THOMSON REUTERS
REVISTA DOS TRIBUNAIS™

DADOS PESSOAIS NO PROCESSO PENAL: TUTELA DA PERSONALIDADE E DA INOCÊNCIA DIANTE DA TECNOLOGIA

Personal data in criminal proceedings: technology and protection of personality and innocence

Revista Brasileira de Ciências Criminais - RBCCrim
vol. 190 - Maio/2022

Flaviane de Magalhães Barros Bolzan de Morais
Pós-Doutorado (2007) em Direito pela Università degli studi di Roma Tre. Doutorado (2003) e Mestrado (2000) em Direito pela Pontifícia Universidade Católica de Minas Gerais. Pesquisadora CNPq – Produtividade em Pesquisa PQ-2. Representante do Colégio de Humanidades – CAPES (2021). Pesquisadora visitante da Università degli studi di Firenze. Professora da Pontifícia Universidade Católica de Minas Gerais e da Universidade Federal de Ouro Preto.
Lattes: [http://lattes.cnpq.br/1159840059123495].
ORCID: [https://orcid.org/0000-0002-2377-6026].
barros.flaviane@gmail.com

Leonardo Augusto Marinho Marques
Doutorado (2006) e Mestrado (2001) em Direito pela Universidade Federal de Minas Gerais. Professor Associado da Universidade Federal de Minas Gerais e Chefe do Departamento de Direito e Processo Penal da Faculdade de Direito da Universidade Federal de Minas Gerais. Advogado Penalista.
Lattes: [http://lattes.cnpq.br/5388381867392010].
ORCID: [https://orcid.org/0000-0001-9687-8405].
leonardo@leonardomarinho.com.br

Jamilla Monteiro Sarkis
Doutorado em andamento pela Pontifícia Universidade Católica de Minas Gerais, com bolsa concedida pela CAPES. Mestrado (2018) em Direito pela Universidade Federal de Minas Gerais. Coordenadora Adjunta do Instituto Brasileiro de Ciências Criminais em Minas Gerais. Professora da Estácio em Belo Horizonte. Advogada Penalista.
Lattes: [http://lattes.cnpq.br/5388381867392010].
ORCID: [https://orcid.org/0000-0002-2730-5950].
DOI: [https://doi.org/10.54415/rbccrim.v190i190.120].
jamilla.sarkis@gmail.com

Área do Direito: Penal; Digital

Resumo: O presente trabalho busca, a partir de uma perspectiva interdisciplinar, bem como do estudo de um caso referência, analisar garantia da pessoa imputada no processo penal de ter protegidos os seus dados pessoais. Para tanto, trabalha a influência da tecnologia no processo, com especial foco na superexposição de dados pessoais. Além disso, demonstra a possibilidade de coexistência entre a publicidade processual e a proteção de dados pessoais, bem como contextualiza os prejuízos gerados pela superexposição de dados pessoais sobre os direitos fundamentais à presunção de inocência e à personalidade com fundamento no marco teórico do modelo constitucional de processo. Diante disso, estuda também a responsabilidade do Estado na preservação dos dados pessoais de pessoas imputadas a

partir da Lei Geral de Proteção de Dados (LGPD) e do Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal (LGPD Penal), na perspectiva do Estado Democrático de Direito. Ao final, conclui que a Lei Geral de Proteção de Dados e suas sanções se aplica ao poder público, devendo ser objeto de atenção por parte dos órgãos de persecução penal.
Palavras-chave: Dados pessoais da pessoa imputada – Tecnologia – Publicidade – Presunção de inocência – Direitos de personalidade

Abstract: The present work seeks, from an interdisciplinary perspective, as well as from the study of a reference case, to analyze the guarantee of the defendant to have his personal data protected. To do so, it works on the influence of technology in the process, with special focus on the overexposure of personal data. Moreover, it demonstrates the possibility of coexistence between procedural publicity and the protection of personal data, as well as contextualizes the damages generated by the overexposure of personal data on presumption of innocence and personality based on the theoretical framework of the constitutional model of process. In light of this, it also studies the responsibility of the State in the preservation of personal data of accused persons based on the General Law of Data Protection and the Draft Law of Data Protection for Public Security and Criminal Prosecution, from the perspective of the Democratic State of Law. In the end, it concludes that the General Data Protection Law and its sanctions apply to the public authorities and should be the object of attention by criminal prosecution agencies.
Keywords: Defendant's personal data – Technology – Presumption of innocence – Personality rights

Para citar este artigo: Morais, Flaviane de Magalhães Barros Bolzan de; Marques, Leonardo Augusto Marinho; Sarkis, Jamilla Monteiro. Dados pessoais no processo penal: tutela da personalidade e da inocência diante da tecnologia. *Revista Brasileira de Ciências Criminais*. vol. 190. ano 30. p. 117-156. São Paulo: Ed. RT, maio/jun. 2022. DOI:[https://doi.org/10.54415/rbccrim.v190i190.120]. Disponível em: inserir link consultado. Acesso em: DD.MM.AAAA.

Sumário:

1.Introdução - 2.Tecnologia e processo: superexposição de dados - 3.Publicidade processual e superexposição de dados: um conflito aparente - 4.Direitos da pessoa imputada aos seus dados pessoais: reflexos em um modelo constitucional de processo - 5.Responsabilidade do Estado sobre os dados de pessoas imputadas - 6.Conclusão - 7.Referências

1. Introdução

Você já procurou o seu nome no *Google*?

É possível que todos respondam, afirmativamente, a esta pergunta. Também é provável que todos já tenham pesquisado nomes de outras pessoas em algum buscador *on-line*: por motivos pessoais, acadêmicos ou profissionais, ninguém escapa da tarefa de procurar, na *internet*, por dados relacionados a indivíduos que, motivadamente ou por pura curiosidade, nos interessam.

Para alguns, todavia, essa consulta – por decorrência da virada tecnológica e da ampliação do ciberespaço, hoje já faz parte da vida cotidiana – pode apresentar resultados indesejáveis, cujos reflexos sobre a vida privada podem comprometer direitos fundamentais à personalidade e à presunção de inocência.

É o caso das pessoas imputadas no processo penal. Basta *googlar*[1] o nome de alguém que responda criminalmente, por qualquer fato, para que sejam publicizadas informações como o número do processo, a comarca e a vara de origem, as outras partes envolvidas, a imputação em processamento e os andamentos processuais, conforme determina a Resolução 121, de 2010, do Conselho Nacional de Justiça (CNJ).

Se o processo for digital, com tramitação por sistemas eletrônicos como PJe, JPe, Projudi, eProc, e-Saj, Themis e outros[2], as informações disponíveis são ainda mais significativas. Uma consulta detalhada pode revelar a inscrição das pessoas imputadas no Cadastro Nacional de Pessoas Físicas, seu endereço, filiação e outros dados pessoais.

Como notaram Ana Frazão e Luiza Santos (2020, p. 60), esse não é um ônus exclusivo das pessoas imputadas no processo criminal: "algoritmos vêm sendo utilizados para análises complexas, decisões e diagnósticos que, além de representarem uma verdadeira devassa na intimidade das pessoas, terão impactos nas possibilidades e no acesso destas a uma série de direitos e oportunidades." As autoras ressaltam que, na atualidade, algoritmos são responsáveis por decidir "quem terá crédito e a que taxa de juros, quem será contratado para trabalhar em determinada empresa, qual a probabilidade de reincidência de determinado criminoso, quem deve ser atropelado em determinadas situações, entre inúmeras outras circunstâncias".

Na esfera penal, todavia, o impacto é ainda maior. Grande parte dos afetados pela exposição de dados se incluem em um universo de fragilidade e exclusão social, pertencendo a classes econômicas menos favorecidas (BARROS, 2018, p. 08). Para essas pessoas, responder ao processo penal é, por si só, uma pena: a estigmatização impede o exercício de toda sorte de direitos, entre eles, o livre desenvolvimento da personalidade.

Efetivamente, esses prejuízos configuram manifesta violação à presunção de inocência que, como regra de tratamento, se refere à condição da pessoa imputada durante o processo e veda a sua equiparação à pessoa culpada em qualquer aspecto (ILLUMINATI, 1979, p. 29). Qualquer pessoa pode ter acesso a dados pessoais de indivíduos que respondem a processos criminais ainda em curso, tudo isso disponível aos toques do teclado, já que diversos *websites* utilizam algoritmos para coletar, e esses dados em bancos públicos, inclusive os de Tribunais (DEL MASSO; GODOY, 2020, p. 108).

Este procedimento não é novo nem exclusividade de um *website* específico: denomina-se mineração de dados e se caracteriza como um processo de exploração e análise de grande quantidade de dados, a fim de descobrir significativos padrões, regras e relações que interessem às mais variadas áreas do conhecimento (MAIMON; ROKACH, 2010, p. 22).

Na evolução dos sistemas informáticos, de acordo com Éric Sadin (2020, p. 57), a mineração de dados ocupa um lugar perturbador, tendo em vista a capacidade de revelar fenômenos que sequer são perceptíveis pela consciência humana, capaz de colocar os computadores em posição de superioridade para a avaliação de determinado conjunto de fatos – por exemplo, a viabilidade da contratação de determinado indivíduo com base nos resultados apresentados pelo *Google* mediante a inserção de seu nome no buscador.

Com efeito, a Lei Geral de Proteção de Dados (LGPD – Lei 13.709/2018) determina, em seu artigo 1º, que todos os dados pessoais – isto é, informações relacionadas a pessoas naturais identificadas ou identificáveis (artigo 5º, I) – devem ser objeto de proteção por pessoa natural ou por pessoa jurídica de direito público ou privado. A finalidade dessa proteção, conforme dispõe a Lei, é garantir os direitos fundamentais de liberdade e de personalidade e o livre desenvolvimento da personalidade da pessoa natural. Da mesma forma, o Marco Civil da Internet (Lei 12.965/2014) traz, em seus artigos 7º e 8º, a privacidade e proteção da intimidade como direito básico de qualquer cidadão, seguindo o que preceitua o artigo 5º, inciso X, da Constituição da República de 1988.

Em matéria penal, todavia, a proteção de dados ainda é matéria controversa, cuja necessidade de regulamentação deu origem à Comissão de Juristas criada pela Câmara dos Deputados para propor o projeto de "Lei de Proteção de Dados para Segurança Pública e Persecução Penal", apresentado em junho de 2020. Com enfoque nos dados pessoais utilizados para atividades de segurança pública e de persecução penal, a proposta não contempla a proteção às informações pessoais daqueles que já respondem a

processos criminais e, por isso, têm seus dados pessoais expostos na rede mundial de computadores.

Partindo dessas premissas, o presente trabalho busca desenvolver a hipótese de que, no processo penal, embora relevante a publicidade dos atos, a pessoa imputada deve ter garantido o sigilo de seus dados pessoais, visto que a salvaguarda dos seus direitos à personalidade e à presunção de inocência deve ser tutelada pelo Estado.

Nesse sentido, a pesquisa irá, inicialmente, trabalhar a influência da tecnologia no processo, com especial foco na superexposição de dados pessoais. Em seguida, será demonstrada a possibilidade de coexistência entre a publicidade processual e a proteção de dados pessoais, bem como contextualizados os prejuízos gerados pela superexposição de dados pessoais sobre os direitos fundamentais à presunção de inocência e à personalidade. Feita essa digressão, a responsabilidade do Estado na tutela dos dados pessoais de pessoas imputadas será estudada a partir da Lei Geral de Proteção de Dados (LGPD) e do Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal (LGPD Penal), na perspectiva do Estado Democrático de Direito.

Para tanto, serão empregadas duas diferentes estratégias metodológicas. A primeira delas se fundamenta na necessidade de compor – diante da interdisciplinaridade que permeia o trabalho – um sistema de conceitos analíticos que servirá como base de referências conceituais, a partir do estudo de doutrinas e legislações e sob o marco teórico do modelo constitucional de processo. O marco é suficiente e necessário para assegurar que a base principiológica que sustenta a compreensão do processo no Estado Democrático de Direito deve possuir capacidade de se aperfeiçoar por meio do esforço argumentativo, em virtude da perfectibilidade defendida por Italo Andolina e Giuseppe Vignera (1997). Assim, tendo em vista que o microssistema, no processo penal, se sustenta especialmente pela existência do princípio regente e condutor da presunção de inocência, exige-se que os demais princípios o considerem quando se trata da atuação jurisdicional perante o processo penal (BARROS, 2018).

Cumpre destacar que o trabalho não tem a pretensão de promover uma revisão bibliográfica sobre presunção de inocência ou proteção de dados, nem mesmo de esgotar os conhecimentos e saberes em análise, sendo todo o arcabouço teórico lançado a título do esforço argumentativo de discutir a questão problema da pesquisa sob o marco escolhido, ancorada na interdisciplinaridade como metodologia regente que busca construir pontes entre saberes.

A segunda estratégia, consolidada com base em uma metodologia prática, será promovida a partir do estudo de caso referência[3]. Tal método se diferencia do estudo de caso, na medida em que é utilizado como base fática para toda a pesquisa teórica a ser desenvolvida, estando seus elementos presentes em todas as etapas do trabalho e fundamentais para a comprovação da hipótese analisada.

Ao final, espera-se evidenciar que o acesso aos dados pessoais, mesmo diante do princípio da publicidade processual, viola a personalidade e a presunção de inocência das pessoas imputadas, motivo pelo qual sua proteção por parte dos órgãos jurisdicionais deve ser objeto de salvaguarda jurídica e tratamento técnico diferenciado.

2.Tecnologia e processo: superexposição de dados

Ao longo das últimas décadas, o sistema jurídico sofreu importantes rupturas pragmáticas. Foram introduzidas significativas mudanças nos fundamentos e propósitos de atuação das instituições a partir de sua introdução ao ciberespaço (LESSIG, 2009, p. 09), quando informações reais assumiram formas intangíveis e passaram a ser acessadas, democraticamente, por qualquer pessoa em qualquer lugar do mundo.

Os impactos desse movimento, conhecido como virada tecnológica, conforme identifica Dierle Nunes (2020,

p. 15-17), transcendem sua mera aplicação instrumental. Impactam, de maneira concreta, o campo processual, seja pela mudança dos institutos jurídicos desde seu âmbito propedêutico, seja pelo dimensionamento de uma nova racionalidade para sua implementação, seja pela criação de novos institutos.

Efetivamente, a virada tecnológica não guarda relação exclusiva com a informatização judicial – como o processo eletrônico – ou com o emprego de tecnologias no exercício das mais diversas carreiras jurídicas – por exemplo, o fluxo de comunicação via e-mail ou aplicativos de comunicação. Nas últimas décadas, como pontuam Orna Rabinovich-Einy e Ethan Katsh (2017, p. 14), o esgotamento dos modelos tradicionais de justiça, causados pela redução de recursos financeiros e pela estrutura física que os definem – necessidade de encontros pessoais, com juízes, promotores e advogado – demandaram avanços tecnológicos capazes de lidar ou de reduzir a litigiosidade, além de melhorar, refinar, agilizar, otimizar e turbinar as atividades forenses (SUSSKIND, 2019, p. 34).

Diante da complexa relação entre direito e tecnologia e suas várias interseções é que Antoine Garapon e Jean Lassègue (p. 13, 2018) estabelecem três dimensões da revolução jurídico-digital: a revolução simbólica, com reflexo não apenas no direito, mas na própria elaboração da lei; a revolução gráfica, responsável pelas mudanças no discurso e no silogismo jurídicos, que podem não deixar de ser escritos, mas certamente precisarão de outras ferramentas comunicativas; a revolução política, consistente na substituição do elemento humano pelas estruturas automatizadas em várias circunstâncias, inclusive de cunho decisório.

Das diversas tecnologias aplicáveis ao direito, a Inteligência Artificial (IA) se destaca na medida em que permite a parametrização, o tratamento e a estocagem de uma grande massa de dados (big data). Na definição de Ben Coppin (2013, p. 5), a IA consiste no "estudo dos sistemas que agem de um modo que a um observador qualquer parece ser inteligente", apresentando "uma capacidade de lidar com novas situações; a capacidade de solucionar problemas, responder a questões, de engendrar planos" que se assemelha ao pensamento e consciência humanos. Jerry Kaplan (2016, p. 5), por seu turno, define a IA como uma habilidade, no sentido de possibilitar generalizações apropriadas e oportunas a partir de dados limitados.

Para Dierle Nunes, a Inteligência Artificial possibilita uma revolução nos institutos jurídicos; mas, ao mesmo tempo que inova ao gerar eficiência para a atuação nas profissões jurídicas, acarreta riscos "de generalizações equivocadas, opacidade (não compreensão de como se chegou aos resultados), geração de preconceitos e discriminação" (NUNES, 2020, p. 21).

Tais consequências, nas palavras de José Luís Bolzan e Flaviane Barros (2020, p. 267), impactam os direitos fundamentais, que se perdem ou se relativizam quando postos lado a lado com as facilidades que são fruto da tecnologia e monetarização de alguns serviços ofertados por empresas (startups) voltadas ao dimensionamento das questões jurídicas) como as Legaltechs ou Lawtechs.

De acordo com a Associação Brasileira de Lawtechs e Legaltechs, as empresas brasileiras voltadas a produtos e serviços de inovação para a área jurídica podem ser divididas em 13 categorias: Analytics e Jurimetria, Automação e Gestão de Documentos, Compliance, Conteúdo Jurídico, Educação e Consultoria, Extração e Monitoramento de Dados Públicos, Gestão – Escritórios e Departamentos Jurídicos, IA – Setor Público, Redes de Profissionais, RegTech, Resolução de Conflitos on-line, TaxTech, Civic Tech e Real EstateTech4. Especificamente naquilo que se refere às Lawtechs e Legaltechs, voltadas à extração e ao monitoramento de -dados públicos, sua atuação tem como bases a coleta e a compilação de todos os atos oficiais administrativos e judiciais praticados no país.

Para ilustrar o problema a partir de um caso referência, promoveu-se a busca por nome aleatório e genérico, composto por prenome e sobrenome que figuram entre os mais comuns do Brasil5, no Google – que encontrou, em cerca de 20 segundos, mais de 4.100.000 de resultados. O primeiro link sugerido pelo buscador foi direcionado ao websiteJusBrasil, em razão de sua utilidade e relevância6.

Conforme se extrai na Política de Privacidade da Plataforma, dados pessoais são extraídos pelo JusBrasil, de forma automatizada7, a partir de "fontes publicamente disponíveis, como diários oficiais, dados oriundos de tribunais referentes a processos, informações de salas de imprensa de órgãos públicos, e legislação", com o objetivo de "ampliar o acesso a esse conteúdo por parte dos seus Usuários"8.

Ainda de acordo com as informações obtidas no próprio portal JusBrasil, a plataforma não atua na criação ou desenvolvimento de dados. Seus serviços se voltam, exclusivamente, na captação de dados que estão disponíveis em bases públicas de consulta, como os websites dos Tribunais de Justiça de cada estado, dos Tribunais Regionais Federais, do Superior Tribunal de Justiça e do Supremo Tribunal Federal:

"Vale ressaltar que o JusBrasil age apenas como ferramenta de busca e não cria, edita ou altera informações pessoais exibidas. Todo o processo de coleta de dados cujo resultado culmina nas informações disponibilizadas é realizado automaticamente, através de fontes públicas pela Lei de Acesso à Informação. Além do que, importante ressaltar que a Constituição Federal assegura o direito de acesso à justiça para todos, inclusive com relação à publicidade dos atos processuais (art. 5º, LX). A publicidade dos atos processuais também está consagrada no Código de Processo Civil brasileiro em seu artigo 189."9

Na Política de Privacidade da Plataforma, o portal JusBrasil chega a reconhecer que, durante o processo de extração automatizada de dados públicos, é possível a obtenção de "eventuais dados sensíveis", cujo tratamento deverá pressupor a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização:

"Dados pessoais cujo acesso é público, ou que foram tornados manifestamente públicos pelo seu titular, incluindo eventuais dados sensíveis constantes desses documentos e conteúdos de acesso público (tais quais definidos pela legislação brasileira, como aqueles que revelem orientação religiosa, política ou sexual, convicção filosófica, participação em movimentos políticos ou sociais, informações de saúde ou genéticas), ressaltando que o tratamento desses dados deve levar em consideração a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização."10

A LegalTech, porém, fundamenta suas atividades na importância da publicidade processual, na relevância da transparência das atividades públicas e na democratização do acesso à informação, ressaltando que possui canais abertos aos usuários para que reportem, por iniciativa própria, a necessidade de remoção de determinados conteúdos:

"Com o propósito de facilitar o acesso à justiça por meio da informação, o Jusbrasil disponibiliza uma plataforma de busca que visa fornecer ferramentas para auxiliar e dinamizar o dia a dia dos operadores do direito, bem como democratizar a busca por conteúdo jurídico pelo público em geral, sempre em busca de conectar as pessoas à justiça e potencializar a efetivação do direito à informação. Neste contexto, reproduzimos e organizamos as informações disponibilizadas pelos órgãos públicos nos seus respectivos sites, como diários oficiais e decisões judiciais, servindo meramente como um indexador de conteúdo. Ocorre que a Constituição Federal garante, em seus arts. 5º, LX, 37 e 93, a publicidade dos atos processuais como regra. Diante do passado ditatorial do Brasil, temos que este é um importante instrumento para a manutenção da democracia. Além disso, todo o sistema normativo, com destaque para a Lei Geral de Proteção de Dados, o Marco Civil da Internet e a Lei de Acesso à Informação, partilha da mesma racionalidade: o tratamento de dados pessoais é instrumental ao princípio constitucional da publicidade da Administração Pública.

[...] Por óbvio, encontramos alguns desafios neste caminho, como a necessidade de compatibilizar o direito à informação, do princípio da publicidade dos atos processuais e o direito à proteção de dados e de desenvolver mecanismos para garantir a proteção dos direitos individuais. No entanto, enquanto mero indexador de informações já disponíveis na internet, resta ao Jusbrasil acompanhar as movimentações dos órgãos públicos neste sentido, sobretudo da Autoridade Nacional de Proteção de Dados, para que realize

futuras adequações que se verifiquem necessárias. Por sua vez, o Jusbrasil está constantemente refletindo e adotando medidas para a proteção da privacidade de indivíduos e para mitigar eventuais riscos, o que demonstra sua boa-fé e proatividade na proteção de dados pessoais de cidadãos. Adotamos, por exemplo, uma política amigável de remoção de conteúdo, a qual determina a remoção completa de informações relacionadas a processos em segredo de justiça, pedidos de remoção feitos pelo Poder Judiciário (como ofício ou decisão judicial) e processos envolvendo menores de idade atualmente e/ou à época do processo. Ainda, disponibilizamos uma ferramenta pela qual o próprio usuário pode reportar uma solicitação de remoção de conteúdo, sem necessidade de entrar em contato conosco. No mais, estamos sempre buscando o estado da arte na tecnologia, a fim de garantir que as informações disponibilizadas na plataforma sejam as mais completas e fidedignas possíveis."11

Depois do direcionamento da pesquisa feita no Google ao JusBrasil, selecionou-se um dos mais de 8.000 processos vinculados ao nome escolhido e boa parte de suas informações passou a ser exibida12. Tratava-se de processo penal relacionado a crimes de trânsito em trâmite perante o Tribunal de Justiça do Estado de São Paulo:

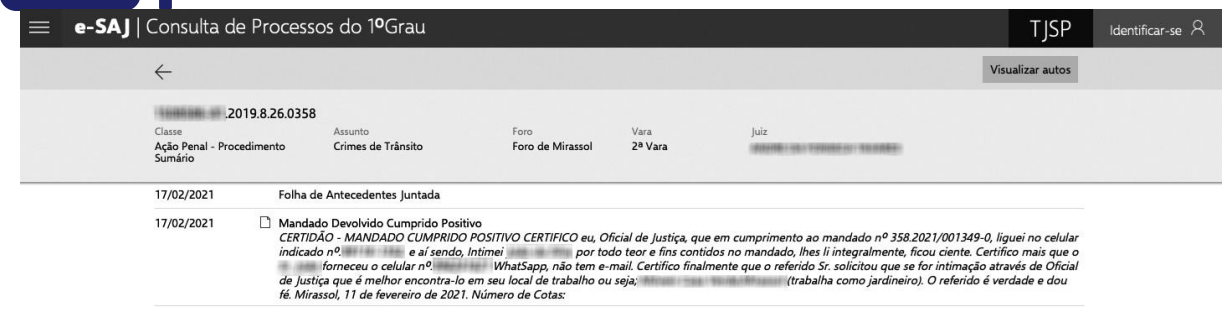
Figura 1 – Consulta a um dos resultados apresentados pelo JusBrasil posteriormente à busca pelo nome escolhido

Fonte: elaborada pelos autores a partir do *website* da *JusBrasil*.

Portanto, o que se verifica é que, ao consultar um nome no Google ou em outros buscadores populares disponíveis na internet, dados pessoais, inclusive relacionados em processos criminais, podem ser facilmente localizados. Em questão de segundos, é possível saber se uma pessoa responde por algum crime, qual a fase do processo, se houve condenação ou absolvição, qual a pena a ser cumprida etc.

Ainda, com base no caso referência, veja-se que bastou inserir na consulta pública do website do Tribunal de Justiça do Estado de São Paulo o número do processo disponibilizado pelo JusBrasil, para encontrar dados pessoais da pessoa imputada, entre os quais seu número de telefone e endereço profissional13:

Figura 2 – Consulta do processo criminal ao qual responde a pessoa de nome escolhido na consulta pública do Tribunal de Justiça de São Paulo



Fonte: elaborada pelos autores a partir do *website* do Tribunal de Justiça de São Paulo.

A partir da situação exposta, constata-se que o JusBrasil, assim como outras empresas de tecnologia voltadas para práticas de inovação e tecnologia jurídicas, atua como uma ferramenta de compilação e exibição de dados que, por sua vez, são disponibilizados por órgãos jurisdicionais. Assim, o centro do problema não parece estar apenas na atuação dessa espécie de LegalTech, mas também na disponibilização, por parte dos órgãos jurisdicionais, de dados sensíveis ao indivíduo – como são as informações pessoais – e com grande potencial de violação a direitos fundamentais. Certamente, a LegalTech estuda possui uma análise de risco legal da sua atividade econômica e assim mantém tranquila a usar dados e potencializar sua exposição, mas tal análise não será aqui pormenorizada porque foge do foco da pesquisa, pois discutiria a questão sob o enfoque no âmbito do direito privado. O objetivo foco da pesquisa é evidenciar que os dados partem e são alimentados pelo Estado Jurisdição.

Se parte, do próprio Estado, a atividade de superexposição dos dados pessoais, a qual se vê potencializada pela atividade de Legaltechs como a JusBrasil, resta compreender se a publicidade processual poderia, legitimamente, justificá-la. Afinal, para publicizar os atos processuais e promover o acesso democrático à informação e à justiça, é necessário violar direitos fundamentais?

3.Publicidade processual e superexposição de dados: um conflito aparente

Para o processo, o princípio da publicidade tem como objetivo a transparência sobre como o poder público trata questões de interesse social. O Conselho Nacional de Justiça, por meio da Resolução 121, de 2010, garante as consultas públicas dos sistemas de tramitação e acompanhamento processual dos Tribunais e Conselhos, disponíveis na rede mundial de computadores, inclusive em processos criminais:

"Art. 1º A consulta aos dados básicos dos processos judiciais será disponibilizada na rede mundial de computadores (internet), assegurado o direito de acesso a informações processuais a toda e qualquer pessoa, independentemente de prévio cadastramento ou de demonstração de interesse.

Art. 2º Os dados básicos do processo de livre acesso são:

I – número, classe e assuntos do processo;

II – nome das partes e de seus advogados;

III – movimentação processual;

IV – inteiro teor das decisões, sentenças, votos e acórdãos."

As exceções se restringem às hipóteses nas quais (i) o processo é sigiloso ou está em segredo de justiça; (ii) o processo teve sentença absolutória já transitada em julgado; (iii) foi declarada a extinção de punibilidade do agente; (iv) foi cumprida, em sua integralidade, a pena. Nesses casos, o nome das pessoas imputadas deixa de aparecer por extenso na consulta púbica, permanecendo o registro apenas das suas iniciais14.

De fato, a realização pública de julgamentos constitui um importante elemento da estrutura republicana e

democrática do processo penal. Trata-se de verdadeira manifestação contrária à inquisitoriedade (CORDERO, 1986, p. 73), cujas características pairam pela órbita da opacidade dos julgamentos e do afastamento da jurisdição em relação aos cidadãos.

Conforme explica Alberto Binder (2000, p. 68), a publicidade figura entre as garantias básicas previstas no artigo 8º da Convenção Americana de Direitos Humanos. Para o autor, a publicidade exerce, na processualidade penal, duas funções: primeiro, dada a especificidade da justiça criminal, serve para transmitir a ideia de respeito à vigência dos valores que embasam a convivência social, o que se faz por meio da cominação de penas (prevenção geral) e da aplicação concreta de sanções (BINDER, 2000, p. 69); em segundo lugar, a publicidade exerce o papel de assegurar o controle popular sobre a administração da justiça (BINDER, 2000, p. 70), a fim de diminuir o abismo que existe entre a vida social e administração da justiça. A ideia da publicidade, portanto, se satisfaria pelo conceito de "julgamentos a portas abertas", a partir dos quais os juízes ditariam as sentenças "frente a frente com o povo" (BINDER, 2000, p. 70).

Contudo, essa visão, apesar de bem-intencionada, acaba dando espaço à chamada "imprensa marrom", que toma para si a função de controle popular das causas – especialmente as criminais – e se converte em poderoso meio de manipulação da opinião pública e opressão em desfavor das pessoas imputadas, conforme aponta Simone Schreiber (2008).

E, se, na era analógica, determinados casos precisavam cair no interesse popular para serem objeto de cobertura midiática espetacularizada (CASARA, 2018) – seja porque envolviam pessoas famosas, personalidades políticas ou crimes de intensa reprovabilidade como filicídio, parricídio ou matricídio15 – na era digital, esse acompanhamento em live streaming de casos criminais foi potencializado.

No YouTube, plataforma de compartilhamento de vídeos mais popular do mundo, existem canais dedicados à transmissão ao vivo de sessões do Tribunal do Júri e acompanhamento de operações policiais; no Reddit, um agregador social de notícias equipado com fórum de discussões on-line, existem milhares de tópicos relacionados à discussão sobre crimes reais, nos quais os usuários passam a se comportar como verdadeiros detetives16.

Sobre a forma como a era digital influencia a publicidade de casos criminais, escreve Tanya Horeck (2019, p. 19):

"No Facebook as pessoas compartilham filmagens de circuito interno de câmeras com criminosos roubando lojas locais ou informações sobre jovens desaparecidos, com o espírito de serem bons samaritanos. Os departamentos de polícia postam fotos de pessoas detidas nas suas páginas do Facebook, nas quais as pessoas são capazes de responder com emojis e comentários. No Twitter as pessoas emitem os seus julgamentos pessoais sobre crimes e criminosos e acompanham os repórteres do tribunal eles postam sobre casos criminais, como relata um repórter do tribunal: 'Tenho sido seguido por juízes e promotores e recebo bastante feedback de agentes da polícia. Eu postei a foto de um acusado não compareceu ao tribunal e um agente de polícia o prendeu depois de tê-lo visto - isso já aconteceu algumas vezes.'"17

Com efeito, a partir do atual nível de interesse e na facilidade do acesso às informações sobre casos criminais em curso, impor limites à transparência e à publicidade em face dos direitos fundamentais é necessário. Em tempos de inteligência artificial e mineração de dados, cabe ao Estado limitar o que é divulgado, assegurando os direitos à intimidade, vida privada, honra e imagem da pessoa, em especial da pessoa imputada que ainda não foi submetida a julgamento e, portanto, deve ser presumida inocente.

Da mesma forma, a publicidade não pode ser subterfúgio para a mercantilização das informações pessoais no mercado das Legaltechs. Nesse sentido, a socióloga Sarah Lageson (2019, p. 395) explica como os dados pessoais publicados pelos Tribunais dos Estados Unidos passaram a ser utilizadas para outros fins, que não a mera transparência e publicidade dos atos processuais.

De acordo com a autora, as empresas passaram a reunir registros públicos, geralmente por meio de atacadistas que compram dados diretamente de agências governamentais e, em seguida, os vendem para outras empresas que buscam verificar os antecedentes criminais de seus clientes ou até mesmo para websites que monetarizam a divulgação de fotografias das pessoas presas, as chamadas mugshots. Nesse ponto, Lageson esclarece que a utilização dos dados pessoais disponibilizados pelos Tribunais também pode servir para outras finalidades mercantis, como a busca por potenciais clientes, devassa indevida da vida alheia e até mesmo extorsões e fraudes.

E as informações relacionadas também têm potencial para elaborar análises preditivas sobre o comportamento de determinado órgão judicial: a partir dos dados coletados, pesquisadores podem encontrar padrões de acusação, fiança e resultados da sentença, especialmente se os dados fornecem informações demográficas sobre os réus. Lageson ressalta, ainda, que os registros obtidos nos Tribunais também oferecem uma excelente fonte de triangulação de dados: "se esses dados contiverem identificadores pessoais, como nome e data de nascimento, os pesquisadores podem recorrer aos registros judiciais online para se aprofundar na mecânica de um caso criminal", ou seja, "esclarecer itens em um conjunto de dados agregado que não são claros para pesquisadores não familiarizados com a terminologia ou decisões de codificação de uma agência de justiça criminal" -(LAGESON, 2019, p. 397)18.

Para além da predição de dados relacionados ao comportamento das agências públicas de justiça criminal, a mineração de informações disponíveis em bancos de dados públicos possibilita a análise preditiva do comportamento de indivíduos potencialmente criminosos (EGBERT; LEESE, 2021), ao melhor (ou pior) estilo Minority Report.

Nesse sentido, cita-se estudo que, mediante acesso aos bancos de dados das cidades de São Francisco, Chicago e Filadélfia (FENG; ZHENG; HAN; REN; LIU, 2018) que explorou uma série cronológica de dados a fim de prever tendências de criminalidade para os anos seguintes, com projeções até mesmo sobre as espécies delituosas que seriam praticadas em determinados períodos do ano e em pontos específicos de cada cidade. A partir de técnicas de mineração de dados de última geração, os resultados experimentais demonstraram que os modelos de prevenção criminal propostos pelos autores são viáveis e capazes de contribuir com os departamentos de polícia locais para acelerar processos de prevenção e resolução de crimes. O custo, porém, é alto: pessoas que sequer praticaram delitos passam a ser consideradas criminosas em potencial em razão do local onde residem, dos produtos que consomem, dos seus hábitos pessoais e outras informações que podem ser obtidas pela análise de dados pessoais.

Outra possibilidade mercadológica é mineração de dados para a venda de produtos direcionada a determinados perfis de consumidores (LINOFF; BERRY, 2011, p. 27). Seguindo o caso referência mencionado no item anterior, imagine que uma empresa seguradora de veículos que, com o objetivo de potencializar seus negócios, desenvolva um algoritmo19 capaz de identificar pessoas envolvidas em acidentes de veículos. Pessoas que respondem criminalmente por condutas praticadas no trânsito seriam os alvos perfeitos dessa espécie de publicidade: seus endereços e telefones estariam à disposição de canais de publicidade e marketing, graças ao acesso aos mandados de citação e intimação cujo acesso é franqueado ao público pelo website do Tribunal de Justiça do estado no qual tramita a ação penal.

O que se verifica, portanto, é que a publicização de dados pessoais da pessoa imputada ultrapassa os limites da publicidade processual. Para além de alimentar a curiosidade e a cultura popular que fazem do crime uma forma de entretenimento, a divulgação do endereço ou do telefone de quem responde, criminalmente, a um processo em nada contribui para que a população possa exercer seu direito de acompanhar ou se aproximar da administração da justiça.

Por outro lado, impede que a pessoa imputada possa escolher o que fazer ou não fazer com suas informações pessoais, tendo maculados seus direitos da personalidade antes mesmo de ser submetido a

julgamento – circunstância que representa, igualmente, uma violação à presunção de inocência.

É como se o fato de ser processada criminalmente, portanto, retirasse da pessoa o direito à autodeterminação informativa20, isto é, sua liberdade de dispor de suas informações pessoais, consoante seu próprio interesse (DONEDA, 2011, p. 91). Há flagrante restrição de liberdade – ainda que não manifestada fisicamente – sobre a pessoa imputada antes mesmo do trânsito em julgado da ação penal.

Assim, apesar de a Resolução do Conselho Nacional de Justiça indicar a forma como o como Estado deve gerir os dados da pessoa imputada, a sua inaplicabilidade prática (demonstrada pelo caso referência) conflita com a presunção de inocência e com os direitos de personalidade, assegurados pela Constituição da República de 1988 e impreteríveis no contexto democrático. A seguir, a importância destes direitos será analisada, na perspectiva interdisciplinar da proteção de dados pessoais e com base no marco teórico do modelo constitucional de processo.

4.Direitos da pessoa imputada aos seus dados pessoais: reflexos em um modelo constitucional de processo

Tradicionalmente, o processo penal lida com a dificuldade de reconhecer, na pessoa imputada, um sujeito de direitos. De acordo com a Exposição de Motivos do Código de Processo Penal21, escrita por Francisco Campos em 1941, seria injustificável a primazia do interesse do indivíduo sobre o da tutela social.

A tônica da lei processual vigente, portanto, é de impedir que o indivíduo, "principalmente quando vem de se mostrar rebelde à disciplina jurídico-penal da vida em sociedade", possa "invocar, em face do Estado, outras franquias ou imunidades além daquelas que o assegurem contra o exercício do poder público fora da medida reclamada pelo interesse social" (CAMPOS, 1941, item II).

Pela redação original do Código de Processo Penal do Estado Novo, a pessoa imputada gozava de um único direito: ser representado por defensor. O julgamento parecia depender apenas do cumprimento da rotina burocrática. Presente o réu, devidamente identificado e acompanhado do defensor, a máquina punitivista entrava em ação. A pessoa imputada, nessa ótica, era tão somente o objeto da punição.

Essa realidade somente se viu alterada pela Constituição da República de 1988, quando o Estado Democrático de Direito foi consagrado e passou a garantir, entre outros, os direitos fundamentais à presunção de inocência e da personalidade. A estrutura da Constituição, em relação às garantias processuais, conforme escreve Flaviane Barros (2018, p. 7), estabelece uma base de princípios que se constituem como o modelo constitucional de processo22, a partir do qual se considera a existência de uma base principiológica uníssona, mas que não desconsidera as especificidades dos diversos microssistemas processuais, em razão da codependência entre garantia do processo e direitos fundamentais.

Entre as especificidades do processo penal, duas delas serão objeto de análise na presente pesquisa. Pela ótica do modelo constitucional de processo, a pessoa imputada é sujeito de direitos fundamentais e o microssistema do processo penal quando a inclui por meio da imputação penal deve constituir toda sua estrutura processual tendo, para além da base uníssona formada pelo contraditório, ampla defesa como ampla argumentação, imparcialidade e fundamentação da decisão, também pelo princípio regente do processo penal que é a presunção de inocência. A presunção de inocência é que dá contornos específicos e próprios ao microssistema do processo penal. Por essa feita é que a discussão do caso referência pode ter respostas diversas em outro microssistema processual. É ela que vai exigir que se faça uma leitura do direito da personalidade, cujos reflexos incidem diretamente sobre a matéria dos dados pessoais no âmbito do sistema de justiça criminal de forma diversa e com maior valor para salvaguarda dos direitos das pessoas imputadas.

4.1.Reflexos da superexposição de dados pessoais na presunção de inocência

A presunção de inocência, direito disciplinador do processo penal (BARROS, 2018, p. 11) está disposta no artigo 5º, LVII, da Constituição de 1988, e na Convenção Americana sobre Direitos Humanos23. Em ambos os textos, a expressão "presunção de inocência", foi adotada como forma de superar a noção positivo-fascista que cunhou o termo "não culpabilidade". Sobre a diferença relevante entre os vocábulos, explica Maurício Zanoide de Moraes (2010, p. 215):

"[...] a noção de 'não consideração prévia de culpabilidade' foi uma criação positivista do fascismo habilmente elaborada a fim de que, por meio de um ataque técnico-jurídico sobre a palavra 'presunção', se atingisse a palavra 'inocência'. Afirmava-se, à época, que se não se pode dizer que o imputado seja culpado no início da persecução penal, também não se pode afirmar seja ele inocente. Portanto, concluía-se melhor afirmá-lo 'não culpado'; jamais inocente."

Como direito fundamental, a presunção de inocência determina três principais consequências: como regra de tratamento – considerar a pessoa imputada inocente até o trânsito em julgado; como regra probatória – considerar a pessoa imputada inocente até que se prove o contrário; e como regra de juízo – considerar a pessoa imputada inocente se não houver prova do contrário24. A partir dessa tríade de aspectos, a presunção de inocência deixa de ser apenas um princípio do processo para tornar-se o próprio processo, constituindo "uma proibição de desautorização ao processo" e seus efeitos sobre a pessoa imputada (GÓMEZ-TRELLES, 2012, p. 37).

Especificamente naquilo que se refere à regra de tratamento, a presunção de inocência "se refere à condição do imputado durante o processo", de modo que "é vedada qualquer forma de equiparação da pessoa imputada à pessoa culpada em qualquer aspecto", sendo também proibida a "execução provisória da sentença condenatória e qualquer antecipação da pena" (ILLUMINATI, 1979, p. 29-30).

Assim, na contemporaneidade, a pessoa imputada tem o direito fundamental de ser considerada inocente durante a tramitação do processo. Até que haja decisão condenatória definitiva, deve poder se valer de todas os direitos atinentes à sua personalidade porque, como norma de tratamento constitucional a presunção de inocência impõe – a todos que atuem na persecução penal – a preservação dos direitos da pessoa imputada à imagem, honra, vida privada e intimidade (CASTILLO, 1992, p. 510).

As exceções, como a violação da privacidade e da intimidade ou do domicílio e da correspondência, somente têm espaço quando amparadas por decisões judiciais fundamentadas: busca e apreensão, interceptações telefônicas e telemáticas são algumas das hipóteses em que a violação aos direitos individuais é permitida, excepcionalmente, pelo ordenamento jurídico como forma de obtenção de provas capazes de influenciar na apuração e no processamento do fato criminal. Assim dispõe, nesse tema, Zanoide de Moraes (2010, p. 371):

"[...] a estrutura constitucional da presunção de inocência não significa que a pessoa não possa sofrer restrições à sua liberdade [sendo que] essas restrições devem ser elaboradas e aplicadas de modo proporcional e com justificação constitucional. Em outras palavras: o direito constitucional da presunção de inocência exige que suas restrições sejam elaboradas, interpretadas e aplicadas de modo restrito e rigoroso porquanto se está no campo excepcional da redução no âmbito de proteção de um direito fundamental. Se a sua redução é inevitável em um sistema de princípios interdependentes, ela deve sempre ocorrer da menor forma possível."

Além do direito de ser considerado inocente até o fim do processo, a presunção de inocência reflete na vedação à antecipação ao cumprimento da pena, seja ela corporal, seja ela social. Sobre o prejuízo social que a presunção de culpabilidade – contrária à presunção de inocência, Jordi Nieva Fenoll (2016) sustenta que, no processo penal, o acusado sempre ocupa a posição mais visível e, ao mesmo tempo, mais adversa.

Para além dessa realidade, o autor (FENOLL, 2016, p. 4) destaca que "o simples fato de apontar uma pessoa como suspeita gera, automaticamente, receios sociais sobre aquele indivíduo"25 e, por isso, é muito difícil

que alguém seja, pela perspectiva popular, considerado presumidamente inocente: "Sempre que aparece uma notícia sobre um suspeito, ou sobre uma simples prisão policial, o público tende sistematicamente a tomar a informação como certa e a considerar a pessoa não como suspeita, mas automaticamente como culpada". Fenoll (2016, p. 5) assevera que isso não acontece apenas com acusações criminais, já que o ser humano tende, por natureza, a acreditar em qualquer rumor negativo sobre uma pessoa; da mesma forma, porém, não ocorre com os rumores positivos, que costumam gerar mais dúvidas que certezas.

No cenário de inserção da sociedade no ciberespaço, o prejuízo social da presunção de culpa é extremamente rigoroso. Se, na tradição inquisitorial, as prisões, mortes e torturas eram executadas e noticiadas na comunidade por meio dos suplícios, antes mesmo que a pessoa imputada tivesse qualquer forma de demonstrar sua inocência, a atualidade revela a face modernizada dessa prática de punição social: a tecnologia permite que, mesmo antes do julgamento, a pessoa imputada seja condenada em rede nacional, rede social ou rede mundial de computadores.

No contexto da atual, cujos marcos são a intangibilidade e alta fluidez informacional, todos se sentem convidados a intervir na realidade político-criminal e a agir como se verdugos tech fossem. Neste ponto, Leonardo Marinho Marques (2019, p. 190) ressalta que a proibição de tratar o imputado como o antigo inimigo ou herege se mostrou insuficiente para tutelar a qualidade de inocência. Hoje, compreende-se que o imputado não pode ser tratado de forma alguma como condenado e reconhece-se que a regra de tratamento produz efeitos internos e externos ao processo.

Nesse sentido, há preocupações objetivas com todos os fatores que remetam à antecipação do juízo de reprovação, mencionados por Nereu Giacomolli (2012, p. 110), como antecedentes criminais, reincidência, uso desnecessário de algemas, exposição de suspeitos, entrevistas coletivas da Polícia e do Ministério Público, divulgação midiática de dados, utilização de uniformes prisionais em audiência etc.

Aqui, pode-se acrescentar a categoria da exposição on-line de dados pessoais. Afinal, quando todos os seus dados pessoais estão disponíveis para quem quiser conhecê-los e utilizá-los, essa punição antecipada se torna ainda mais fácil.

As consequências relacionadas à superexposição dos dados e ao progressivo incremento dos recursos tecnológicos no processo penal repercutem de forma concreta na presunção de inocência das pessoas imputadas, gerando prejuízos profissionais, familiares e nas relações pessoais. Pode-se reportar eliminação precoce em processos seletivos e dificuldade de inserção profissional, fechamento sumário e imotivado de conta bancária ou recusa de crédito por instituições financeiras, dificuldade de renovação de documentos (certidões e passaportes), encerramento de contratos e desligamentos forçados em face das regras de compliance das empresas. Há situações que se estendem, por tempo indeterminado, mesmo depois de uma absolvição. Mas não é somente no âmbito da presunção de inocência que a superexposição de dados pessoais gera prejuízos às pessoas imputadas. Existe uma outra gama de direitos – os da personalidade – que também são garantidos, pela ótica do modelo constitucional de processo, àqueles que respondem por processos criminais e são violados pela superexposição de dados pessoais.

4.2.Reflexos da superexposição de dados pessoais nos direitos da personalidade

Antes mesmo da vigência do texto constitucional democrático, René Ariel Dotti (1980, p. 23) definiu os direitos da personalidade como aqueles que asseguram ao indivíduo o domínio sobre a essência de suas mais importantes características, tais como a imagem, o nome, o domicílio e a correspondência, a honra e a reputação, a integridade física e moral e a vida profissional. Asseverava o autor, ainda na década de 198026, que a informática "criou no homem uma necessidade de reação contra algo de extraordinário que há bem pouco tempo não passaria de ficção, mas que hoje ameaça gravemente o desenvolvimento natural da personalidade (DOTTI, 1980, p. 256).

Conforme explica Anderson Schreiber (2013, p. 05-09), os direitos da personalidade enfrentaram muita resistência ao longo da história; inicialmente, em decorrência do pensamento liberal e, depois, pela falta de consensos e definições sobre suas características. Na experiência jurídica contemporânea, a privacidade, a intimidade, a imagem e a honra ganham protagonismo somente quando reconhecida a importância da dignidade da pessoa humana e consagrado o referido princípio como fundamento máximo da liberdade.

A questão da privacidade ganhou novos contornos, segundo Stefano Rodotà (2008), a partir do momento em que as pessoas e seus corpos foram multiplicados, desterritorializados e desmaterializados: primeiro perderam a unidade, que foi decomposta em órgãos, células, gametas e outras porções que vão além das utilidades estabelecidas pela natureza; em seguida, enfrentaram a crise de sua materialidade quando iniciada a contraposição ao corpo físico do corpo eletrônico.

Hoje, no ciberespaço, os corpos se tornaram um conjunto de dados, um grande sistema de informações. As senhas, imprescindíveis nas relações eletrônicas, impressões digitais, reconhecimento facial, biometria, geometria de mãos e orelhas, forma da íris e retina, traços vocais e faciais, marchas e frequência de digitação: estes e outros elementos marcam a individualidade e compõem a personalidade de cada um, podendo servir para sua identificação (RODOTÀ, 2004, p. 91-93).

Diante disso, nas eras da "automação" e "transformação", não podem restar dúvidas de que os dados pessoais devem integrar o rol dos direitos da personalidade (SARLET; SAAVEDRA, 2020, p. 50), seja em sua dimensão subjetiva, na qual "se decodifica em um conjunto heterogêneo de posições subjetivas de natureza defensiva (negativa), mas também assume a condição de direito a prestações, cujo objeto consiste em uma atuação do estado" (SARLET, 2020, p. 194), seja em sua dimensão objetiva, no sentido de outorgar às normas que preveem direitos subjetivos função autônoma que "desemboca no reconhecimento de conteúdos normativos e, portanto, de funções distintas aos direitos fundamentais mediante a disponibilização de prestações de natureza fática ou normativa" (SARLET, 2020, p. 198).

Embora possam ser definidos como o controle acerca da coleta e utilização das próprias informações pessoais, o protagonismo dos direitos da personalidade na atualidade não pode ser isolado da matéria dos dados pessoais. No âmbito do Supremo Tribunal Federal, o assunto foi objeto de análise por ocasião da declaração de inconstitucionalidade da Medida Provisória 954/2020, que previa o compartilhamento de dados dos usuários de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE) para a produção de estatística oficial durante a pandemia causada pelo vírus SARS-CoV-2. Na ocasião, a Corte decidiu, por maioria, que a proteção de dados pessoais é direito fundamental, traduzido no fundamento da dignidade da pessoa humana e nas garantias de proteção à inviolabilidade da intimidade, à vida privada, à honra e à imagem das pessoas, assim como à autodeterminação informativa e ao sigilo dos dados (MENDES, 2021).

Assim, apesar de a Constituição da República de 1988 não fazer expressa menção à tutela dos dados pessoais – até mesmo por motivos de cunho temporal – é inadequada a sua exclusão do rol de direitos da personalidade. Anderson Schreiber (2013, p. 15) ressalta que a identidade pessoal também não está prevista constitucionalmente como direito da personalidade, ressaltando que "Na falta de explícito reconhecimento legal, é preciso definir se tais manifestações integram ou não a dignidade humana".

Diante da ausência de previsão constitucional, a matéria dos dados pessoais passou a ser regida pela Lei Geral de Proteção de Dados (LGPD – Lei 13.709/2018)27 que, nos termos do artigo 2º que estabelece que a disciplina dos dados pessoais se fundamenta, entre outros, no respeito aos direitos da personalidade. A tutela jurídica desses dados pessoais se justifica diante do desenvolvimento de tecnologias avançadas, capazes de reunir, manipular e compartilhar quantidades massivas de dados capazes de identificar pessoas, categorizá-las de acordo com padrões de consumo ou até mesmo discriminá-las em razão de -determinados estigmas. Itens aparentemente inofensivos, como um número de telefone ou de inscrição no Cadastro

Nacional de Pessoas Físicas, quando reunidos em conjunto, podem gerar efeitos significativos sobre a vida da pessoa exposta – entre eles, a sua categorização ou estigmatização28. São, nessa vertente, as lições de Anderson Schreiber (2013, p. 137):

"Embora a privacidade possa ser definida como o direito ao controle da coleta e da utilização das próprias informações pessoais, sua real importância não pode ser compreendida na observação isolada de cada dado pessoal. A obtenção de um número de telefone ou de um endereço de e-mail, vista de modo fragmentado, pode parecer inofensiva. Reunindo-se, contudo, um conjunto de informações disponíveis sobre certa pessoa, é possível classificar tais informações de acordo com critérios estipulados pelo organizador dos dados para construir "perfis" de consumidores, segurados, empregados, devedores e assim por diante. Tais "perfis" guiam decisões, ações e estratégias de entidades privadas e públicas. Toda a complexidade da pessoa humana, em sua singular individualidade, fica reduzida à inserção em uma ou outra "categoria", como fruto da sua representação virtual a partir de dados coletados de modo autorizado ou não."

Essas tecnologias, como não poderia deixar de ser, deram origem a um grande mercado (SCHWARTZ, 2003, p. 2.056) no qual informações pessoais valem, objetivamente, dinheiro. Muito dinheiro: trata-se de um modelo de negócios altamente rentável, capaz de "prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado" (ZUBOFF, 2018, p. 18).

Quanto mais relevante o dado mercantilizado, maior sua capacidade de monetarização. Exatamente por isso, informações que são capazes de identificar um indivíduo (em inglês, Personally Identifiable Information ou PII) possuem alto valor de mercado e, na mesma proporção, alto potencial de danos aos seus titulares (SCHWARTZ; SOLOVE, 2011, p. 1812). A partir daí, surge um novo estágio da economia capitalista que decorre da lógica atual de acumulação: se antes, desejava-se bens, agora busca-se por dados (SAMPAIO; MENDIETA; FURBINO; -BOCCHINO, 2021, p. 94).

As definições acerca dos dados pessoais e suas características também ficam a cargo da LGPD, já que "o tratamento de dados só poderá[ia] ser realizado se existi[sse] uma base normativa que o autoriz[asse]" (MENDES, 2019, p. 3). Sua grande inovação, de acordo com Laura Mendes e Danilo Doneda (2018, p. 556), "pode ser compreendida na instituição de um modelo ex ante de proteção de dados, baseado no conceito de que não existem mais dados irrelevantes diante do processamento eletrônico e ubíquo de dados na sociedade da informação".

Conforme se extrai do artigo 5º da referida Lei, "dados pessoais" são informações relacionadas a pessoas naturais identificadas ou identificáveis. Além disso, são "dados pessoais sensíveis"29 aqueles que se referem à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculados a uma pessoa natural.

A LGPD traz, ainda, outro importante conceito referente ao tema dos dados pessoais: a definição de quem seriam os seus titulares – verdadeiro objeto de proteção (MENDES, 2020, p. 134) e foco da norma (FRAZÃO; OLIVA; -ABILIO, 2019, p. 680). Assim, o mesmo artigo 5º, a titularidade dos dados pessoais é conferida às pessoas naturais a quem se referem as informações que são objeto de tratamento.

No processo penal, portanto, as pessoas imputadas têm direito à proteção de seus dados pessoais. Se, por séculos, lhes foi negado todo e qualquer direito individual, a vigência da Constituição da República de 1988 e os tratados internacionais de direitos humanos mudaram o cenário: não se pode admitir a afetação dos direitos da personalidade antes do trânsito em julgado da condenação.

Mesmo que existam exceções às regras que protegem a privacidade, o domicílio e as comunicações, a pessoa imputada continua sendo titular de seu nome, seu endereço, sua filiação, seus registros etc. O fato de responder criminalmente não retira do indivíduo sua condição de pessoa, muito menos de sujeito de

direitos.

Com efeito, a titularidade dos dados pessoais não pode ser confundida com a gestão exercida sobre essas informações. Apesar de os dados pessoais das pessoas imputadas lhes pertencerem, sua utilização continua necessária no processo – os dados pertencem à pessoa, e não ao processo, mas nele existem e coexistem com outras informações. Mas, afinal, a quem cabe a proteção dos dados de pessoas imputadas que estão relacionados no processo criminal? É a esta pergunta que o próximo tópico buscará responder, com base na Lei Geral de Proteção de Dados (LGPD) e no Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal, apresentado à Câmara dos Deputados pela Comissão de Juristas presidida pelo Ministro do Superior Tribunal de Justiça Nefi Cordeiro.

5.Responsabilidade do Estado sobre os dados de pessoas imputadas

Os dados pessoais, diante da tutela constitucional aos direitos de personalidade, demandam maior atenção por parte do Estado. Quando postos em conflito com outros interesses, também devem prevalecer: é o caso da Lei de Acesso à Informação que, como exceção à transparência intrínseca às democracias (BLUM; LÓPEZ, 2020, p. 173), atribui aos órgãos e às entidades do poder público, observadas as normas e os procedimentos específicos aplicáveis, assegurar a proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso (artigo 6º, III, da Lei 12.527/2011).

Seguindo essa mesma premissa, o artigo 23 da LGPD ressalva que o tratamento de dados pessoais pelas pessoas jurídicas de direito público deverá ser realizado para o atendimento de sua finalidade pública. Sendo assim, se justifica quando empregado na persecução do interesse coletivo, inclusive no âmbito penal.

A necessidade de coleta de dados da pessoa imputada, para fins de persecução penal, é premente. As fases de investigação, processamento e julgamento de fatos penais dependem, necessariamente, da identificação e individualização daqueles que, ao menos em tese, podem ser criminalmente responsáveis pela prática delitiva. É natural, portanto, que os bancos de informação do Estado sejam utilizados para fins de identificação criminal, desde que regulamentados com base nos direitos constitucionalmente consagrados.

Situação diferente, porém, ocorre quando a pessoa imputada que ainda está sendo investigada ou processada – ou seja, que ainda não se viu submetida à decisão transitada em julgado – tem cerceados seus direitos da personalidade e limitada a sua autodeterminação informacional. O fato de responder a um inquérito ou processo criminal não pode implicar, automaticamente, em uma renúncia tácita do direito aos próprios dados pessoais. Especialmente, porque ter seu nome e seus dados pessoais a processos e investigações penais significa diferenciar-se dos demais cidadãos, sendo incluído em uma categoria de criminosos – mesmo sem que haja condenação transitada em julgado.

Como pontua Winfried Hassemer (2009, p. 78), a atual política criminal aceita diferenciar, a partir da reputação, os criminosos dos demais cidadãos. Atua, ainda, para consolidar o real temor da população diante do crime. De fato, conforme reconhece o autor, essa é uma característica também dos Estados democráticos, que se consubstancia nas necessidades de segurança da população.

Diante disso, princípios genuínos e que garantem os direitos fundamentais das pessoas imputadas, tais como a presunção de inocência e os direitos de personalidade, passam para um segundo plano. Nessa nova ordem, deixa-se de garantir aos criminosos – inimigos da segurança pública – o conteúdo total de dignidade humana e personalidade (HASSEMER, 2009, p. 79).

Não se pode, porém, perder de vista o fato de que "o simples manuseio dessas necessidades podem arruinar" o direito e o processo penal: "o medo do crime é um veneno político-criminal para as garantias e os mecanismos de salvaguarda", dos quais o direito necessita, seja pelas vias constitucionais, seja pelas

tradições de direitos humanos (HASSEMER, 2009, p. 78).

Na realidade dos dados pessoais, o medo da sociedade em relação ao criminoso não pode justificar a violação à presunção de inocência e aos direitos de personalidade. Essa postura do Estado, muitas vezes fundamentada a partir de interesses supostamente legítimos de pessoas que temem se aproximar pessoal ou profissionalmente de quem responde a um processo penal, possibilita a distinção entre pessoas nas categorias "criminosos" e "não criminosos".

Com isso, o Estado se torna o próprio agente da discriminação (SABA, 2007, p. 23) das pessoas imputadas no processo penal. Por trás de uma norma aparentemente neutra e democrática, como é o caso da publicidade, se possibilita – ainda que indiretamente – a estigmatização daqueles que respondem a ações penais e têm seus dados pessoais disponibilizados a qualquer um e por qualquer motivo na internet.

Vale destacar que, no contexto brasileiro, a estigmatização tem cor e endereço: são os pretos e moradores de periferias quem mais sofrem com a discriminação. Com a disponibilização de seus dados pessoais na internet, além da raça e da condição social, grande maioria das pessoas imputadas em processos penais30 também passa a ostentar o rótulo on-line de "criminosos", circunstância que lhes gera prejuízos pessoais e profissionais antes mesmo de eventual condenação criminal.

E essa preocupação também precisa ser compartilhada com o processo penal. A ralé, composta por pessoas pretas, pobres e periféricas, foi e continua sendo a grande "clientela" do processo penal (BARROS, 2018, p. 18). A invisibilidade sempre foi a regra e serve para encobrir o desrespeito às garantias; o processo penal, nesses casos, esteve e continua em crise democrática.

Essa crise, contudo, tem ganhado importantes reforços. Os discursos emergenciais (CHOUKR, 2002; MOCCIA, 2011) de combate à corrupção, à lavagem de dinheiro e à criminalidade organizada atingem uma gama de pessoas muito diferente da clientela penal típica: empresários vetados por regras de compliance, profissionais demitidos de grandes corporações ou comerciantes impedidos de celebrar negócios; estes são os novos alvos atingidos pela violação de garantias fundamentais. A partir da liberação irrestrita de seus dados pessoais, esses sujeitos também passam a sofrer os males da estigmatização, antes mesmo de serem condenados definitivamente.

É relevante, neste aspecto, encarar a situação sem revanchismos, afinal, o descaso histórico aos direitos e às garantias daqueles que sempre estiveram submetidos aos arbítrios do sistema penal não pode justificar o atual estado de coisas (BARROS, 2018, p. 20). Pelo contrário: se a invisibilidade impedia a constatação das violações que o Estado pratica em desfavor das pessoas imputadas no processo penal, deve-se aproveitar o atual momento de crise constitucional para buscar soluções aos problemas delimitados.

No caso da tutela dos dados pessoais, deve-se reconhecer que o verdadeiro desenvolvimento democrático se vislumbra na interação entre o Estado e a pessoa imputada, titular dos seus dados (BLUM; LÓPEZ, 2020, p. 175). Essa interação, por sua vez, somente é possível pelo reconhecimento e regulamentação de ambos os direitos: o da sociedade, de ter acesso a processos públicos; e o das pessoas imputadas no processo penal, de terem sua privacidade e intimidade preservados até a decisão definitiva, como forma de assegurar a presunção de inocência.

Para isso, o rigor imposto pela LGPD à gestão dos dados pelo poder público – determinando a necessidade de indicação de pessoa encarregada pelo tratamento de dados pessoais (artigo 39) e relacionando as sanções às quais se sujeitam os agentes de tratamento de dados em caso de violação à norma (artigo 52, § 3º) – precisa ser aplicado àquele que dá publicidade a dados de pessoas imputadas, notadamente quando desnecessários ou não relacionados com a persecução penal. No caso que ilustra este trabalho, seria a hipótese de que o encarregado de dados do Tribunal de Justiça respondesse: por qual motivo os números de telefone, endereço e outros dados pessoais de pessoas imputadas estão disponíveis para acesso ao público?

Outro fator de suma importância é reconhecer que "há um enorme déficit de proteção dos cidadãos, visto que não há regulação geral sobre a licitude, a transparência ou a segurança do tratamento de dados em matéria penal" (BRASIL, 2020, p. 2). Partindo dessa premissa, a Câmara dos Deputados criou uma Comissão de Juristas, para propor uma LGPD Penal.

O Anteprojeto da chamada "Lei de Proteção de Dados para Segurança Pública e Persecução Penal" foi apresentado em junho de 2020 e dispõe sobre o tratamento de dados pessoais realizado por autoridades competentes para atividades de segurança pública e de persecução penal, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural sujeita à investigação criminal.

Em seu artigo 2º, a LGPD Penal apresenta como fundamentos que disciplinam a proteção de dados pessoais em atividades de segurança pública e de persecução penal a dignidade e os direitos humanos; o livre desenvolvimento da personalidade e o exercício da cidadania pelas pessoas naturais; a autodeterminação informativa; o respeito à vida privada e à intimidade; a liberdade de manifestação do pensamento, de expressão, de informação, de comunicação e de opinião; a presunção de inocência; a confidencialidade e integridade dos sistemas informáticos pessoais; e as garantias do devido processo legal, da ampla defesa, do contraditório, da motivação e da reserva legal.

Ao titular dos dados pessoais – ou seja, à pessoa imputada –, a proposta legislativa garante o direito de obter do controlador, em relação aos dados do titular por ele tratados, entre outros, a anonimização, o bloqueio ou a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei (artigo 19, IV). Além disso, determina que os sistemas utilizados para o tratamento de dados pessoais sejam "estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais" (artigo 37), ressaltando que a pessoa "responsável pelo tratamento deve implementar medidas técnicas e organizacionais adequadas para garantir que, por padrão, apenas os dados pessoais necessários para cada finalidade específica do tratamento sejam processados" (artigo 37, § 3º).

As particularidades do ambiente penal são diversas e uma Lei Geral de Proteção de Dados específica é necessária para consagrar direitos fundamentais às pessoas imputadas. Nada obstante, sua efetiva contribuição dependeria de, pelo menos, mais três fatores.

Primeiro, deve-se reconhecer que a implementação da LGPD Penal precisa estar em cotejo com a realidade e a prática dos Tribunais, bem como com as possibilidades oferecidas pelas diversas plataformas digitais adotadas pelos órgãos jurisdicionais ao redor do Brasil (PJe, JPe, Projudi, eProc, e-Saj, Themis e outros). É preciso que as ferramentas tecnológicas sejam, constantemente, submetidas a juízos valorativos e críticos (technology assessment) acerca de seus riscos e de suas vantagens, com orientações interdisciplinares que orientam a complexa interação da tecnologia nos diversos ramos do conhecimento jurídico (PERÉZ LUÑO, 2009, p. 82).

Igualmente, depende dos Estados a adoção de medidas relacionadas à proteção de dados, sendo necessária a indicação de pessoa física encarregada pelo tratamento dos dados pessoais. Essa determinação, já presente no artigo 39 da LGPD e em vigor desde setembro de 2020, até então não foi adotada.

A pessoa física encarregada de dados deverá garantir a gestão dos dados pessoais e promover mudanças relacionadas com o incremento da segurança das informações disponíveis em processos judiciais. Ainda, estará sujeito a sanções em caso de violação das normas de proteção de dados, podendo ser responsabilizado civil e administrativamente por atos ou omissões que prejudiquem seus titulares.

Em segundo lugar, cumpre reconhecer a necessidade de que as pessoas imputadas, até o trânsito em julgado de decisão condenatória, tenham seus dados pessoais protegidos do acesso público. O raciocínio

aqui empregado não é inédito no sistema processual penal: a lógica é idêntica à que rege a emissão das certidões criminais por todo o Brasil.

Durante a tramitação de processo criminal, a certidão criminal solicitada em nome de pessoas imputadas é negativa; posteriormente à condenação transitada em julgado, a certidão é positiva. É o que determina a já mencionada Resolução 121, de 2010, do CNJ, em seu artigo 8º, § 1º, I:

"Art. 8º A certidão judicial, cível ou criminal, será negativa quando não houver feito em tramitação contra a pessoa a respeito da qual foi solicitada.

§ 1º A certidão judicial criminal também será negativa:

I – quando nela constar a distribuição de termo circunstanciado, inquérito ou processo em tramitação e não houver sentença condenatória transitada em julgado."

Com efeito, se uma pessoa que deseja saber se outra responde a um processo criminal apenas terá tal informação depois do trânsito em julgado de sentença condenatória, é um contrassenso permitir que, a partir de uma simples busca no Google, esse dado esteja disponível. Principalmente, considerando que a propriedade sobre os dados pessoais recai sobre seus titulares, e não ao processo em si. O direito garantido à pessoa imputada de não ter, contra si, certidão negativa enquanto não transitar em julgado a sentença condenatória deve, então, se estender para as outras modalidades de acesso às informações processuais, assim como a certidão da pessoa imputada cujo caso referência foi analisado no item 1 deste artigo se apresentará negativa porquanto ainda pendentes sentença e trânsito em julgado, seus dados pessoais deveriam ser preservados, de forma a impedir a identificação do titular.

As duas medidas aqui propostas, em complementação ao Anteprojeto da LGPD Penal, possibilitam uma ampliação da esfera de direitos individuais da pessoa imputada ao contexto tecnológico atual, além de em nada prejudicarem o acesso às informações necessárias para a persecução penal, que poderia ser acessada a qualquer tempo por advogados, promotores, policiais, juízes ou serventuários.

A sociedade, da mesma forma, não seria lesada em seus direitos, podendo acompanhar os andamentos processuais com a devida transparência e, assim, exercer o controle democrático da atuação judicial. Para tanto, não é preciso saber onde vive a pessoa imputada ou qual o seu número de telefone.

Dessa forma, o rigor estabelecido sobre a circulação de dados pessoais, que "se manifesta sobretudo pela proibição de sua coleta por parte de determinados sujeitos (por exemplo, empregadores) e pela exclusão de legitimidade de certas formas de coleta e circulação" (RODOTÀ, 2008, p. 64), seria uma alternativa para possibilitar, simultaneamente, a proteção do direito à informação coletiva e o interesse privado.

Por fim, pode-se falar também em um terceiro fator, cuja abrangência não foge ao objeto deste trabalho: é imperiosa uma definição de diretrizes éticas para a utilização de dados pessoais, em especial aqueles sensíveis ou que podem, de qualquer maneira, interferir nos direitos de personalidade.

Na União Europeia, os riscos que as diversas plataformas de IA podem representar também têm sido encarados com máxima seriedade. Em 2019, a Comissão Europeia divulgou o "Guia Ético para uma Inteligência Artificial Confiável"31, documento que, apesar de não ter caráter vinculativo, serve como parâmetro para a atuação científica e legal do tema. O modelo se ampara sobre quatro pilares éticos básicos: a autonomia humana – no sentido de que os sistemas de IA não podem subordinar, coagir, enganar, manipular, condicionar ou arregimentar injustificadamente os seres humanos; a prevenção se danos – que impede os sistemas de IA de afetarem negativamente a vida dos seres humanos de qualquer forma; a equidade – a fim de garantir uma distribuição equitativa e justa dos benefícios e dos custos; e a explicabilidade – cuja intenção é garantir que os processos de IA sejam transparentes e abertos ao público em geral (ROSSI, 2019, e-book).

Tais limites éticos já encontram, ao menos em solo europeu, efeitos práticos. Em meados de 2021, o Comitê Europeu de Proteção de Dados (EDPB) e a Autoridade Europeia para a Proteção de Dados (EDPS) emitiram uma opinião conjunta32 que sugere o banimento do emprego de IA para reconhecimento facial de pessoas em ambientes públicos, exatamente considerando a incompatibilidade entre tal ferramenta tecnológica e a garantia de direitos e liberdades fundamentais, com destaque para a privacidade e anonimização individual.

De fato, as potencialidades da tecnologia não podem ser recepcionadas acriticamente, como se fossem sempre benéficas ou facilitadoras da vida humana (BORDONI, 2017, e-book). Quando potencialmente violador de direitos fundamentais, o tratamento de dados pessoais deve, assim como a Inteligência Artificial, ser parametrizado por princípios éticos que garantam ao indivíduo – sujeito dos seus dados pessoais – maior segurança, ao invés do medo constante de ter sua privacidade invadida pelo Estado, exposta por plataformas on-line de busca e, consequentemente, de se ver socialmente excluído ou discriminado -(BORDONI, 2017, e-book).

6.Conclusão

A Lei Geral de Proteção de Dados é um passo importante na proteção dos -direitos de personalidade que, no processo penal, estão atrelados à presunção de inocência. Compete aos agentes do Estado restringir o acesso a dados pessoais de indivíduos penalmente processados. Os princípios da transparência e publicidade podem conviver perfeitamente com os direitos de personalidade e com o tratamento dispensado ao inocente.

Aos sujeitos, como titulares de seus dados pessoais, deve ser assegurado o livre desenvolvimento da personalidade, em todas as suas facetas constitucionais. À pessoa imputada, no processo penal, deve ser possibilitado o pleno exercício da personalidade até que transitada em julgado a condenação.

Para isso, o Estado não pode se eximir de suas responsabilidades. Todos os órgãos públicos, no trato com dados pessoais, estão vinculados à LGPD e devem se ater, detidamente, aos seus termos. Os Tribunais e demais agências públicas estão obrigados, pela legislação vigente, a nomear agentes encarregados de cuidar do tratamento de dados pessoais, os quais estarão sujeitos a sanções cíveis e administrativas quando violada a proteção aos dados pessoais.

Conhecer as disposições da LGPD e seus princípios fundantes, bem como promover uma atividade legislativa própria para a proteção de dados no âmbito penal é um passo relevante, mas não suficiente. O Estado precisa se empenhar e levar a sério e com rigor ético a proteção dos dados individuais e as disposições legislativas, da mesma forma como tem exigido o compromisso e a adesão de empresas privadas. Afinal, não se pode demandar, no setor privado, uma tutela que inexiste no âmbito público quando a obrigação é compartilhada.

Ademais, as pessoas imputadas têm direito de serem tratadas como inocentes, preservarem seus empregos, renovarem documentos, manterem laços sociais, participarem de processos seletivos, abrirem contas em instituições financeiras, dando continuidade às atividades íntimas e privadas até que, efetivamente, venham a ser julgados. Os holofotes da Justiça Criminal não podem ultrapassar os limites estabelecidos pela Constituição e pela Lei Geral de Proteção de Dados.

7.Referências

AMARAL, Augusto Jobim do. A pré-ocupação de inocência no processo penal. Revista da Faculdade de Direito da UFMG, n. 62, p. 85-118, 2013.

ANDOLINA, Italo; VIGNERA, Giuseppe. I fondamenti costituzionali della giustiziacivile: il modello costituzionale del processo civile italiano. 2. ed. Torino: Giappichelli, 1997.

ANDRADE, André; JOIA, Luiz Antonio. Organizational structure and ICT strategies in the Brazilian Judiciary System. Government Information Quarterly, v. 29, p. S32-S42, 2012.

BARROS, Flaviane de Magalhães. A atual crise do processo penal brasileiro, direitos fundamentais e garantias processuais. Duc In Altum, v. 10, n. 21, p. 05-33, 2018.

BEIGNER, Bernard. Les droits de la personnalité. Paris: PUF, 1992.

BINDER, Alberto. Iniciación al proceso penal acusatório: para auxiliares de la Justicia. Buenos Aires: Campomanes Libros, 2000.

BLUM, Renato Opice; LÓPEZ, Nuria. Lei Geral de Proteção de Dados no setor público: transparência e fortalecimento do Estado Democrático de Direito. Cadernos Jurídicos, São Paulo, v. 21, n. 53, p. 171-177, jan.-mar. 2020.

BORDONI, Carlo. State of fear: in a liquid word. Nova Iorque: Routledge, 2017.

BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Dispõe sobre o tratamento de dados pessoais realizado por autoridades competentes para atividades de segurança pública e de persecução penal, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. 2020. Disponível em: [https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf]. Acesso em: 07.08.2021.

CAMPOS, Francisco. Exposição de motivos do Código de Processo Penal. 1941. Disponível em: [https://honoriscausa.weebly.com/uploads/1/7/4/2/17427811/exmcpp_processo_penal.pdf]. Acesso em: 03.08.2021.

CASARA, Rubens Roberto Rebello. Processo penal do espetáculo (e outros ensaios). São Paulo: Tirant Lo Blanch, 2018.

CASTILLO, Gerardo Barbosa. Presunción de inocencia, derecho al honor y libertad de prensa. Derecho Penal y Criminología, v. 14, n. 47-48, p. 159-171, 1992.

CHOUKR, Fauzi Hassan. Processo penal de emergência. Rio de Janeiro: Lumen Juris, 2002.

COPPIN, Ben. Inteligência Artificial. Rio de Janeiro: LTC, 2013.

CORDERO, Franco. Guida alla procedura penale. Torino: UTET, 1986.

CRUZ, Marco Aurélio da Cunha e; CASTRO, Matheus Felipe de. O habeas data e a concretização do direito à proteção de dados pessoais na metódica constitucional de Friedrich Müller. Revista de Direitos e Garantias Fundamentais, 19(1), p. 191-230, 2018.

DEL MASSO, Fabiano; GODOY, Eduardo. Os efeitos da quarta revolução industrial na dinâmica do trabalho jurídico. Revista Direitos Culturais, v. 15, n. 37, p. 101-121, 2020.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. EspaçoJurídico Journal of Law, v. 12, n. 2, p. 91-108, 2011.

DOTTI, René Ariel. Proteção da vida privada e liberdade de informação. São Paulo: Ed. RT, 1980.

EGBERT, Simon; LEESE, Matthias. Criminal futures: predictive policing and everyday police work. Nova

Iorque: Routledge, 2021.

FENG, Mingchen; ZHENG, Jiangbin; HAN, Yukang; REN, Jinchang; LIU, Qiaoyuan. Big data analytics and mining for crime data analysis, visualization and prediction. International Conference on Brain Inspired Cognitive Systems, Cham, p. 605-614, 2018.

FOLLE, Ana Júlia Cecconello; SCHELEDER, Adriana Fasolo Pilati. As novas tecnologias e a uniformização do processo eletrônico: vantagens e desvantagens. Direito e Novas Tecnologias I: XXIII Congresso Nacional do CONPEDI. 2014.

FRAZÃO; Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados pessoais. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro. São Paulo: Ed. RT, 2019.

FRAZÃO, Ana; SANTOS, Luiza Mendonça da Silva Belo. Plataformas digitais e o negócio de dados: necessário diálogo entre o direito da concorrência e a regulação dos dados. Revista de Direito Público, v. 17, n. 93, 2020.

GARAPON, Antoine; LASSÈGUE, Jean. Justice digitale. Paris: PUF, 2018.

GIACOMOLLI, Nereu José. O devido processo penal: abordagem conforme a Constituição e o Pacto de São José da Costa Rica. São Paulo: Atlas, 2015.

GÓMEZ-TRELLES, Javier Sánchez-Vera. Variaciones sobre la presunción de inocencia: análisis funcional desde el derecho penal. Madrid: Marcial Pons, 2012.

HORECK, Tanya. Justice on demand: true crime in the digital streaming era. Detroit: Wayne University Press, 2019.

ILLUMINATI, Giulio. La presunzione d'innocenza dell'imputato. Bologna: Zanichelli, 1979.

JORDI, Fenoll Nieva. La razón de ser de la presunción de inocencia. 2016. Disponível em: [https://indret.com/wp-content/themes/indret/pdf/1203_es.pdf]. Acesso em: 07.07.2021.

KAPLAN, Jerry. Artificial Intelligence: what everyone needs to know. Oxford: Oxford University Press, 2016.

LAGESON, Sarah Esther. Creating digital legal subjects: the use of online criminal court records for research. Research Handbook on Law and Courts, p. 394--403, 2019.

LESSIG, Lawrence. Code 2.0. Nova Iorque: Soho Books, 2009.

LINOFF, Gordon S.; BERRY, Michael J. Dana mining techniques: for marketing, sales and customer relationship management. Indianapolis: Wiley Publishing, 2011.

MAIMON, Oded; ROKACH, Lior. Introduction to Knowledge Discovery and Data Mining. In: MAIMON, Oded; ROKACH, Lior (Eds.). Data mining and knowledge discovery – Handbook. 2. ed. Londres: Springer, 2020.

MARQUES, Leonardo Augusto Marinho. A dimensão da inocência no processo penal: o direito de ser julgado sem juízos incriminatórios alternativos. In: PINTO, Felipe Martins (Coord.). Presunção de inocência: estudos em homenagem ao Professor Eros Grau. Belo Horizonte: Editora Instituto dos Advogados, 2019.

MENDES, Laura Schertel. Habeas data e autodeterminação informativa: os dois lados da mesma moeda. Direitos Fundamentais e Justiça, v. 12, n. 39, p. 185-2016, 2019.

MENDES, Laura Schertel. O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais: rumo

a um direito fundamental autônomo. In: DONEDA, Danilo (Coord.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018), o novo paradigma da proteção de dados no Brasil. Revista deDireito do Consumidor, v. 120, p. 555-587, 2018.

MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. STF reconhece direito fundamental à proteção de dados. Revista de Direito do Consumidor, São Paulo, v. 130, p. 471-478, 2020.

MOCCIA, Sergio. La perenne emergenza: tendenze autoritarie nel sistema penale. 2. ed. Napoli: Edizioni Scientifiche Italiane, 2011.

MORAIS, José Luiz Bolzan de; BARROS, Flaviane de Magalhães. Compartilhamento de dados e devido processo: como o uso da inteligência artificial pode implicar em uma verdade aleteica. In: NUNES, Dierle; LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro. Inteligência artificial e direito processual: os impactos da virada tecnológica no direito processual. Salvador: JusPodivm, 2020.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). Revista de Direitos e Garantias Fundamentais, v. 19, n. 3, p. 159-180, 2018.

NUNES, Dierle. Virada tecnológica no direito processual (da automação à transformação): seria possível adaptar o procedimento pela tecnologia? In: NUNES, Dierle; LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro. Inteligênciaartificial e direito processual: os impactos da virada tecnológica no direito processual. Salvador: JusPodivm, 2020.

O'NEIL, Cathy. Weapons of math destruction: how big data increases inequality and threatens democracy. Nova Iorque: Crown Publishers, 2016.

PÉREZ LUÑO, Antonio Enrique. Ensayos de informática jurídica. Colonia del Carmen: Distribuciones Fontamara, 2009.

RABINOVICH-EINY, Orna; KATSH, Ethan. Digital justice. Oxford: Oxford University Press, 2017.

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

RODOTÀ, Stefano. L'ansia di sicurezza che cancella i diritti. La Repubblica. Publicado em 23 out. 2001. Disponível em: [https://www.repubblica.it/online/speciale/ventitreottobredue/ventitreottobredue/ventitreottobredue.html]. Acesso em: 07.08.2021.

RODOTÀ, Stefano. Transformações do corpo. Revista Trimestral de Direito Civil, v. 19, n. 19, p. 91-107, 2004.

ROSSI, Francesca. Il confine del futuro: possiamo fidarci dell'intelligenza artificiale? Milão: Feltrinelli Editore, 2019.

SABA, Roberto. (Des)igualdad estructural. In: ALEGRE, Marcelo; GARGARELLA, Roberto (Coords.). El derecho a la igualdad: aportes para un constitucionalismo igualitário. Buenos Aires: LexisNexis, 2007.

SADIN, Éric. La inteligencia artificial o el desafio del siglo: anatomia de um anti-humanismo radical. Buenos Aires: Caja Negra, 2020.

SAMPAIO, José Adércio Leite; MENDIETA, David; FURBINO, Meire; BOCCHINO, Lavínia Assis. Capitalismo de vigilância e a ameaça aos direitos fundamentais da privacidade e da liberdade de expressão. Revista

Jurídica, v. 1, n. 63, p. 89-113, 2021.

SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. Direitos Fundamentais & Justiça, n. 42, p. 179-218, 2020.

SARLET, Ingo Wolfgang; SAAVEDRA, Giovani Agostini. Fundamentos jusfilosóficos e âmbito de proteção do direito fundamental à proteção de dados pessoais. Revista deDireito Público, v. 17, n. 93, 2020.

SCHREIBER, Anderson. Direitos da personalidade. 2. ed. São Paulo: Atlas, 2013.

SCHREIBER, Simone. A publicidade opressiva de julgamentos criminais. Rio de Janeiro: Renovar, 2008.

SCHWARTZ, Paul M. Property, privacy, and personal data. Harvard Law Review, v. 117, p. 2056, 2003.

SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII problem: Privacy and a new concept of personally identifiable information. The New York University Law Review, v. 86, p. 1814, 2011.

SUSSKIND, Richard. Online courts and the future of justice. USA: Oxford University Press, 2019.

UNDERWOOD, Ben; SAIEDIAN, Hossein. Mass surveillance: A study of past practices and technologies to predict future directions. Security and Privacy, 2021.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. In: Harvard Law Review, v. IV, n. 5, 1890.

ZANOIDE DE MORAES, Maurício. Presunção de inocência no processo penal brasileiro. Rio de Janeiro: Lumen Juris, 2010.

ZUBOFF, Shoshana. Big other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta; GUILHON, Luciana; MELGAÇO, Lucas. Tecnopolíticas da vigilância: perspectivas da margem. São Paulo: Boitempo, 2018.

1 .Neologismo que corresponde ao ato de pesquisar no buscador on-line "Google".

2 .No Brasil, a informatização dos processos judiciais é regida pela Lei 11.419/06 e regulamentada pelo próprio Poder Judiciário. Apesar de o Conselho Nacional de Justiça ter instituído, a partir da Resolução 185/13, o Sistema Processo Judicial Eletrônico – PJe como sistema de processamento de informações e prática de atos processuais, cada Tribunal tem autonomia para implantar o sistema eletrônico que melhor atenda às suas necessidades. Sobre a falta de padronização e uniformização dos ambientes judiciários virtuais, veja-se: FOLLE; SCHELEDER, 2014.

3 .Técnica foi desenvolvida por Rosângela Cavallazzi na sua tese de doutoramento (A plasticidade na teoriacontratual), defendida em 1993 na Universidade Federal do Rio de Janeiro.

4 .Disponível em: [https://ab2l.org.br/ecossistema/radar-de-lawtechs-e-legaltechs/]. Acesso em: 27.07.2021.

5 .Os dados sobre os nomes mais comuns entre a população brasileira estão disponíveis no portal "Nomes do Brasil", criado pelo Instituto Brasileiro de Geografia e Estatística e disponível em: [https://censo2010.ibge.gov.br/nomes/#/search]. Acesso em 15.01.2022.

6 .De acordo com o Google, a relevância e utilidade dos resultados apresentados a cada pesquisa no buscador é indexada por uma série de algoritmos que se baseiam em vários fatores, inclusive palavras da consulta, relevância e usabilidade das páginas, conhecimento das fontes, bem como seu local e configurações. Nesse sentido, veja-se: [https://www.google.com/intl/pt-BR/search/howsearchworks/algorithms/]. Acesso em: 14.01.2022.

7 .No Brasil, a automação do sistema judicial pode ser dividida em três fases: a pré-automação, caracterizada pela falta de coordenação nas ações, entre as unidades judiciais, e é marcada pelas iniciativas individuais de juízes e servidores; a automação, a partir da qual os softwares são capazes de executar rotinas básicas, como a distribuição de petições iniciais, acompanhamento de processo, rotinas de publicação, escalas de audiências; virtualização dos processos, que substitui a utilização de papel para processar ações em ambientes eletrônicos (ANDRADE; JOIA, 2012).

8 .Disponível em: [https://suporte.jusbrasil.com.br/hc/pt-br/articles/360041534212]. Acesso em: 27.07.2021.

9 .Disponível em: [https://suporte.jusbrasil.com.br/hc/pt-br/articles/360041539772-Por-que-meu-nome-apareceu-no-Jusbrasil-]. Acesso em: 27.07.2021.

10 .Disponível em: [https://suporte.jusbrasil.com.br/hc/pt-br/articles/360048466791-Quais -s%C3%A3o-os-dados-armazenados-pelo-Jusbrasil-]. Acesso em: 27.07.2021.

11 .A fim de desenvolver uma pesquisa sempre atenta à ética e, igualmente, em respeito ao contraditório, os dados deste trabalho foram encaminhados ao JusBrasil pelo e-mail suporte@jusbrasil.com.br, a fim de que a LegalTech pudesse contribuir, de alguma forma, com os resultados. Em resposta, a JusBrasil encaminhou o seguinte texto, cujo intervalo não colacionado no corpo do texto em razão das regras editoriais do periódico diz: "Desta forma, o Jusbrasil potencializa a materialização do direito fundamental de acesso à informação e influência, diretamente, no acesso à justiça para a sociedade. Compreendemos que há interesse público na divulgação de atos processuais e no acompanhamento das atividades do Poder Judiciário. O trabalho do Jusbrasil amplia o grau de acesso à informação de cunho jurídico e permite a realização de análises quantitativas, através de estatísticas e dados agregados (como a divulgação de quantos processos foram julgados em determinado período ou informações orçamentárias), e qualitativas, o que inclui acompanhamento do teor das decisões e da qualidade da atuação do Poder Judiciário. Inclusive, entre os interesses na análise qualitativa de documentos processuais diversos (e não somente decisões judiciais), apontamos: (i) compreensão de quem são os players que acessam o poder judiciário e como as diferenças de poder afetam o resultado dos processos; (ii) accountability de poder estatal de investidura não democrática; (iii) compreensão sobre tendências jurisprudenciais para auxiliar advogados e partes no

desenho de estratégias de atuação judicial; (iv) fornecer subsídios para que agentes externos possam contribuir com a melhoria da gestão do sistema de justiça. Neste contexto, destacamos ainda a importância da manutenção dos nomes de pessoas físicas em nossa plataforma. O acesso a este tipo de informação que o Jusbrasil viabiliza é útil desde situações simples do cotidiano, como ao verificar se uma empresa é confiável para a compra de eletrônicos por meio de uma pesquisa pelo seu CNPJ na plataforma, até casos mais complexos, como ao permitir a análise dos processos contra jornalistas em um determinado período de tempo para verificar o indicativo de perseguição política."

12 .Para acessar determinados dados específicos, como a íntegra dos andamentos e o valor da causa, é necessário ser assinante do JusBrasil.

13 .Por coerência teórica, os dados pessoais do indivíduo foram ocultados pelos autores.

14 .A publicidade, de acordo com as determinações do CNJ, serviu também como motivação para o Ministro Supremo Tribunal Federal Marco Aurélio Mello quando, em diversas decisões monocráticas, determinou que os nomes completos de pacientes de habeas corpus fossem divulgados na consulta pública, em substituição às iniciais. Veja-se, nesse sentido, as medidas cautelares monocráticas proferidas nos seguintes processos sob relatoria do Ministro: HC 159.113/SP, HC 169.358/RJ, HC 173.989/SP e HC 182.464/SP.

15 .Os casos Daniella Perez, PC Farias, Nardoni e Richthofen são alguns exemplos.

16 .Veja-se, nesse sentido, a reportagem intitulada "Seis vezes em que usuários do Reddit interfiram em casos judiciais", disponível em inglês: [https://www.cbc.ca/shortdocs/features/reddit-websleuths]. Acesso em: 27.07.2021.

17 .No texto original: "On Facebook people share closed-circuit television (CCTV) footage of criminals stealing from local shops or information about missing young people in the spirit of being Good Samaritans. Police departments now post mug shots on their Facebook pages, where people are able to respond with emojis and comments.11 On Twitter people tweet their personal judgments about crimes and criminals and follow court reporters as they live tweet about criminal cases; as one court reporter recounts: "I've been followed by judges and barristers and I get quite a bit of feedback from police officers. I tweeted that one defendant hadn't turned up for a court appearance and a police officer who follows me saw the tweet and then saw him in the street, and arrested him – that's happened a couple of times."

18 .No texto original: "For instance, a researcher may receive a data set of probationers or prisoners from a state level data repository. If these data contain personal identifiers, such as name and date of birth, researchers can turn to online court records to dig deeper into the mechanics of a criminal case. This may clarify items in an aggregate dataset that are unclear for researchers not familiar with the terminology or coding decisions of a criminal justice agency."

19 .Cathy O'Neil (2016, p. 11) alerta que, na atualidade, modelos algorítmicos como este são opacos, não regulamentados e incontestáveis, além de reforçarem a discriminação.

20 .Interessante notar que, apesar de não estar expressamente previsto no rol de garantias fundamentais da Constituição da República de 1988, há expressa vinculação entre a autodeterminação informacional e os direitos fundamentais à liberdade e à dignidade da pessoa humana (MENDES, Laura Schertel, 2019, p. 190).

21 .Disponível em: [https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-3689-3-outubro-1941-322206-exposicaodemotivos-149193-pe.html]. Acesso em: 03.08.2021.

22 .Sobre o modelo constitucional de processo, Flaviane Barros (2018, p. 9) escreve: "Tal compreensão de modelo constitucional de processo, de um modelo único e de tipologia plúrima, se adéqua à noção de que na Constituição encontra-se a base uníssona de princípios que define o processo como garantia, mas que para além de um modelo único ele se expande, aperfeiçoa e especializa, exigindo do intérprete compreendê-lo tanto a partir dos princípios bases, como também, de acordo com as características próprias daquele processo, como especificado por Andolina e Vignera (1997, p. 10)."

23 .A Corte Interamericana de Direitos Humanos já teve a oportunidade de se manifestar, em alguns casos, sobre a presunção de inocência. Em Suárez Rosero vs. Equador, definiu que "princípio da presunção de inocência atende ao propósito das garantias, ao firmar a ideia de que uma pessoa é inocente até que a sua culpabilidade seja demonstrada". Já no caso Ricardo Canese vs. Paraguai, decidiu que "o direito à presunção de inocência é um elemento essencial para a realização efetiva do direito de defesa e acompanha o acusado durante toda a tramitação do processo até que uma sentença condenatória que determine a sua culpabilidade se torne imutável".

24 .Para Augusto Jobim do Amaral (2013, p. 107), poder-se-ia falar, ainda, em uma quarta consequência: "a natureza de regra de fechamento, quer dizer, horizonte de expectativa a ser preenchido com a decisão política auferida na sentença quando persistir a dúvida a ser convertida em certeza jurídica."

25 .A fim de confirmar seu pensamento, Fenoll (2016, p. 6) menciona que existem múltiplas frases, nas mais diversas línguas, que reforçam a ideia de presunção de culpa: em espanhol "cuando el río suena, agua lleva" ou "no hay humo sin fuego"; em inglês "where there is a smoke, there is a fire"; em alemão, "kein rauch ohne flamme". Em francês, "pas de fumée sans feu"; em italiano "non c'è fumo senza arrosto". Na língua portuguesa, a tendência se mantém com a frase popular "onde há fumaça, há fogo".

26 .A necessidade concreta de garantir uma proteção à privacidade pessoal veio a ser percebida somente no final do século XIX. Nesse sentido, o pioneirismo de Warren e Brandeis (1890). Para uma análise historiográfica dos direitos da personalidade, veja-se Beigner (1992, p. 50-58) e Rodotà (2008).

27 .Sobre o histórico mundial da proteção legislativa aos dados pessoais, assim descrevem Marco Aurélio Cruz e Matheus de Castro (2018, 209-210): "A resposta legislativa sobre a proteção dos dados pessoais pode ser categorizada em fases (DONEDA, 2006). A inicial se caracteriza pelo rigor na criação dos arquivos informatizados, com princípios de proteção amplos e abstratos, centrados na atividade do processamento de dados, com regras dirigidas aos agentes do processamento (LIMBERGER, 2008). [...] A segunda fase se compõe de normas menos austeras para a criação de arquivos e fundamentadas na proteção dos dados pessoais como uma liberdade negativa e não mais no fenômeno computacional (LIMBERGER, 2000). [...] Inicia a terceira fase o Convênio de Estrasburgo, de 28.01.1981, com a pretensão de unificação do direito europeu. É uma tentativa de garantir os direitos e de não obstar o desenvolvimento da informática. Preocupa-se em garantir a liberdade de fornecer ou não os dados pessoais. [...] Danilo Doneda (2006, 2011) identifica uma quarta geração das leis que se caracteriza por tentar equalizar as desvantagens da ênfase individual, além de disseminar o modelo das autoridades independentes, criar normas conexas específicas para alguns setores."

28 .Stefano Rodotà (2001) critica, nesse ponto, as medidas que buscam aproximar a falta de privacidade ao incremento da segurança, geralmente acompanhadas da retórica falaciosa de que "quem não deve não teme". O autor incorpora ao argumento a metáfora do "homem de vidro", popularizada na Alemanha nazista, que se baseava na pretensão estatal de conhecer até mesmo os aspectos mais íntimos da vida dos cidadãos, transformando-os sempre em suspeitos os que buscavam a salvaguarda de sua privacidade. Rodotà pontua que, com as novas tecnologias e a inclusão da pessoa no ciberespaço, a retórica falaciosa do "quem não deve não teme" fica ainda mais comprometida, já que a exposição de informações pessoais sujeita os indivíduos ao temor concreto de discriminação e estigmatização.

29 .Conforme salienta MULHOLLAND (2018, p. 165-166), o tratamento jurídico dos dados pessoais sensíveis já era conhecido na legislação brasileira desde a promulgação da Lei de Cadastro Positivo – Lei 12.414/11 (LGL\2011\1883) – que em seu artigo 3º, § 3º, II, proíbe anotações em bancos de dados usados para análise de crédito de "informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas". De acordo com a autoria, "Este princípio não discriminação é dos mais relevantes, no que diz respeito ao tratamento de dados sensíveis. É esse o ponto fundamental quando diante do uso de dados sensíveis potencialmente lesivo, em decorrência de sua capacidade discriminatória, seja por entes privados – i.e. fornecedoras de produtos e serviços – seja por entes públicos".

30 .Sempre válida a menção ao Relatório do Conselho Nacional de Justiça, cujos mais recentes resultados (2020) evidenciam que "O Brasil possui cerca de 860 mil presos, a terceira maior população carcerária do mundo, com cerca de 55% dos detentos sendo jovens com idades entre 15 e 20 anos, negros, de baixa escolaridade e de segmentos de baixa renda da população". Disponível em: [https://www.cnj.jus.br/pesquisas-abordam-relacao-entre-vulnerabilidade-imprensa-e-prisoes/]. Acesso em: 03.08.2021.

31 .Disponível em: [https://www.aepd.es/sites/default/files/2019-12/ai-ethics-guidelines.pdf]. Acesso em: 03.11.2021.

32 .Disponível em: [https://edps.europa.eu/press-publications/press-news/press-releases/ 2021/edpb-edps-call-ban-use-ai-automated-recognition_en]. Acesso em: 03.11.2021.