, a política pública de acoplamento das câmeras nas fardas dos policiais também é questionada quanto ao argumento de violação da privacidade dos cidadãos, privacidade dos policiais, consequências indesejadas, com gravação de momentos constrangedores que podem intimidar policiais e a própria vítima que podem inibir algumas abordagens (ALBARDEIRO, 2020).

Uma aliada tecnológica para o desenvolvimento de políticas públicas de segurança mais personalizadas e eficientes no combate à criminalidade é a IA, sendo amplamente utilizada no videomonitoramento com reconhecimento facial biométrico, destacando-se as habilidades que softwares de computados possuem de analisar rostos humanos constante de uma base de dados específica, se utilizando de conexões de internet para catalogar indivíduos, via captação de sua biometria extraída por smartphones, computadores e câmeras de vigilância (COSTA; OLIVEIRA, 2019).

Como política pública no Brasil, o reconhecimento facial biométrico começou a ser estimulado e previsto dentro dos objetivos do PNS de 2018, quando da previsão dessa possibilidade de uso da tecnologia no objetivo/estratégia nº 8, uma vez que há a expressa menção de estímulo pelo Estado, da utilização de reconhecimento facial como política de segurança pública para fiscalização de fronteiras, divisas interestaduais, portos, aeroportos, rodoviárias e ferrovias (PNS, 2018, p. 57), sendo o Estado da Bahia pioneiro na implementação do reconhecimento facial como política de segurança pública, em 2018.

A análise de múltiplos dados pessoais, até mesmo sensíveis, como a voz, biometria facial, das mãos, dedos e da íris, depois que coletados, são tratados pela IA para se tornarem um algoritmo, criar padrões dos indivíduos e, a partir daí, possibilitar a sua identificação e comparações com maior assertividade dos resultados da tecnologia (ARAUJO; CARDOSO; PAULA, 2021). Nesse sentido, essa personalização realizada pelo reconhecimento facial via IA, tem resultado em formulação e implementação de políticas públicas, com maior integração entre homem/máquina. Ressalta-se, entretanto que a utilização da IA na segurança pública não é pacífica, visto que apresenta vantagens (ALCADIPANI, 2020; PAGNAN, 2021; DUARTE, 2022), mas também críticas quanto a possíveis violações de direitos fundamentais (SILVA, 2020; NORRIS; ARMSTRONG, 1999; SOLOVE, 2011).

Diante da análise dos planos nacionais de segurança pública no Brasil, no aspecto da promoção de políticas pública de segurança com o envolvimento da tecnologia, percebe-se um avanço no estímulo à inovação importante para a sociedade ao longo das últimas duas décadas, como forma de ampliar a eficiência da promoção de tecnologias como políticas de segurança pública. No entanto, há de se avançar nas análises de tais políticas, buscando compreender seus limite e possibilidades como estratégia de melhoria dos índices de criminalidade no país, mas também, evitando possíveis violações de direitos fundamentais das pessoas.

6. CONSIDERAÇÕES FINAIS

Um tema instigante que denota interdisciplinaridade ao tratar sobre ações de governança, direito e políticas públicas na sociedade contemporânea, o presente artigo objetivou analisar a inserção das TICs nas políticas de segurança pública implementadas no Brasil nos últimos anos, e o controle digital por parte das políticas de segurança pública implementadas, com sua evolução de uma sociedade disciplinar para uma sociedade do controle digital.

Demonstrou-se, a ampliação sistemática do uso das TICs como solução para diminuição dos índices de criminalidade e violência no Brasil, destacadas na evolução da sociedade e no impacto das TICs, mediante os desdobramentos das revoluções industriais, do surgimento da Sociedade da Informação e da sua evolução para o desenvolvimento do Panoptismo Digital.

Nesse diapasão, destacaram-se o fato de que o impacto das TICs e o surgimento da internet, principalmente após 1987, com a internet comercial, contribuíram sobremaneira, para a valorização da informação e, posteriormente, do tratamento de dados pessoais como um ativo extremamente valioso para a construção de perfis de consumo, difundir produtos e serviços e proporcionar mais lucros e riquezas para as empresas que detém o *know-how* da tecnologia e controle e poder para os governos.

A construção de perfis das pessoas, através da exploração do corpo humano, em sua forma de extração de dados biométricos e análise comportamental ou de emoções para personalizar seus produtos e serviços, levou-se a conclusão de que esta prática, se realizada de forma reiterada e indiscriminada pode implicar, caso não haja controle efetivo desta utilização, em uma sociedade da vigilância, marcada pelo panoptismo digital.

No que se refere à aplicação da tecnologia de IA de reconhecimento facial como política pública no Brasil, foram identificados planos ou projetos no Brasil, a partir da aplicação das tecnologias de IA. Observou-se a temporalidade, a partir dos anos 2000, do estímulo à formulação de políticas públicas envolvendo a tecnologia (BRASIL, 2000) e a primeira menção ao reconhecimento facial, via IA, no PNSP 2018-2028 para fiscalização de fronteiras, portos e aeroportos. Pelo estudo, foi constatado de que houve uma maior formulação de políticas públicas de natureza tecnológica, principalmente após a existência de editais de financiadoras públicas, a partir de 2012.

Nesse sentido, esse artigo contribuiu para a identificação da inserção das TICs nas políticas públicas de segurança, e apesar de não ter a pretensão de preencher na totalidade essa lacuna, espera-se que as reflexões propostas possibilitem para que estudos futuros sejam ampliados na compreensão árdua e desafiadora tarefa de entender o uso das TICs, especialmente nas políticas de segurança pública, sua potencialidades e limitações sob a ótica dos direitos fundamentais da

liberdade, privacidade e proteção dos dados pessoais, e os riscos de uma hipervigilância, que é uma característica de Estados totalitários.

REFERÊNCIAS

ALBARDEIRO, N. M. E. **Body-Worn Cameras: Perceção dos polícias com funções operacionais da Divisão Policial da Amadora**. 2020. 98 f. Dissertação (Mestrado) – Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa, 2020. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/32969/1/156427_Albardeiro_Body-Worn%20Cameras-Perce%c3%a7%c3%a3o%20dos%20Pol%c3%adcias%20com%20fun%c3%a7%c3%b5es%20operacionais%20da%20Divis%c3%a3o%20Policial%20.pdf. Acesso em: 03 abr. 2022.

ALCADIPANI, R.; BUENO, S.; LIMA, R. S. de. Evolução das mortes violentas intencionais no Brasil. *In*: FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Anuário Brasileiro de Segurança Pública 2021**, [São Paulo], ano15, 2021. ISSN 1983-7364. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2021/07/anuario-2021-completo-v4-bx.pdf. Acesso em: 03 maio 2022

ALCADIPANI, R. Novas tecnologias e a criminalidade: o crime do futuro e a polícia do passado. **Estadão**, São Paulo, 14 jan. 2020. Disponível em: https://politica.estadao.com.br/blogs/gestao-politica-e-sociedade/novas-tecnologias-e-a-criminalidade-o-crime-do-futuro-e-a-policia-do-passado/. Acesso em: 03 abr. 2022.

ARAUJO, R. A.; CARDOSO, N. D.; PAULA, A. M. Regulação e uso do Reconhecimento facial na Segurança Pública do Brasil. **Revista de Doutrina Jurídica**, Brasília-DF, v. 112, 2021.

AUGUSTO, T. Há 26 anos, WWW em domínio público permitiu a expansão da Internet como conhecemos. **Canaltech**, abr. 2019. Disponível em: https://canaltech.com.br/internet/ha-26-anos-www-em-dominio-publico-permitiu-expansao-da-internet-como-conhecemos-138027/. Acesso em: 04 jun. 2021.

BARBOSA, Attila Magno e Silva. Da disciplina ao controle: novos processos de subjetivação no mundo do trabalho. 2012. Disponível em: https://periodicos.ufsc.br/index.php/politica/article/view/21757984.2012v11n22p75. Acesso em: 28 ago. 2021.

BARBOSA, Kátia Borges; SANTOS, Fabiele Almeida Dos. Direitos humanos e segurança pública no Brasil: caminhos que se cruzam, 2009.

BATKINS, S. The Tech Giants Are Out to Get You. **Regulation**, 52, p. 52-53, Summer 2019.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial da União**, Brasília, DF, 2011.

_____. Decreto nº 10.882, de 03 de dezembro de 2021. Regulamenta o Tratado de Marraqueche para Facilitar o Acesso a Obras Publicadas às Pessoas Cegas, com Deficiência Visual ou com Outras Dificuldades para Ter Acesso ao Texto Impresso. **Diário Oficial da União**, Brasília, DF, 06 dez. 2021a. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Decreto/D10882.htm#:~:text=DECRETO%20N%C2%BA%2010.882%2C%20DE%203%20DE%20DEZEMBRO%20DE%202021&text=Regulamenta%20o%20Tratado%20de%20Marraqueche,Ter%20Acesso%20ao%20Texto%20Impresso. Acesso em: 04 ago. 2021.

BRASIL. Ministério de Segurança Pública. **Plano Nacional de Segurança 2000**. Disponível em: https://cispregional.mpba.mp.br. Acesso em: 20 dez. 2020.

_____. Ministério da Segurança Pública. **Plano Nacional de Segurança Pública e Defesa Social 2018-2028**. 2018. Disponível em: https://cispregional.mpba.mp.br/wp-content/uploads/2020/04/11.-Plano-Nacional-de-Seguran%C3%A7a-P%C3%BAblica-2018-compactado.pdf. Acesso em: 20 dez. 2020.

_____. Ministério de Segurança Pública. Plano Nacional de Segurança 2000.
BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. **Diário Oficial da União**. Brasília, DF, 2022c. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 11 fev. 2022.

CASTELLS, M. **A Galáxia Internet:** Reflexões sobre Internet, Negócios e Sociedade. [S.L.: s.n.], 2004.

_____. **A Sociedade em rede**. Tradução: Rosineide Venâncio Majer; Atualiz. 6. ed.: Jussara Simões. São Paulo: Paz e Terra, 1999. (A era da informação: economia, sociedade e cultura, v. 1). Disponível em: https://globalizacaoeintegracaoregionalufabc.files.wordpress.com/2014/10/castells-m-a-sociedade-em-rede.pdf. Acesso em: 04 maio 2020.

COSTA, R. S.; OLIVEIRA, S. R. O uso de tecnologias de reconhecimento facial em sistemas de vigilância e suas implicações no direito à privacidade. **Revista de Direito, Governança e Novas Tecnologias**, Belém, v. 5, n. 2. P. 1-21, jul./dez. 2019.

DONDA, D. **Guia Prático de Implementação da LGPD**. Labrador: São Paulo, 2020.

DUARTE, D. E. Câmeras corporais e a ação policial: As condições de emergência e os impactos dos dispositivos de controle em São Paulo. **NEV**, São Paulo, 2022. Disponível em: https://nev.prp.usp.br/noticias/cameras-corporais-e-acao-policial-as-condicoes-de-emergencia-e-os-impactos-dos-dispositivos-de-controle-em-sao-paulo/. Acesso em: 01 jun. 2022.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 7º Anuário Brasileiro de Segurança Pública 2013. Disponível em: https://forumseguranca.org.br/storage/7_anuario_2013-corrigido.pdf. Acesso em: 12 fev. 2022.

FOUCAULT, M. **Vigiar e punir:** nascimento da prisão. Petrópolis: Vozes, 1999.

_____. **Microfísica do Poder**, 2011. Disponível em: http://www.foucault.ileel.ufu.br/foucault/textos/microfisica-do-poder. Acesso em: 02 jan. 2021.

FREITAS FILHO, N. B**. O videomonitoramento nas tecnologias de comunicação na Secretaria de Segurança Pública do Estado da Bahia** in MAGALHÃES, A. C. S.; JESUS, A. R. de. Telecomunicações na Segurança Pública do Estado da Bahia: Do sino a era digital. Biblioteca Digital COGER, 2018. Disponível em: https://bibliotecacoger.ssp.ba.gov.br/. Acesso em: 03 maio 2022.

G1 RIO. **Policiais vão começar a usar câmera nos uniformes no dia 16 de maio, anuncia governo**. Rio de Janeiro, 27 abr. 2022. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2022/04/27/policias-vao-comecar-a-usar-cameras-nos-uniformes-no-dia-16-de-maio-anuncia-governo.ghtml. Acesso em: 30 abr. 2022.

GRECO, Rogério. **Direitos humanos, sistema prisional e alternativas à privação de liberdade.** São Paulo: Saraiva, 2011.

HAN, B. C. **No enxame:** perspectiva do digital. Tradução Lucas Machado. Petrópolis, RJ: Vozes, 2018.

KOERNER, A. Capitalismo e vigilância digital na sociedade democrática. **Rev. Bras. Ci. Soc**., v. 36, n. 105, 2021. Disponível em: https://www.scielo.br/j/rbcsoc/a/3RSTj7mCYh6YcHRnM8QZcYD/. Acesso em: 03 abr. 2021

LEVY, P. **Cibercultura**. São Paulo: Editora 34, 1999.

_____. **Inteligencia Colectiva**: por uma antropologia del ciberspacio. Trad. do francês por Felipe Mártinez Álvarez. [S.L.: s.n.], 2011. Disponível em: https://drive.google.com/drive/folders/0B-YLV8egGwSuUm9yRldCbWgzbVU. Acesso em: 10 dez. 2020.

LIMA, G. D. de; OLIVEIRA, N. F. de; COSTA, S. T. da S. Gestão da Segurança Pública no Brasil: A utilização da Tecnologia a favor da sociedade. **GETEC**, Monte Carmelo, MG, v. 10, n. 25, p. 101-118, 2021. Disponível em: https://revistas.fucamp.edu.br/index.php/getec/issue/view/142. Acesso em: 04 fev. 2022.

LOPES, E. S. **Política e segurança pública: uma vontade de sujeição**. Rio de Janeiro: Contraponto, 2009.

LOPES. R. S. As TICs e a "Nova Economia": Para além do determinismo Tecnológico. **Ciência e Cultura**, São Paulo, v. 60, n. 1, 2008. Disponível em: http://cienciaecultura.bvs.br/scielo.php?script=sci_arttext&pid=S0009-67252008000100012. Acesso em: 03 abr. 2021.

MARCINEIRO, N. P; GIOVANNI, C. **Polícia Comunitária**: Evoluindo para a polícia do século XXI. Florianópolis: Insular, 2005.

MENEZES, P. Fases da Revolução Industrial: características e mudanças na produção. **Diferença**, [S.L.], 2022. Disponível em: https://www.diferenca.com/revolucao-industrial/. Acesso em: 03 dez. 2022.

NETO, V. J. S.; BONACELLI, M. B. M; PACHECO, C. A. O sistema tecnológico digital: Inteligência artificial, computação em nuvem e Big Data. **Revista Brasileira de Inovação**, Campinas, SP, n. 19, p. 1-31, 2020. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/rbi/article/view/8658756. Acesso em: 14 fev. 2022.

NORRIS, C., ARMSTRONG, G. **The Maximun Surveillence Society**. The Rise of CCTV. Oxford: Berg, 1999.

OBSERVATÓRIO DE SEGURANÇA PÚBLICA. Site sobre segurança pública. 2020. Disponível em: https://www.observatoriodeseguranca.org/a-seguranca-publica-no-brasil/#tab-polticasdeseguranapblica. Acesso em: 10 mar. 2022.

OLIVEIRA. S. R. Sorria você está sendo filmado. Repensando Direitos na Era do Reconhecimento Facial. **Revista dos Tribunais**. São Paulo. 2021.

PAGNAN, R. No 1º mês de uso das câmeras 'grava-tudo', PM de SP atinge menor letalidade em 8 anos. **Folha de São Paulo**, São Paulo, 10 jul. 2021. Disponível em: https://www1.folha.uol.com.br/cotidiano/2021/07/no-1o-mes-de-uso-das-cameras-grava-tudo-pm-de-sp-atinge-menor-letalidade-em-8-anos.shtml. Acesso em: 02 maio 2022.

PECK, P. P. **Direito Digital**. 6. ed. São Paulo: [s.n.], 2019.

PINHEIRO, E. N.; FERRAZ, D. O uso da inteligência artificial na criação de profiling e o direito do titular dos dados na revisão automatizada. *In*: JESUS, D. M. de (Org.). **Estudos multirreferenciados**. Salvador: Mente Aberta, 2021. p. 29-41, (Ciências Sociais Aplicadas, V).

POGREBINSCHI, T. Foucault, para além do poder disciplinar e do biopoder. **Lua Nova**: Revista de Cultura e Política, [S.L.], n. 63, p. 179-200, 2004. (Identidade e igualdades em conflito).

RODRIGUES, R. B. **Novas Tecnologias da Informação e da Comunicação**. Recife: IFPE, 2016. ISBN: 978-85-9450-008-3. Disponível em: https://www.ufsm.br/app/uploads/sites/413/2018/12/arte_tecnologias_informacao_comunicacao.pdf. Acesso em: 03 mar. 2022.

RODOTÀ, S. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar. 2008.

SANTOS, A. S.; LIMA, E. G. de; SOUZA, W. B. de **Tecnologia da Informação na Segurança Pública**: a necessidade de criação de uma base nacional de dados de registro de ocorrência e atendimentos de emergência. 2020. Disponível em: https://dspace.mj.gov.br/bitstream/1/4606/1/Tecnologia%20da%20Informa%C3%A7%C3%A3o%20na%20Seguran%C3%A7a%20P%C3%BAblica_A%20necessidade%20de%20cria%C3%A7%C3%A3o%20de%20uma%20Base%20Nacional%20de%20Dados%20de%20Registr

o%20de%20Ocorr%C3%AAncia%20e%20Atendimento%20de%20Emerg%C3%AAncia.pdf. Acesso em: 04 maio 2022.

SCHNEIDER, C. B.; MIRANDA, P. F. M. Vigilância digital como instrumento de promoção de segurança pública. **Revista UEPG**, Ponta Grossa, n. 28, p. 1-14, 2020. Disponível em: https://www.revistas.uepg.br/index.php/sociais/article/view/14435/209209212734. Acesso em: 30 nov. 2021.

SCHWAB, K. **A quarta revolução industrial**. Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016.

SIQUEIRA, D. P.; LARA, F. C. P. Quarta Revolução Industrial, inteligência artificial e a proteção do homem no direito brasileiro. **Revista Meritum**. v. 15, n. 4. p. 300-311, 2020. Disponível em: https://eds.p.ebscohost.com/eds/detail/detail?vid=1&sid=825b5068-aa49-4c35-b34b-541aa4ecacd9%40redis&bdata=Jmxhbmc9cHQtYnImc2l0ZT1lZHMtbGl2ZQ%3d%3d#AN=152543197&db=foh. Acesso em: 04 jan. 2022.

SILVA, T. Racismo Algorítmico em Plataformas Digitais: microagressões e discriminação em código. *In*: _____. (org.). **Comunidades, algoritmos e ativismo digitais**: olhares afrodiaspóricos. São Paulo: Literarua, 2020.

SOLOVE, D. J. **Understanding Privacy**. Cambridge, Havard University Press. 2008.

VIDAL, E. L. **Monitoramento Eletrônico: Aspectos Teóricos e Práticos**. 2014. 106 f. Dissertação (Mestrado) – Universidade Federal da Bahia, Salvador, 2014. Disponível em: https://repositorio.ufba.br/bitstream/ri/17989/1/Disserta%c3%a7%c3%a3o%20final%20-%20Eduarda%20de%20Lima%20Vidal.pdf. Acesso em: 03 abr. 2021.

WERTHEIN, J. A Sociedade da Informação e seus desafios. **Ci. Inf.**, Brasília, v. 29, n. 2, p. 71-77, maio-ago. 2000. Disponível em: https://www.scielo.br/j/ci/a/rmmLFLLbYsjPrkNrbkrK7VF/?format=pdf&lang=pt. Acesso em: 02 fev. 2022.

ZUBOFF, S. Big Brother*:* capitalismo de vigilância e perspectivas para uma civilização de informação. *In*: BRUNO, F. et al. (orgs.). **Tecnologias da vigilância**: perspectivas da margem. Trad. H. M. C. et al. São Paulo: Boitempo, 2018. p. 17-68.