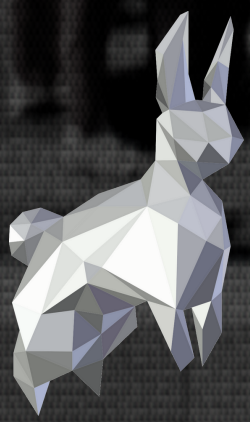
2021 | MARÇO

NOTA TÉCNICA

SOBRE O ANTEPROJETO DE LEI DE PROTEÇÃO DE DADOS PARA A SEGURANÇA PÚBLICA E INVESTIGAÇÃO CRIMINAL



LAPIN

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

Realização:

Laboratório de Políticas Públicas e Internet - LAPIN

Autoria:

Carolina Reis

Eduarda Costa

Felipe Silva

Henrique Bawden

José Renato Laranjeira de Pereira

Paulo Sarmento

Revisão:

Amanda Espiñeira

Carolina Reis

José Renato Laranjeira de Pereira

Thiago Guimarães Moraes

Imagem de Capa:

martinwimmer, Getty Images Signature

LAPIN
LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

lapin.org.br
@lapin.br
/lapinbr
/lapinbr

Sobre esta nota técnica

Em novembro de 2020, foi apresentado à Presidência da Câmara dos Deputados um **Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Investigação Criminal**. O objetivo da futura lei é cumprir o que determina o art. 4º, inciso III, da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD): a existência de legislação específica que trate da matéria no âmbito penal.

Considerando a relevância e a urgência do tema e visando contribuir com o debate no Congresso Nacional, o **Laboratório de Políticas Públicas e Internet - LAPIN** editou esta Nota Técnica para apresentar suas considerações sobre a primeira versão do Anteprojeto de Lei.

Quem somos nós

O Laboratório de Políticas Públicas e Internet (LAPIN) é um *think tank* de composição multidisciplinar com sede na capital federal brasileira. Seu objetivo é apoiar o desenvolvimento de políticas públicas voltadas para a regulação das tecnologias digitais por meio da pesquisa e da conscientização da sociedade.

SUMÁRIO

Sumário Executivo

O **Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Investigação Criminal**[1] é o resultado do trabalho da Comissão de Juristas nomeada pela Presidência da Câmara dos Deputados em novembro de 2019[2]. Atualmente, não há legislação específica que trate da matéria no ordenamento brasileiro, apesar da exigência contida no art. 4º, inciso III da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD). Com isso, falta transparência e há pouco direcionamento legal na atuação de autoridades policiais e de persecução penal no que concerne ao tratamento de dados pessoais e ao uso de tecnologias de vigilância.

A **proteção de dados pessoais** é um direito fundamental autônomo, amparado constitucionalmente pelos direitos à liberdade, à privacidade e ao livre desenvolvimento da personalidade, conforme decidido pelo Supremo Tribunal Federal (STF) em mais de uma ocasião[3]. Considerando o **interesse público na manutenção da segurança e da ordem**, também garantido constitucionalmente, é imprescindível a edição de legislação específica no âmbito penal que delimite e balanceie as fronteiras entre a esfera penal e a garantia de direitos fundamentais.

Portanto, o objetivo da Comissão de Juristas foi elaborar um texto capaz de cumprir a exigência de legislação específica, mas que também acompanhasse o atual estado da arte da temática no mundo. Em que pese o trabalho abrangente da Comissão, **o Anteprojeto possui pontos a serem discutidos e melhorados antes de sua aprovação como lei**. Apresentado em novembro de 2020 à Câmara dos

---

[1]O Anteprojeto de Lei, na versão apresentada pela Comissão de Juristas, pode ser acessado aqui: 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

[2]JANARY JR. "Maia cria comissão de juristas para propor lei sobre uso de dados pessoais em investigações". **Agência Câmara de Notícias**. 27 de novembro de 2019. Disponível em: https://www.camara.leg.br/noticias/618483-maia-cria-comissao-de-juristas-para-propor-lei-sobre-uso-de-dados-pessoais-em-investigacoes/ Acesso em: 02 mar. 2021.

[3]Ver decisões do STF na Ação Direta de Inconstitucionalidade nº 6.387 (ADIN nº 6.387) e na Arguição de Descumprimento de Preceito Fundamental nº 695 (ADPF nº 695), ambas do Distrito Federal.

Deputados[4], no momento da publicação desta Nota, o Anteprojeto segue à espera de um relator para que possa seguir os trâmites no Congresso Nacional. Contudo, seu texto já está aberto a contribuições da sociedade civil.

A presente Nota Técnica trata sobre a versão do Anteprojeto apresentada pela Comissão de Juristas à Câmara dos Deputados e é o primeiro aporte do LAPIN à discussão. Seus sete capítulos estão ordenados de acordo com a ordem em que os artigos aparecem no Anteprojeto. Cada capítulo apresenta, em seu início, a síntese dos argumentos levantados e, ao final, uma tabela comparativa com a redação atual do Anteprojeto e o texto recomendado pelo LAPIN. O Anexo I contém um quadro completo com todas as alterações textuais propostas por esta Nota Técnica, elencadas também em ordem crescente de acordo com os artigos do Anteprojeto. Por fim, os Anexos II e III contêm, respectivamente, uma lista das abreviações utilizadas ao longo do texto e um glossário com os termos mais importantes para o entendimento do Anteprojeto.

As principais recomendações desta Nota Técnica são:

[art. 4º] Inclusão do dever, para o controlador, de fundamentar decisões que neguem o exercício de direitos pelo titular de dados, quando tal decisão se fundamentar nas excludentes de defesa nacional e segurança do Estado;

[art. 5º] Inclusão dos conceitos de pseudonimização, perfilização (*profiling*) e dado biométrico;

[art. 6º] Revisão da redação dos dispositivos concernentes aos princípios da licitude e da proporcionalidade para definições mais compatíveis com o ordenamento brasileiro;

[art. 23] Determinação explícita de que a autorização prévia da autoridade supervisora para a adoção de sistemas responsáveis por decisões automatizadas diga respeito à adoção de tecnologia específica por cada

[4] BAPTISTA, Renata. "Câmara recebe proposta para criar lei sobre dados de segurança pública". **UOL Tilt.** 06 de novembro de 2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/11/06/camara-recebe-anteprojeto-para-controle-de-dados-de-investigacoes-criminais.htm Acesso em: 02 mar. 2021.

autoridade competente que pretender utilizá-la, ao invés de autorizações genéricas a respeito de uma tecnologia;

[arts. 25 e 26] Estruturação mais detalhada de mecanismos de transparência de sistemas de decisão automatizada.

[arts. 13, 23, 24] Inclusão de prescrições mais detalhadas às autoridades competentes sobre a formulação do RIPD;

[arts. 26 e 29] Organização de capítulo específico para o Relatório de Impacto à Proteção de Dados (RIPD);

[art. 42] Inclusão de parâmetros para realização da análise de impacto regulatório (AIR) que indiquem a necessidade, adequação e proporcionalidade da adoção da tecnologia;

[art. 43] Manutenção da vedação ao uso de tecnologias de monitoramento com identificação de forma massiva e contínua, nos termos já previstos no Anteprojeto, tendo em vista seu elevado risco de violações de direitos fundamentais e garantias constitucionais;

[art. 44] Previsão de publicação de relatório, pela autoridade supervisora, acerca do uso de tecnologias de monitoramento não mais anualmente, mas a cada seis meses;

[arts. 53 e 57] Definição se as condições para a realização de transferências internacionais de dados sã o cumulativas ou alternativas;

[arts. 53 e 55] Adequação dos termos que se referem ao controlador do tratamento;

[art. 55] Inclusão de critérios para análise das garantias adequadas para transferências internacionais de dados;

[art. 55] Inclusão de obrigação de comunicação para o Conselho Nacional de Justiça (CNJ) em caso de transferências internacionais;

[arts. 56 e 57] Adequação dos termos que se referem à cooperação jurídica internacional, limitando-a apenas ao âmbito penal;

[art. 57] Explicitação de quem seria a autoridade de controle;

[art. 59] Previsão expressa sobre a não-subordinação hierárquica da Unidade Especial de Proteção de Dados em Matéria Penal (UPDP) em relação ao Plenário do Conselho Nacional de Justiça (CNJ);

[art. 60] Alteração da competência para indicação da Diretoria da UPDP, para ser realizada pela Presidência da República com sabatina no Senado Federal;

[art. 60] Previsão expressa de vedação ao exercício de atividades profissionais concomitantes aos ocupantes dos cargos da Diretoria da UPDP;

[art. 62] Especificação de que a autoridade supervisora será competente para agir sobre todos os tratamentos de dados cuja finalidade é a segurança pública e a persecução penal, independente de quem os realize;

[art. 62] Inclusão de competência para o aconselhamento de outros órgãos públicos pela autoridade de supervisão;

[art. 62] Ampliação das hipóteses em que relatórios de impacto à proteção de dados pessoais (RIDP) podem ser solicitados;

[art. 62] Ampliação do âmbito da comunicação para órgãos de controle externo nos casos de descumprimento da futura lei.

I - Do âmbito, condições e base principiológica de aplicação da lei

Este capítulo se divide em três títulos: das excludentes de defesa nacional e segurança do Estado; dos conceitos de pseudonimização, perfilização e dado biométrico; e dos princípios da licitude e da proporcionalidade. As recomendações decorrentes destes subcapítulos se inserem, respectivamente, no âmbito de aplicação da futura lei, das condições de sua aplicação e da base principiológica que a norteará.

a. Das excludentes de defesa nacional e segurança do Estado

[art. 4º] Inclusão do dever, para o controlador, de fundamentar decisões que neguem o exercício de direitos pelo titular de dados, quando tal decisão se fundamentar nas excludentes de defesa nacional e segurança do Estado.

De acordo com o art. 4º do Anteprojeto de Lei, **as disposições contidas na futura legislação não se aplicarão**, em princípio, às questões que envolvam exclusivamente **matéria de defesa nacional e segurança do Estado**. Esse artigo criaria, assim, exceções ao âmbito de aplicação da norma.

Tais preceitos servem para restringir a aplicação de uma futura norma cujo objetivo é garantir direitos aos cidadãos; logo, tal restrição deveria atrair uma interpretação igualmente restritiva destes dispositivos[5]. No entanto, apesar de ser prática comum também em legislações estrangeiras[6], consideramos que o art. 4º emprega conceitos abstratos e vagos, como "questões de defesa nacional" e "segurança do Estado".

Para **garantir que tais exceções sejam empregadas somente em hipóteses excepcionais**, algumas legislações estrangeiras preveem mecanismos como a explicação minuciosa desses conceitos ou mesmo condições bem delimitadas para a

[5] FERRAZ JR., Tercio Sampaio. **Introdução ao Estudo do Direito**: técnica, decisão, dominação. 10. ed. rev. atual. e aum. São Paulo: Atlas, 2018. p. 319.
[6] Podemos citar como exemplos a Consideranda 14 da Diretiva 2016/680 da União Europeia e o artigo 110, (1), da Data Protection Act do Reino Unido.

aplicação destas exceções. Dessa forma, pretende-se confirmar que todas as garantias previstas nestas leis sejam aplicadas plenamente, sendo o seu não-emprego efetivamente exceções.

Podemos citar como exemplo o modelo adotado na legislação argentina. A *Ley n. 25.326* optou por não definir minuciosamente o que seria a segurança nacional e, consequentemente, quais tratamentos estariam justificados por ela.

O legislador argentino, ao contrário, optou por estabelecer a postura que deve ser adotada pelo controlador caso este recuse - com base na justificativa de segurança nacional, ordem e segurança pública ou para a proteção dos direitos e interesses de terceiros - um pedido formulado por um titular de dados. Nestes casos, o controlador deve apresentar uma justificativa fundamentada para tal negativa[7]. O que este dispositivo impõe ao controlador, em suma, é o dever da aplicação do princípio da razoabilidade, onde deverá ser descrita a ponderação entre o direito negado ao titular e a atividade estatal que se busca resguardar com esta negativa[8].

Dessa forma, a previsão da lei argentina garante uma maior transparência à limitação ao exercício dos direitos dos titulares de dados em comparação com o Anteprojeto, inclusive assegurando uma revisão posterior desta decisão por via judicial.

Portanto, recomenda-se que a futura lei brasileira exija que **o controlador de dados pessoais fundamente sua decisão quando** houver recusa ao exercício de direitos dos titulares de dados **sob a justificativa de defesa nacional e segurança do Estado**.

Redação atual

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de defesa nacional e segurança do Estado.

[7] Artigo 17 da Ley nº 25.326. Los responsables o usuarios de bancos de datos públicos pueden, **mediante decisión fundada**, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros.

[8] CAYUSO, Susana. **La aplicación del principio de razonabilidad y las limitaciones a los derechos fundamentales**. Pensamiento Constitucional, Buenos Aires, Argentina, v. 6, ed. 6, 1999.

Redação sugerida

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de defesa nacional e segurança do Estado.

Parágrafo único. O controlador ou operador de dados que recusar o exercício dos direitos previstos nesta legislação sob a justificativa de defesa nacional e segurança do Estado deverá fundamentar sua decisão, sob pena de nulidade, nos termos do artigo 19, §3º, desta lei.

b. Dos conceitos de pseudonimização, perfilização e dado biométrico

[art. 5º] Inclusão dos conceitos de pseudonimização, perfilização (*profiling*) e dado biométrico;

O art. 5º do Anteprojeto de Lei traz uma série de conceitos que serão úteis para a plena compreensão das demais disposições contidas em seu texto. Tal conteúdo é fundamental para a futura legislação, considerando a alta complexidade que exige o emprego de termos não usuais.

Apesar do extenso rol apresentado pela Comissão de Juristas no Anteprojeto, certas expressões estão ausentes do seu texto final, enquanto outras deveriam ser mais bem definidas, uma vez que são empregadas posteriormente sem uma definição prévia.

Dentre estas definições, recomenda-se o acréscimo dos conceitos de pseudonimização, perfilização (*profiling*) e dado biométrico, haja vista estes conceitos serem utilizados durante o texto proposto, em seus artigos 37, §2º, 33, inciso VI, e 5, inciso II, respectivamente, sem que haja uma conceituação específica.

Para manutenção da coerência entre diferentes leis, o conceito de **pseudonimização** deve ser idêntico ao adotado no art. 13, §4º, da Lei nº 13.709/18, a LGPD, que consiste no "tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro".

Para a conceituação de **perfilização** e de **dado biométrico**, indica-se a adoção da redação contida na Diretiva 2016/680 da União Europeia, em seu art. 3º, §§ 4º e 13[9], respectivamente, considerando a precisão do texto europeu para delimitar os temas.

O agrupamento de titulares em perfis, uma das modalidade de tratamento de dados contidas no art. 33 do Anteprojeto, naturalmente levanta uma série de repercussões graves na formação de vieses algorítmicos, levantando em especial receios quando aplicadas a persecuções penais[10]. Não delimitar a que se refere esta prática de tratamento de dados pode acarretar lacunas desnecessárias à legislação e, consequentemente, aplicações arbitrárias desta modalidade de tratamento de dados que afetarão gravemente os direitos dos titulares.

Redação sugerida

Art. 5º Para os fins desta Lei, considera-se:
(...)

XXV - **pseudonimização:** tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro;

XXVI - **perfilização:** qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados para avaliar aspectos pessoais de um titular de dados, nomeadamente para analisar ou prever aspectos relacionados com o seu desempenho profissional, a sua situação econômica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocamentos;

XXVII - **Dados biométricos:** dados pessoais resultantes de um tratamento técnico específico, relativos às características físicas, fisiológicas ou comportamentais de um titular de dados, que permitem ou confirmam a sua identificação única, tais como imagens faciais ou dados dactiloscópicos.

---

[9] Diretiva (UE) 2016/680, Artigo 3º. Para efeitos da presente diretiva, entende-se por:
(...)
4) «Definição de perfis», qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações;
(...)
13) «Dados biométricos», dados pessoais resultantes de um tratamento técnico específico, relativos às características físicas, fisiológicas ou comportamentais de uma pessoa singular, que permitem ou confirmam a sua identificação única, tais como imagens faciais ou dados dactiloscópicos;

[10] NOBLE, Safiya Umoja. **Algorithms of Oppression**: How Search Engines Reinforce Racism. Nova Iorque, EUA: [s. n.], 2018.

c. Dos princípios da licitude e da proporcionalidade

[art. 6º] Revisão da redação dos dispositivos concernentes aos princípios da licitude e da proporcionalidade para definições mais compatíveis com o ordenamento brasileiro;

De forma similar à LGPD, o art. 6º do Anteprojeto de Lei prescreve quais princípios nortearão o tratamento de dados pessoais para fins da futura legislação. Apesar de a grande maioria das diretrizes prescritas pelo art. 6º do Anteprojeto serem idênticas às contidas no art. 6º da LGPD, dois princípios do Anteprojeto não têm equivalentes expressos na LGPD: os princípios da licitude e da proporcionalidade, indicados nos incisos I e II, respectivamente.

Entende-se a relevância da previsão do **princípio da licitude**, especialmente no que se refere ao tratamento de dados pessoais realizado pelo Estado no âmbito da segurança pública. Entretanto, sua conceituação pode ser aprimorada para garantir maior proteção ao titular de dados.

A título de exemplo, a Diretiva 2016/680 da União Europeia acrescenta um dever positivo aos agentes de tratamento de dados para que estes **especifiquem ao menos o objetivo do tratamento, o dado pessoal tratado e sua finalidade**[11]. Uma previsão similar neste Anteprojeto não somente traria maior segurança aos titulares de dados, dialogando com o princípio da transparência, como também traria maior efetividade para o princípio da licitude.

Já em relação ao **princípio da proporcionalidade**, este pode se mostrar redundante, já que possui redação quase idêntica ao princípio da adequação, contido no inciso III do art. 6º do Anteprojeto de Lei[12].

---

[11] Diretiva (UE) 2016/680, Artigo 8º. Licitude do tratamento. 2. O direito de um Estado-Membro que rege o tratamento no âmbito da presente diretiva especifica pelo menos **os objetivos do tratamento, os dados pessoais a tratar e as finalidades do tratamento**.

[12] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
(...)
III - adequação: pertinência e relevância do tratamento com os objetivos pretendidos, de acordo com o contexto do tratamento;

A *Ley General De Protección De Datos Personales En Posesión De Sujetos Obligados*, norma mexicana que regulamenta o tratamento de dados pessoais realizado por agentes públicos sob sua jurisdição, pode orientar uma alternativa de redação. A lei mexicana traz certos critérios para a determinação da legalidade de seu tratamento, ao estabelecer que **o tratamento de dados pessoais deve ser adequado, relevante e estritamente necessário para a finalidade que se pretende alcançar**[13].

Sugere-se, portanto, alterar o texto do Anteprojeto de Lei não somente para distinguir o princípio da proporcionalidade do princípio da adequação, conforme exposto acima, mas igualmente para dar-lhe maior efetividade, permitindo uma posterior avaliação da legalidade do tratamento com base em critérios mais objetivos.

Redação atual

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

(...)

V – proporcionalidade: compatibilidade do tratamento com os objetivos pretendidos, de acordo com o contexto do tratamento;

Redação sugerida

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

(...)

V – proporcionalidade: **garantia de limitação de tratamento de dados pessoais somente aos dados que se mostrem adequados, relevantes e estritamente necessários;**

(...)

Parágrafo Único: o agente de tratamento deverá descrever os objetivos do tratamento, os dados pessoais tratados e a finalidade do tratamento de maneira acessível aos cidadãos.

[13] Articulo 25. El responsable sólo deberá tratar los datos personales que resulten **adecuados, relevantes y estrictamente necesarios** para la finalidad que justifica su tratamiento.

II - Dos sistemas de decisão automatizada

Sistemas de decisão automatizada são aqueles que tomam decisões com pouca ou nenhuma interferência humana. No âmbito da segurança pública e persecução penal, tais decisões podem acarretar graves violações de direitos fundamentais, já que podem influenciar diretamente na liberdade de indivíduos. Por esse motivo, tais tecnologias devem ser utilizadas com cautela e em contextos específicos. De modo a garantir maior transparência sobre seu uso e funcionamento, este capítulo defende que haja autorização específica da autoridade supervisora para cada nova adoção de sistemas dessa natureza.

a. Da autorização específica pela autoridade supervisora para cada novo sistema de decisão automatizada adotado

[art. 23] Revisão da redação dos dispositivos concernentes aos princípios da licitude e da proporcionalidade para definições mais compatíveis com o ordenamento brasileiro;

Os artigos 23 a 26 do Anteprojeto regulamentam o uso de sistemas de decisões automatizadas. Trazem disposições específicas a respeito da elaboração de relatórios de impacto de proteção de dados pessoais (RIPD), a necessidade de instrução mais detalhada do processo legislativo de lei que pretender regulamentar o tema, a realização de auditorias, bem como garantia do desenvolvimento de mecanismos adequados para garantir maior transparência desses sistemas.

A exposição de motivos do Anteprojeto, inclusive, faz referência explícita à promoção de explicações desses sistemas, muitas vezes tidos como "caixas pretas" por não permitirem a compreensão, por humanos, de seu funcionamento ou de decisões que venham a tomar, apesar dos riscos que impõem ao exercício de direitos fundamentais[14].

[14] PASQUALE, F. **The Black Box Society**. The Secret Algorithms That Control Money and Information. Harvard University Press. Cambridge, Massachusetts. 2015.

A lógica do Anteprojeto segue o passo de estudos recentes que chamam atenção para os riscos identificados em sistemas preditivos vinculados a seu potencial discriminatório, especialmente no que diz respeito a vieses racistas ou de gênero[15]. Por isso, tais estudos refletem uma preocupação em superar a ultrapassada ideia de que esses sistemas seriam neutros[16], bem como de garantir maior escrutínio por parte da sociedade e ferramentas para responsabilização e compensação por eventuais erros que sejam causados por intermédio dessas ferramentas. Esses riscos motivam a recomendação desta Nota Técnica em relação ao art. 23.

O art. 23 determina que o uso de sistemas de decisões automatizadas que afetem os interesses dos titulares de dados devem ser previamente autorizados pelo Conselho Nacional de Justiça (CNJ), no papel de autoridade supervisora. A iniciativa é louvável, já que garante o controle prévio da atividade pela entidade estatal especializada na proteção de dados para fins penais, permitindo maior supervisão no tratamento de dados pessoais. Além disso, age de forma similar ao que determina a Diretiva 2016/680 da União Europeia em seu artigo 11, com a diferença de que esta exige especificamente a elaboração de lei.

No entanto, considera-se cabível a inclusão de parágrafo ao art. 23 que preveja que tal autorização se refira individualmente a cada sistema adotado por uma autoridade competente específica. Ou seja, não basta que seja concedida pelo CNJ uma autorização genérica a respeito do uso de uma tecnologia específica, mas que cada nova autoridade que venha a utilizá-la requeira uma autorização individual para o uso no escopo de sua competência.

Isso porque **a funcionalidade e a acurácia de cada modelo de decisão automatizada varia de acordo com uma série de fatores que devem ser analisados caso a caso**. Modelos de *machine learning*, por exemplo, que compõem uma subdivisão do guarda-chuva da inteligência artificial, são formados por *algoritmos*, ou seja, uma série de instruções computacionais a respeito de como o sistema deve agir para tomar

---

[15] National Institute of Standards and Technology—NIST. **Face Recognition Vendor Test (FRVT) Part 3**: Demographic Effects. Disponível em https://doi.org/10.6028/NIST.IR.8280 (2019). Acesso em 20 Jan 2020.

[16] BUCHER, T. **If... then:** algorithmic power and politics. Oxford University Press, New York, 1st edition, 2018.

decisões[17], bem como pelos *dados* que utilizam para aprender a realizar predições e para emitir decisões, comumente chamadas de *outputs*[18]. Alguns sistemas, como o de reconhecimento facial, também dependem de *hardware* específico, como a câmera que capta as imagens que serão objeto de análise pelo algoritmo.

Nesse sentido, deve ser objeto de escrutínio o funcionamento não só dos algoritmos, que variam de acordo com cada marca e modelo de *software*, mas também dos dados sobre os quais eles se apoiam para gerar as predições e do *hardware* que se utiliza para coletar novos dados. Trata-se, pois, de ao menos três variáveis que se alteram individualmente em relação a cada aplicação de *machine learning*, o que torna insuficiente a concessão de autorizações genéricas.

Retornando ao exemplo do sistema de reconhecimento facial, o algoritmo desenvolvido por uma empresa será diferente daquele desenvolvido por outra. Além disso, o banco de dados utilizado para buscar foragidos pela polícia do Amazonas poderá ter imagens com resolução diferente daquele das autoridades de Alagoas. Por fim, os modelos das câmeras e os *softwares* utilizados por cada órgão poderão também variar.

Todos esses fatores afetam inevitavelmente a qualidade ou, pelo menos, o modo de funcionamento dos sistemas adotados. Por este motivo, é recomendável que **cada nova aplicação seja objeto de escrutínio específico pela autoridade supervisora**, razão pela qual sugerimos a inclusão de novo parágrafo no âmbito do art. 23.

Redação atual

Art. 23. As decisões tomadas com base no tratamento automatizado de dados pessoais, que afetem os interesses do titular, devem ser precedidas de autorização do Conselho Nacional de Justiça e de publicação de relatório de impacto, que comprove a adoção das garantias adequadas para os direitos e liberdades do titular, incluído o direito de solicitar a revisão da decisão por uma pessoa natural e observado o disposto no artigo 25.

(...)

[17] JOLLIFFEE, I. **Principal component analysis**. International Encyclopedia of Statistical Science; Springer: Berlin, Germany, 2011; pp. 1094–1096.
[18] SHALEV-SHWARTZ, S. & BEN-DAVID, S. **Understanding Machine Learning**: From Theory to Algorithms, Cambridge University Press, Cambridge, 2014.

Redação sugerida

Art. 23. As decisões tomadas com base no tratamento automatizado de dados pessoais, que afetem os interesses do titular, devem ser precedidas de autorização do Conselho Nacional de Justiça e de publicação de relatório de impacto, que comprove a adoção das garantias adequadas para os direitos e liberdades do titular, incluído o direito de solicitar a revisão da decisão por uma pessoa natural e observado o disposto no artigo 25.

(...)

§5º As autorizações de que trata o caput serão concedidas de forma individualizada para cada autoridade competente, levando em conta o contexto e a finalidade de sua aplicação específica, sendo vedadas autorizações genéricas referentes a um sistema responsável por decisões automatizadas.

b. Da transparência dos sistemas de decisões automatizadas

[arts. 25 e 26] Estruturação mais detalhada de mecanismos de transparência de sistemas de decisão automatizada.

Sistemas responsáveis pela tomada de decisões automatizadas, como aqueles baseados em inteligência artificial, têm sido cada vez mais utilizados na segurança e na persecução penal[19]. Pelo fato de se basearem em dados que acumulam décadas de práticas reveladoras de discriminação por parte tanto de autoridades policiais quanto pelos seus próprios desenvolvedores, tais sistemas apresentam frequentemente vieses racistas ou de gênero nas decisões que tomam[20].

Tal característica, no entanto, vem frequentemente desacompanhada de uma preocupação, tanto das autoridades quanto dos próprios desenvolvedores da tecnologia, de maior transparência a respeito do funcionamento desses sistemas e em

[19] RICHARDSON, Rashida, & SCHULTZ, Jason & CRAWFORD, Kate. **Dirty Data, Bad Predictions:** How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice (13 fev 2019). 94 N.Y.U. L. REV. ONLINE 192 (2019). Disponível em: https://ssrn.com/abstract=3333423. Acesso em 14 jan 2021.

[20] RAMOS, Silvia (coord.). **Retratos da Violência** – Cinco meses de monitoramento, análises e descobertas. Rio de Janeiro: Rede de Observatórios da Segurança/CESeC, novembro de 2019.

relação aos procedimentos adotados pela autoridade a partir do momento em que o sistema realiza determinada predição.

Essa opacidade impede que haja escrutínio público que permita a análise de quais medidas devem ser tomadas para garantir o funcionamento justo, ético e adequado dessa tecnologia. Pelo contrário, os motivos em volta dos erros desses sistemas ficam majoritariamente encerrados dentro dos próprios órgãos, o que impede a reflexão sobre meios de evitá-los e a responsabilização de eventuais culpados. Essa postura relega esses erros à constante repetição.

Um caso no Rio de Janeiro representa bem essa realidade. Em 2019, uma mulher foi detida após ser erroneamente confundida com uma foragida da polícia por um sistema de reconhecimento facial. Somente após ser levada à delegacia para apuração é que os policiais se deram conta de que a foragida já havia sido presa e não era mais procurada pela polícia. Identificado o erro, a mulher foi liberada[21].

O caso reflete a existência de ao menos três equívocos. O primeiro se refere à base de dados, que não havia sido corretamente atualizada, permitindo que imagens de pessoas que já não eram mais procuradas constassem em seu banco.

O segundo compreende um erro de procedimento da polícia. As autoridades policiais trabalhavam com uma taxa de 70% de possibilidade de compatibilidade entre a imagem capturada pela câmera e a presente na base de dados,[22] o que pode ser uma marca insuficiente levando em conta o impacto que pode haver para uma pessoa ser detida por engano por um erro tecnológico.

Por fim, houve uma falha ou do algoritmo, que não funcionou de forma adequada, ou da própria câmera, cuja resolução poderia ser inadequada ou que poderia estar mal posicionada no momento. A esse respeito, pela falta de informações

---

[21] G1 Rio. **Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano**, 11 de julho de 2019. Disponível em https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml. Acesso em 21 jan. 2021.

[22] Olhar Digital. **Mulher é detida no Rio por erro em câmera de reconhecimento facial.** 10 de julho de 2019. Disponível em https://olhardigital.com.br/2019/07/10/seguranca/mulher-e-detida-no-rio-por-erro-em-camera-de-reconhecimento-facial/#:~:text=As%20c%C3%A2meras%20de%20seguran%C3%A7a%20com,como%20uma%20foragida%20da%20Justi%C3%A7a.&text=De%20acordo%20com%20o%20porta,por%20isso%2C%20ocorreu%20o%20erro. Acesso em 21 jan. 2021.

públicas disponibilizadas pela polícia, não é possível identificar onde tenha ocorrido o equívoco.

Para superar esse tipo de situação, é necessário que ferramentas legais sejam incluídas no Anteprojeto de forma a garantir que as autoridades competentes, que utilizam sistemas de decisão automatizada, proporcionem maior transparência.

Pelo menos **três fatores deveriam ser objeto de maior clareza** por parte dos órgãos que fazem uso de sistemas responsáveis por decisões automatizadas frente à autoridade de supervisão de proteção de dados para fins penais:

1. as **bases de dados** utilizadas para alimentar esses sistemas;
2. em casos que se mostrarem essenciais para averiguar potencial discriminatório ou para conferir se não houve erros, garantir que só sejam adotados sistemas interpretáveis ou que forneçam explicações adequadas descrevendo as **variáveis, correlações e inferências** realizadas pelos sistemas, que devem estar em linguagem a ser compreendida tanto por leigos quanto por técnicos em tecnologia da informação;
3. os **procedimentos adotados pela autoridade competente** uma vez que uma decisão automatizada é realizada[23].

Além disso, seguindo na esteira da obrigação imposta pelo art. 26, §2º do Anteprojeto, de que tais sistemas devem ser auditáveis, é necessário que a autoridade competente apresente informações que permitam que decisões individualizadas do sistema sejam explicadas mediante determinação do CNJ. Por isso, a criação de sistemas interpretáveis ou capazes de fornecer explicações a respeito de seus processos de tomada de decisão é fundamental.

Uma sugestão de solução que poderia auxiliar no fornecimento de explicações é o uso de contra-fatos (*counterfactuals*), isto é, informações sobre que parâmetros deveriam ser alterados para que uma decisão fosse diferente.[24] Se bem utilizados, os

[23] CITRON, D. & PASQUALE, Frank. **The Scored Society**: Due Process for Automated Predictions. University of Maryland Francis King Carey School of Law Legal Studies Research Paper, No. 2014 – 8

[24] WACHTER, S., MITTELSTADT, B., RUSSELL, C. Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR. University of Oxford. 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063289. Acesso em: 19 mar. 2021.

contra-fatos podem ajudar titulares de dados a (i) entender por que uma decisão particular foi alcançada; (ii) fornecer motivos para contestar adversamente decisões, e (iii) entender o que poderia ser alterado para receber um resultado desejado no futuro, com base no modelo de tomada de decisão atual.[25]

A obrigação de disponibilização de tais informações para a autoridade de proteção de dados para fins penais varia caso a caso e poderá ser auditada nos termos do que descreve o art. 26 do Anteprojeto.

A esse respeito, é adequada a alteração do art. 26 em alguns pontos, de modo a **deixar mais claro quais informações poderão ser objeto de investigação por parte da auditoria desses sistemas**. O §3º pode ser acrescido de uma exigência de que o sistema deve ser interpretável a ponto de permitir a compreensão do procedimento de adoção de determinada decisão automatizada, não só da lógica do sistema como um todo. A redação proposta pretende dar maior liberdade para que a autoridade supervisora adapte sua atuação ao desenvolvimento dessas tecnologias.

Tal noção segue o racional descrito em estudo do Berkman Klein Center a respeito do **papel da *explicabilidade* em sistemas de inteligência artificial** para a responsabilização de indivíduos por decisões tomadas por esses modelos. O estudo propõe que as seguintes perguntas sejam respondidas pelo sistema quando for necessária a compreensão do racional de uma decisão específica para garantir o exercício de direitos do titular de dados:

1. Quais os principais fatores (inputs) tomados em conta na tomada de decisão automatizada? Por exemplo, a localização de um sujeito, sua raça, o fato de participar de determinado grupo ou se interagiu recentemente com um conteúdo específico?

2. Qual foi o peso de cada um desses fatores na tomada de decisão?

3. Algum dos dados levados em consideração pode receber pesos distintos em decisões automatizadas semelhantes?[26]

---

[25] Ibid, p. 4.

[26] DOSHI-VELEZ, F. et al. **Accountability of AI Under the Law**: The Role of Explanation. Berkman Klein Center Working Group on Explanation and the Law, Berkman Klein Center for Internet & Society working

A importância de ressaltar melhor os mecanismos de transparência a serem observados em sistemas responsáveis por decisões automatizadas segue preocupações advindas das divergências de interpretações do Regulamento Geral de Proteção de Dados Pessoais europeu (RGPD) a respeito de como e quais informações deveriam ser fornecidas por controladores de dados responsáveis por esses sistemas.[27]

Nesse sentido, de modo a traduzir a inclusão de tais noções de transparência no texto do Anteprojeto, propõe-se as seguintes alterações:

Redação atual

Art. 25. Os sistemas responsáveis por decisões automatizadas a que se referem os artigos 23 e 24 devem ser auditáveis, não discriminatórios e passíveis de comprovação acerca de sua precisão e grau de acurácia.

(...)

§3º É garantido ao titular o direito de solicitar a revisão da decisão por uma pessoa natural.

Redação sugerida

Art. 25. Os sistemas responsáveis por decisões automatizadas a que se referem os artigos 23 e 24 devem ser auditáveis, não discriminatórios e passíveis de comprovação acerca de sua precisão e grau de acurácia.

(...)

§ 3º É garantido ao titular o direito de solicitar a revisão da decisão por uma pessoa natural, **bem como de requerer explicações a respeito do processo de tomada de decisões automatizadas específicas que afetem o exercício de seus direitos ou que possuam fundados indícios de terem sido feitas de forma equivocada.**

§ 5º O pedido de fornecimento de explicações a respeito do processo de tomada de decisões automatizadas específicas será dirigido à autoridade competente para avaliação de seu cabimento, com possibilidade de recurso ao Conselho Nacional de Justiça.

paper, 2017. Available at nrs.harvard.edu/urn-3:HUL.InstRepos:34372584. Accessed on 11 December 2020.

[27]Para mais informações a respeito dessa discussão no contexto europeu, vide WACHTER, S; MITTELSTADT, B; FLORIDI, L. **Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation**. IDPL, n. 76, 2017 e SELBST, Andrew D. & POWLES, Julia. **Meaningful Information and the Right to Explanation**. International Data Privacy Law, vol. 7(4), 2017, pp. 233-242. Disponível em: https://ssrn.com/abstract=3039125. Acesso em 26 ago 2020.

§ 6º As explicações de decisões automatizadas específicas de que trata o parágrafo anterior poderão ser fornecidas, caso possam afetar a condução de investigação policial, exclusivamente ao Conselho Nacional de Justiça, que avaliará e informará o titular de dados a respeito da compatibilidade de tais explicações com o exercício dos direitos e princípios previstos nesta lei.

Redação atual

Art. 26 (...)

§ 3º Os parâmetros a serem considerados na auditoria prevista no § 2º contemplarão, entre outros:
I - a precisão, incluindo a taxa de falsos positivos ou falsos negativos;
II - a reprodutibilidade e disponibilidade de documentação acerca do seu funcionamento;

Redação sugerida

Art. 26 (...)

§ 3º Os parâmetros a serem considerados na auditoria prevista no § 2º contemplarão, entre outros:

I - a precisão, incluindo a taxa de falsos positivos ou falsos negativos;
II - a reprodutibilidade e disponibilidade de documentação acerca do seu funcionamento;
III - o grau de interpretabilidade do sistema, de modo a permitir à auditoria a compreensão dos critérios e dos procedimentos utilizados para a realização de uma decisão automatizada.

III - Do Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

O presente capítulo diz respeito a um dos instrumentos mais importantes para a efetivação do direito à proteção de dados pessoais. Por essa razão, faz-se necessário detalhar e prescrever a forma e o conteúdo do RIPD e ter esses preceitos todos organizados num único capítulo. Este título, portanto, delineia a forma de fazê-lo.

[arts. 13, 23, 24] Inclusão de prescrições mais detalhadas às autoridades competentes sobre a formulação do RIPD;

[arts. 25 e 26] Estruturação mais detalhada de mecanismos de transparência de sistemas de decisão automatizada.

O relatório de impacto à proteção de dados (RIPD) pode ser definido como um processo para a avaliação dos impactos sobre a privacidade e sobre a proteção de dados gerados por um projeto, política, programa, serviço, produto ou outra iniciativa. São feitos em consulta com as partes interessadas, de modo a impulsionar a adoção de medidas preventivas necessárias para evitar ou minimizar os impactos negativos do tratamento de dados pessoais[28]. Com isso, passa-se de uma lógica pautada em medidas meramente reativas a violações à privacidade e à proteção de dados para medidas preventivas aos riscos para esses direitos[29].

Essa mudança de paradigma é significativa sobretudo em um contexto de crescente desconfiança pública acerca das novas tecnologias[30], principalmente sobre aquelas relacionadas ao tratamento massivo de dados e intrusivas à privacidade,

[28] DE HERT, Paul; DARIUSZ, Kloza; WRIGHT, David. **Recommendations for a Privacy Impact Assessment Framework for the European Union**. Brussels – London, 2012, p.5. Disponível em: https://piafproject.wordpress.com/. Acesso em: 18 de dez. 2020.

[29] DARIUSZ, Kloza. **Privacy Impact Assessment as a Means to Achieve the Objectives of Procedural Justice**. Jusletter IT. Die Zeitschrift für IT und Recht, 2014, p.2. Disponível em: https://cris.vub.be/en/publications/privacy-impact-assessments-as-a-means-to-achieve-the-objectives-of-procedural-justice(7b7e11e7-641d-4d56-aebf-3e0e7522f7b9).html. Acesso em: 16 de dez. 2020.

[30] Nesse sentido, ver: CONGER, Kate; FAUSSET, Richard; KOVALESKI, Serge. **San Francisco Bans Facial Recognition Technology.** New York Times, 2019. Disponível em: https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html. Acesso em: 11 de jan. 2021; BBC NEWS. **Facial recognition**: EU considers ban of up to five years. 2020. Disponível em: https://www.bbc.com/news/technology-51148501. Acesso em: 13 de jan. 2020.

utilizadas tanto por agentes públicos como privados[31]. Portanto, os RIPD são considerados como verdadeiras ferramentas de responsabilização e prestação de contas[32].

Além da função de prevenir riscos aos direitos dos indivíduos, os RIPD são instrumentos para a redução dos custos de implementação de projetos que envolvem o tratamento de dados pessoais[33]. Isso porque as avaliações de risco têm o condão de detectar potenciais ameaças, possibilitando o desenvolvimento de salvaguardas antes dos gastos para a efetiva implementação do projeto. Assim, reduz-se custos referentes, por exemplo, ao gerenciamento do tempo e à conformidade com as normas.

Sob um ponto de vista pragmático, a elaboração de RIPD com efetiva participação dos atores envolvidos, como os titulares dos dados e as autoridades de controle, possibilita uma boa relação entre tais sujeitos. Isso permite a compreensão de suas perspectivas, previne relações públicas negativas, evita a perda de reputação e atrai a confiança pública[34].

No entanto, **é imprescindível que o ordenamento jurídico estipule procedimentos mínimos a serem adotados pelas autoridades competentes**, a fim de maximizar os benefícios de uma abordagem preventiva. Tal atuação é representada justamente pela adoção sistemática de relatórios de impacto à proteção de dados pessoais.

Aliás, no contexto em que o Anteprojeto se insere, a exigência desses procedimentos mínimos está diretamente relacionada à concreção dos próprios fundamentos da disciplina da proteção de dados pessoais em atividades de segurança pública. A efetiva observância dos fundamentos expressos no art. 2º, inciso VII do Anteprojeto - devido processo legal, ampla defesa, contraditório, motivação e reserva

---

[31] CLARKE, Roger. **Privacy Impact Assessment**: Its Origins and Development. Computer Law & Security Review, vol. 25 ed. 2ª, 2009, p. 123–135. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0267364909000302?via%3Dihub. Acesso em: 23 de dez. 2020.

[32] DARIUSZ, Kloza. *opt. cit*, p. 6.

[33] WRIGHT, David. 2012. **The State of the Art in Privacy Impact Assessment**. Computer Law & Security Review vol. 28 ed. 1ª, 54–61, p.55. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S026736491100183X. Acesso em: 5 de jan. 2021.

[34] DARIUSZ, Kloza. *opt. cit*, p. 6.

legal - depende de que os atores envolvidos compreendam o processo que culmina na tomada de decisões que afetam seus direitos.

Contudo, o Anteprojeto apresenta menções esparsas e sujeitas a ambiguidades acerca dos procedimentos a serem seguidos pelas autoridades competentes para a realização de RIPD. O art. 29, que estipula as hipóteses de obrigatoriedade e alguns componentes mínimos dos relatórios, seria a única exceção.

A título de exemplo, por vezes é previsto que a autoridade competente deverá somente elaborar e informar ao Conselho Nacional de Justiça (CNJ)[35] a elaboração do RIPD (art. 13). Em outros dispositivos, afirma-se que o relatório também deverá ser publicado e posteriormente examinado pelo CNJ para decidir se o tratamento poderá ou não ser realizado (art. 23). Além disso, estão ausentes parâmetros claros e precisos sobre, por exemplo, o momento de elaboração, a forma de divulgação e os meios pelos quais os atores poderão participar.

Portanto, sugere-se (i) que **a normatização o RIPD seja concentrada em um capítulo próprio**, com vistas a favorecer a sistematização, bem como (ii) seja adotada uma **abordagem mais prescritiva** com relação a quatro pontos principais, quais sejam[36]:

1. Continuidade - RIPD como processo

Porquanto o objetivo dos RIPD seja evitar ou minimizar os impactos negativos sobre a privacidade e sobre a proteção de dados pessoais, essas avaliações devem ser operacionalizadas antes, durante e mesmo após a implementação de projetos que tenham como objetivo o tratamento de dados pessoais. Primeiro porque eventuais ameaças aos direitos dos titulares também são noticiadas após a efetiva

---

[35] O CNJ, através de uma unidade específica a ser criada através da futura lei, foi designada pelo Anteprojeto como autoridade supervisora de proteção de dados à segurança pública. Esta Nota Técnica, em seu Capítulo VI, discute essa escolha. Caso a futura lei decida por outro órgão para cumprir o papel de autoridade supervisora, as recomendações deste capítulo continuam válidas para ele.

[36] Nesse sentido, tomou-se como base os elementos definidos no projeto "A Privacy Impact Assessment Framework for data protection and privacy rights", financiado pela União Europeia e destinado a incentivar a UE e os seus Estados-Membros a adotarem uma política progressiva de avaliação do impacto na privacidade como meio de dar resposta às necessidades e desafios relacionados com a privacidade e a proteção de dados pessoais. Para mais informações: https://piafproject.wordpress.com/.

implementação do tratamento. Em segundo lugar, progressivamente novas tecnologias são disponibilizadas e, com elas, novos riscos também estão presentes. Portanto, não basta que o texto da Lei preveja as hipóteses de obrigatoriedade, **é preciso prescrever quando as avaliações serão realizadas e atualizadas**. Nesse sentido, sugere-se que o Anteprojeto de Lei preveja que os controladores atualizem os RIPD:

I - anualmente;

II - quando da ocorrência de modificações substanciais na forma de realização de tratamento de dados, se comparados com o descrito no RIPD anterior;

III - após detecção de incidentes de segurança;

IV- quando solicitado pela autoridade competente, sob devida justificativa.

2. Contextualidade - RIPD voltado às circunstâncias do tratamento

Além de ser um projeto em constante aprimoramento, a elaboração do RIPD envolve uma análise detida das particularidades do contexto em que está envolvido o tratamento de dados pessoais que se pretende implementar. No particular da proteção de dados em matéria penal, lida-se diretamente com o direito de ir e vir e, por isso, avaliações equivocadas dos riscos envolvidos podem gerar repercussões imediatas nas esferas individuais dos titulares.

Por isso, em termos práticos, o texto da futura lei deve prever **critérios mínimos a serem observados pelas autoridades competentes no momento de realização da avaliação de riscos**[37], tais como:

I - a descrição da natureza dos dados pessoais tratados;

II - as finalidades específicas do tratamento;

[37] Nesse sentido, ver sugestões elaboradas pela Associação Data Privacy Brasil que foram incluídas em parte nesta nota técnica: BIONI, Bruno; EILBERG, Daniela Dora; CUNHA, Brenda; SALIBA, Pedro; VERGILI, Gabriela. **Proteção de dados no campo penal e de segurança pública**: nota técnica sobre o Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2020.

III - a metodologia utilizada para a coleta e para a garantia da segurança das informações;

IV - os agentes de tratamento de dados envolvidos; e

V - a quantidade de titulares de dados potencialmente atingidos.

3. Responsabilidade – RIPD como legitimação do processo de tratamento de dados

Responsabilidade, no contexto do RIPD, significa não apenas adotar e implementar as medidas de salvaguardas, como também ter a capacidade de demonstrar, caso solicitado, que as medidas foram adotadas no caso concreto. Essa dupla faceta da responsabilidade das autoridades competentes insere-se em um contexto no qual a decisão final baseada no processo de tratamento de dados deve ser minimamente auditável. Portanto, é necessário que **a autoridade supervisora não somente seja informada da existência do RIPD**, como prevê o art. 13, **mas também analise o RIPD nos casos de tratamento automatizado** para que se proceda com a autorização do tratamento.

4. Transparência – RIPD como interação entre os agentes interessados

Para a concreção dos fundamentos da disciplina da proteção de dados em atividades de segurança pública e de persecução penal, dispostos no art. 2º, inciso VII do Anteprojeto, os processos de tomada de decisão devem ser transparentes. Isso envolve a divulgação de informações referentes aos RIPD. Neste sentido, exige-se transparência em dois principais aspectos: (i) sobre o processo de avaliação em si e (ii) sobre os resultados da avaliação. Portanto, o texto da futura lei deve dispor de **medidas a serem tomadas pelas autoridades competentes para garantir a transparência das informações relevantes aos atores envolvidos, a exemplo da publicação dos respectivos RIPD nos sites institucionais das autoridades**.

Portanto, ao invés de menções esparsas ao RIPD, sugere-se um capítulo específico para sistematizar a disciplina. Os atuais arts. 13, 23, 24, 26 e 29 teriam suas **menções ao RIPD remetidas a um capítulo específico localizado entre os capítulos referentes às tecnologias de monitoramento e ao compartilhamento de dados**. Se

mantida a redação como está atualmente, o capítulo para RIPD seria, portanto, o capítulo VIII do Anteprojeto. Por fim, e para facilitar a compreensão da tabela, remetemos os artigos esparsos que se referem ao RIPD para o capítulo específico sob a seguinte nomenclatura: X, X+1, X+2, etc., já que não se sabe ao certo a numeração dos artigos no novo capítulo sugerido.

Redação atual

Art. 13. O tratamento de dados pessoais sensíveis somente poderá ser realizado por autoridades competentes se estiver previsto em lei, observadas as salvaguardas desta Lei.

Parágrafo único. A autoridade competente responsável pelo tratamento de dados pessoais sensíveis elaborará relatório de impacto à proteção de dados pessoais **e informará ao Conselho Nacional de Justiça.**

Redação sugerida

Art. 13. O tratamento de dados pessoais sensíveis somente poderá ser realizado por autoridades competentes se estiver previsto em lei, observadas as salvaguardas desta Lei.

Parágrafo único. A autoridade competente responsável pelo tratamento de dados pessoais sensíveis elaborará relatório de impacto à proteção de dados pessoais **nos termos dos artigos X e seguintes.**

Conforme sugestão para novo capítulo

Redação atual

Art. 23. As decisões tomadas com base no tratamento automatizado de dados pessoais, que afetem os interesses do titular, devem ser precedidas de autorização do Conselho Nacional de Justiça e **de publicação de relatório de impacto, que comprove a adoção das garantias adequadas para os direitos e liberdades do titular, incluído o direito de solicitar a revisão da decisão por uma pessoa natural e observado o disposto no artigo 25.**

(...)

§1º O relatório de impacto à proteção de dados pessoais deve ser publicado na página da autoridade competente e enviado ao Conselho Nacional de Justiça, demonstrando as garantias para a proteção dos direitos e liberdades do titular requeridas no caput, que deverão ser adequadas à natureza dos dados tratados.

§2º O Conselho Nacional de Justiça deverá examinar o relatório de impacto e decidir acerca da possibilidade da decisão automatizada com base no tratamento automatizado de dados, à luz das garantias para os direitos e liberdades do titular e dos riscos apresentados.

Redação sugerida

Art. 23. As decisões tomadas com base no tratamento automatizado de dados pessoais, que afetem os interesses do titular, devem ser precedidas de autorização do Conselho Nacional de Justiça **e ser objeto de relatório de impacto nos termos dos artigos X e seguintes.**

Conforme sugestão para novo capítulo

O texto dos §§ 1º e 2º do art. 23 deve ser remetido ao novo capítulo sobre RIPD. *Seu conteúdo se incorporará ao texto dos artigos sugeridos.*

Redação atual

Art. 24. (...)

§ 2º O controlador elaborará relatório de impacto de proteção de dados pessoais à luz das circunstâncias concretas do tratamento em questão.

§ 3º O Conselho Nacional de Justiça deverá examinar o relatório de impacto e decidir acerca da possibilidade da decisão automatizada com base no tratamento automatizado de dados, às luz das garantias para os direitos e liberdades do titular frente aos riscos apresentados

Redação sugerida

Art. 24. (...)

§ 2º O controlador elaborará relatório de impacto de proteção de dados pessoais à luz das circunstâncias concretas do tratamento em questão, **nos termos dos artigos X e seguintes.** *Conforme sugestão para novo capítulo.*

O texto do §3º do art. 24 deve ser remetido ao novo capítulo sobre RIPD.
Seu conteúdo se incorporará ao texto dos artigos sugeridos.

Redação atual

Art. 26. O relatório de impacto à proteção de dados que fundamentar decisões automatizadas nos termos desta lei verificará, entre outros, as medidas tomadas para a garantia da não-discriminação e transparência.

Redação sugerida

O texto do art. 26, incluindo caput e parágrafos, deve ser remetido ao novo capítulo sobre RIPD.

Seu conteúdo se incorporará ao texto dos artigos sugeridos.

Redação atual

Art. 29. É obrigatória a elaboração de relatório de impacto à proteção de dados pessoais para tratamento de dados pessoais sensíveis, sigilosos, ou em operações que apresentem elevado risco aos direitos, liberdades e garantias dos titulares de dados.

(...)

Redação sugerida

O texto integral do art. 29, incluindo caput e parágrafos, deve ser remetido ao novo capítulo sobre RIPD.

Seu conteúdo se incorporará ao texto dos artigos sugeridos.

Estruturação do Capítulo reservado ao RIPD	
Redação sugerida para novo capítulo	**Observações**
CAPÍTULO ( ) DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS	Sugere-se a inclusão do novo capítulo entre aqueles referentes às tecnologias de monitoramento (atualmente Capítulo VII) e ao compartilhamento de dados (atualmente capítulo VIII).
Art. X. É obrigatória a elaboração de relatório de impacto à proteção de dados pessoais para tratamento de dados pessoais sensíveis, sigilosos, ou em operações que apresentem elevado risco aos direitos, liberdades e garantias dos titulares de dados**, incluindo, mas não se limitando a, tratamento de dados que:** **I. Envolva decisões tomadas com base em tratamento automatizado que afete os interesses dos titulares;** **II.Envolva o uso de tecnologias de monitoramento** **III. Envolva o uso de novas tecnologias** § 1º **A autoridade supervisora poderá, a qualquer**	O texto deste artigo tem como base o atual **art. 29** do Anteprojeto de Lei, acrescido de sugestões de redação pelo LAPIN. As sugestões ao texto original do art. 29 estão marcadas em negrito.

momento e independente dos critérios descritos no caput, determinar ao controlador que elabore **e publique** relatório de impacto à proteção de dados pessoais, referente a quaisquer das suas operações de tratamento de dados.

§ 2º A elaboração e apresentação de relatório de impacto à proteção de dados pessoais também poderá ser requisitada pelo Ministério Público e pela Defensoria Pública na defesa de direitos individuais ou coletivos, quando cabível no exercício de suas atribuições.

§ 3º. Os relatórios de impacto elaborados por autoridades competentes responsáveis por tratamento de dados pessoais, cuja finalidade seja a realização de atividades de segurança pública e de persecução penal, deverão ser enviados à autoridade supervisora.

§ 4º. Observado o disposto no caput deste artigo, o relatório de impacto à proteção de dados deve ser atualizado:
I - anualmente;
II - quando da ocorrência de modificações substanciais na forma de realização de tratamento de dados, se comparados com o descrito no relatório de impacto anterior;
III - após detecção de incidentes de segurança; e
IV - quando solicitado pela autoridade competente, sob devida justificativa.

§ 5º. Observado o disposto no caput deste artigo, o relatório de impacto a proteção de dados deverá conter, no mínimo:
I - a descrição da natureza dos dados pessoais tratados;
II - as finalidades específicas do tratamento;
III - a metodologia utilizada para a coleta e para a garantia da segurança das informações
IV - **os agentes** de tratamento de dados envolvidos;
V - a quantidade de titulares de dados potencialmente atingidos;
VI - se houver, informação sobre nova utilização de algum

tipo tecnologia; VII - informação sobre a possibilidade de tratamento discriminatório; VIII - as expectativas legítimas do titular de dados; IX - a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados; e **X - com quem são compartilhados os dados advindos do tratamento.**	
Art. X+1. O relatório de impacto à proteção de dados verificará, entre outros, as medidas tomadas para a garantia da não-discriminação e transparência. § 1º Os parâmetros para verificação da natureza discriminatória contemplarão o peso de dados pessoais, incluindo aqueles referentes à situação socioeconômica e os dados demográficos relacionados ao local de residência ou os demais, sejam potencialmente capazes de revelar informações sensíveis. § 2º No caso de relatório de impacto que fundamente decisões automatizadas, os sistemas responsáveis pelas decisões devem ser auditáveis nos termos a serem determinados pela autoridade supervisora, que não serão restringidos pelo segredo industrial e comercial. § 3º Os parâmetros a serem considerados na auditoria prevista no § 2º contemplarão, entre outros: I - a precisão, incluindo a taxa de falsos positivos ou falsos negativos; II - a reprodutibilidade e disponibilidade de documentação acerca do seu funcionamento.	O texto deste artigo tem como base o atual **art. 26** do Anteprojeto de Lei, acrescido de sugestões de redação pelo LAPIN. As sugestões ao texto original do art. 26 estão marcadas em negrito.
Art. X+2. O relatório de impacto referente ao tratamento de dados de elevado risco ou que utilize tecnologias de monitoramento deve conter, além dos requisitos do §5º do art. X, no mínimo: I - uma descrição do escopo do tratamento e das	A redação do caput é uma sugestão integral do LAPIN. Este artigo se refere também à possibilidade de decisão automatizada

capacidades da tecnologia de monitoramento; II - testes ou relatórios relativos aos efeitos do tratamento e da tecnologia de monitoramento na saúde e na segurança de pessoas; III – descrição dos impactos potencialmente díspares do tratamento de dados e da tecnologia de monitoramento ou de sua política de uso em quaisquer populações específicas; IV - as medidas previstas para fazer frente aos riscos mencionados nos incisos anteriores; V - as garantias, as medidas de segurança e os mecanismos para assegurar a proteção dos dados pessoais e demonstrar a conformidade do tratamento com a presente lei; e VI - a política de uso e as garantias dos direitos dos titulares. **Parágrafo único - Dentre outras, considera-se atividade de tratamento de dados de elevado risco:** **I - definição do risco de envolvimento em infração penal ou de reincidência do titular do dado pessoal por meio do uso de sistemas de decisões automatizadas;** **II – criação de perfil comportamental do titular do dado;** **III - controle sistemático de áreas de grande circulação pública;** **IV - tratamento em larga escala de dados sensíveis;** **V - tratamento em larga escala de dados sigilosos.**	com base no tratamento automatizado de dados, mencionada nos **art. 23, § 2º e art. 24, § 3º.** Os incisos deste artigo proposto foram retirados do **§ 2º do art. 42** da atual redação do Anteprojeto de Lei. O parágrafo único é uma sugestão baseada no relatório da organização Data Privacy Brasil[38].
Art. X+3. As autoridades competentes responsáveis pelo tratamento de dados pessoais deverão publicar os relatórios de impacto em seu site oficial. **Parágrafo único. A autoridade supervisora poderá prever exceções ao disposto no caput.**	O texto deste artigo tem como base o atual **art. 23, §1º,** do Anteprojeto de Lei, acrescido de sugestões de redação pelo LAPIN.

[38] BIONI, Bruno; EILBERG, Daniela Dora; CUNHA, Brenda; SALIBA, Pedro; VERGILI, Gabriela. **Proteção de dados no campo penal e de segurança pública**: nota técnica sobre o Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2020.

IV - Das tecnologias de monitoramento e tratamento de dados de elevado risco

As tecnologias de monitoramento e tratamento de dados de elevado risco têm ganhado papel cada vez mais importante nas operações de segurança pública e investigação criminal. Por este motivo, elas também se destacam no Anteprojeto de Lei, tendo recebido um capítulo específico para sua regulação, o Capítulo VII.

O presente título analisa o tratamento dispensado pelo Anteprojeto a tais tecnologias e se divide em três subtítulos: dos parâmetros para a realização da análise de impacto regulatório; das tecnologias de monitoramento com identificação; e do relatório sobre o uso das tecnologias de monitoramento elaborado pela autoridade supervisora.

a. Dos parâmetros para a realização da análise de impacto regulatório

[art. 42] Inclusão de parâmetros para realização da análise de impacto regulatório (AIR) que indiquem a necessidade, adequação e proporcionalidade da adoção da tecnologia;

Justamente porque o uso das tecnologias dependerá de previsões legais específicas, a análise do seu impacto deve ser a mais abrangente possível. Os parâmetros para elaboração da análise de impacto regulatório (AIR) propostos pelo Anteprojeto de Lei no capítulo VII são muito importantes, mas podem ser complementados.

Sugere-se a **inclusão de requisitos voltados a refletir sobre a necessidade, adequação e proporcionalidade da adoção da tecnologia**[39]. Tais parâmetros refletiriam, respectivamente, a identificação do problema que se pretende solucionar, a indicação de potenciais alternativas para enfrentar a mesma questão, bem como os

[39] A título de exemplo, estas já são exigências previstas no Decreto Federal nº 10.411/2020, que regulamenta a análise de impacto regulatório para atividades econômicas que sejam objeto de normas editadas pela Administração Pública Federal.

impactos dessas alternativas. Dessa forma, o legislador teria que examinar não apenas o impacto do uso da tecnologia à proteção de dados, mas também por que ela não poderia ser substituída por outras opções e qual sua conformidade ao ordenamento jurídico em comparação com outras possibilidades.

Além disso, sugere-se a **previsão de que a autoridade supervisora seja consultada para indicar se a tecnologia a ser autorizada pela legislação específica estaria adequada ao texto da futura lei**. Tal opinião seria mais um fator necessário de cautela e precaução, em razão da natureza e possíveis riscos impostos por tecnologias de monitoramento.

Redação atual

Art. 42 (...)

§ 2º O processo legislativo será instruído de análise de impacto regulatório que contenha:

(...)

Redação sugerida

Art. 42 (...)

§ 2º O processo legislativo será instruído de análise de impacto regulatório que contenha:

(...)

VII - identificação do problema que se pretende solucionar, com a apresentação de suas causas e sua extensão;

VIII – descrição das alternativas possíveis ao enfrentamento do problema identificado, consideradas as opções de não ação, de soluções dependam de normas e de, sempre que possível, soluções não normativas;

IX – exposição dos possíveis impactos das alternativas identificadas, inclusive quanto aos seus custos;

X - opinião emitida pela autoridade supervisora sobre a adequação da tecnologia a esta lei.

b. Das tecnologias de monitoramento com identificação

[art. 43] Manutenção da vedação ao uso de tecnologias de monitoramento com identificação de forma massiva e contínua, nos termos já previstos no Anteprojeto, tendo em vista seu elevado risco de violações de direitos fundamentais e garantias constitucionais;

O Anteprojeto traz um dispositivo específico sobre o uso das tecnologias de vigilância que permitem a identificação de pessoas em tempo real. Além disso, ele pretende criar mecanismos adequados para mitigação de riscos de violação de direitos fundamentais de privacidade e liberdade. Segundo o art. 43, essas ferramentas tecnológicas apenas poderiam ser usadas quando houvesse autorização legal e judicial específica e quando ocorresse no âmbito da persecução penal individualizada. **Os parâmetros previstos pelo Anteprojeto são necessários para evitar a instauração de estado de vigilância e a violação de direitos fundamentais**.

Diante da peculiaridade de algumas tecnologias de vigilância, é mais adequado que elas sejam utilizadas apenas para fins de persecução penal, visto que essa atividade visa a investigação e a apuração de infrações penais já praticadas. É diferente da prevenção de cometimento de crimes contra a ordem pública, como ocorre na atividade de segurança pública.

Isso explica por que **não há necessidade de se utilizar essas tecnologias de monitoramento contínuo para identificar sujeitos que não praticaram nenhuma violação à lei penal**. Neste ponto, nota-se ainda mais como a atividade de persecução penal é diferente da de segurança pública em sentido estrito: naquela, há maiores indícios que justificam uma investigação individualizada e uma tentativa de identificação específica dos sujeitos de interesse da polícia.

Segundo o previsto no Anteprojeto, seria necessária a edição prévia de lei que autorize o uso dessas tecnologias e que o processo legislativo dessa lei observe os requisitos descritos em seu texto, como a produção de análise de impacto regulatório (AIR) prévia.

Além da lei específica, seria essencial uma **autorização judicial**. Esse requisito é um mecanismo para evitar que a utilização de sistemas de vigilância ocorra de

maneira discricionária ou desproporcional, além de respaldar o uso da tecnologia para momentos específicos, necessários e não massivos. Dessa forma, os riscos seriam mitigados pela atuação do magistrado como ator competente para julgar e conhecedor do caso concreto para autorizar uso da tecnologia. Um outro ponto relevante é que o processo judicial garante maior transparência na motivação do uso da tecnologia e evidencia os mecanismos legais para se opor ao uso no caso específico, se necessário.

A necessidade de autorização judicial prevista no Anteprojeto de Lei é similar ao determinado na *Section 11* da Lei ESSB 6280 do estado de Washington, Estados Unidos. Esta norma proíbe especialmente o uso da tecnologia de reconhecimento facial para sistemas de vigilância em tempo real ou de forma persistente, a menos que seja obtido o que se chama de *warrant*, que é um mandado específico que autorize o uso da tecnologia para essas finalidades, as circunstâncias exijam, ou haja ordem judicial para identificar pessoas perdidas ou consideradas mortas[40]. Dessa forma, a previsão de uma autorização judicial que permita o uso da tecnologias de identificação encontra precedente em legislação estrangeira, como é o caso de Washington.

Essas previsões são fundamentais, já que o uso irrestrito dessas tecnologias significa um elevado risco para direitos de privacidade e proteção de dados, permite a instauração de um estado de constante vigilância e dá poder para os Estados identificarem e vigiarem pessoas, mesmo que em atividades rotineiras e íntimas.

Ainda, é relevante pontuar que a possibilidade de monitorar a rotina dos cidadãos como um todo não contribui para alcançar a finalidade de gerar maior segurança pública para a sociedade. Isso ocorre porque as informações pessoais de milhares de pessoas seriam tratadas sem o enfoque necessário em pessoas consideradas, motivadamente, como sujeitos de interesse. Ainda, **não há nenhum estudo que comprove a utilidade e eficiência das tecnologias**, como o reconhecimento facial, em reduzir a violência e o impacto no cotidiano das pessoas que transitam pelos espaços que usam a tecnologia. Nesse sentido, nota-se que

[40]State of Washington. **ESSB 6280**. 2020. Disponível em: http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Passed%20Legislature/6280-S.PL.pdf?q=20200430142448. Acesso em: 21 jan. 2021.

grupos minoritários e estigmatizados devem ser os mais afetados pela uso dessas ferramentas, já que são frequentemente os maiores alvos dos usos de mecanismos de repressão[41].

Além disso, a vigilância em massa subverte o princípio da presunção da inocência, previsto no art. 5º, LVII, da Constituição Federal, segundo o qual determina que ninguém será considerado culpado antes da sentença penal condenatória. Autorizar em lei o estabelecimento de um processo de vigilância constante e irrestrito como regra coloca todas as pessoas que circulam numa determinada região como possíveis criminosas, ou pelo menos suspeitas, o que é uma quebra do princípio constitucional supracitado. Esta questão é ainda mais sensível se considerado o uso de ferramentas de identificação de pessoas, de forma que, além de saber que alguém frequenta um local rotineiramente, seria possível identificá-la, relacionando tal informação a outros dados contidos em bases distintas, como nome ou endereço residencial.

Logo, se houver a necessidade de se utilizar tecnologias de monitoramento, essas devem ser usadas para casos específicos, com autorização legal e judicial, para que sejam concretizados os mecanismos de minimização de riscos e violações de direitos fundamentais. Diante dos riscos, o art. 43 do Anteprojeto pretende estabelecer salvaguardas necessárias e se manter genérico sobre as tecnologias de vigilância que possibilitam a identificação. Isso é importante, já que o desenvolvimento tecnológico é uma constante e, se a previsão fosse específica para alguns sistemas tecnológicos, logo ela estaria obsoleta e não aplicável à evolução dos instrumentos de reconhecimento e identificação de pessoas.

Um exemplo concreto de aplicação dessas salvaguardas é o caso das tecnologias de reconhecimento facial (TRF). A informação tratada por TRF é dado biométrico[42], o que significa que a tecnologia permite a identificação e autenticação

---

[41] RONDON FILHO, Edson Benedito. **Polícia e minorias**: estigmatização, desvio e discriminação. DILEMAS - Vol. 6 - nº 2 - ABR/MAI/JUN 2013 - pp. 269-293. p. 290

[42] Dados biométricos são aqueles relacionados a características físicas que distinguem indivíduos. Geralmente, tais características são únicas e relativamente difíceis de serem modificadas, especialmente a curto prazo. São dados biométricos, por exemplo, a impressão digital, a voz, a retina, o DNA e as características faciais. Para mais informações, ver: UFRJ. O que é biometria. 2007. Disponível em: https://www.gta.ufrj.br/grad/07_2/eliseu/Oquebiometria..html. Acesso em: 02 mar. 2021.

de pessoas baseada em um conjunto de informações únicas e específicas para cada pessoa[43]. Neste sentido, a informação facial é um dado personalíssimo e singular de cada pessoa, como as digitais dos dedos, a íris dos olhos e o DNA.

De acordo com a LGPD, um dado biométrico, quando vinculado a uma pessoa natural, é um dado sensível (art. 5º, II). Com isso, a legislação prevê um tratamento especial para os dados pessoais sensíveis, já que, caso esses "sejam conhecidos e submetidos a tratamento, podem se prestar a uma potencial utilização discriminatória ou lesiva e que apresentaria maiores riscos potenciais do que outros tipos de informação"[44].

Não é de forma alguma comprovado que o uso de TRF para a manutenção de segurança pública seja de fato eficaz. **Os riscos identificados no uso da tecnologia levantaram questionamentos em diversas experiências internacionais.** Na cidade de São Francisco, nos Estados Unidos, o órgão governamental competente baniu TRF, visto o seu alto potencial de uso abusivo e a consequência de uma vigilância opressiva e massiva[45].

Em outro momento, após o início do movimento *Black Lives Matter* nos EUA em 2020, a IBM, uma das maiores empresas de tecnologia do mundo, anunciou que deixaria de investir em TRF. Segundo a empresa, esse instrumento é usado, majoritariamente, para controle social e opressão pelas forças policiais[46].

---

[43] THALES. **Biometrics**: authentication & identification (definition, trends, use cases, laws and latest news) - 2020 review. 2020. Disponível em: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics. Acesso em: 5 mai. 2020.

[44] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019. p. 143

[45] CONGER, Kate; FAUSSET, Richard. KOVALESKI, Serge. **San Francisco Bans Facial Recognition Technology**. 2019. Disponível em: https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html. Acesso em: 5 mai. 2020.

[46] IBM. **IBM CEO's Letter to Congress on Justice Reform**. 2020. Disponível em: https://www.ibm.com/blogs/policy/facial-recognition-sunset—justice-reforms/. Acesso em: 5 set. 2020.

No contexto europeu, várias organizações da sociedade civil, como a Access Now e o Article 19, uniram-se para defender o banimento do uso de tecnologias de vigilância que utilizam dados biométricos[47].

Nessa perspectiva, o impacto do tratamento indevido de dados faciais é significativo e os riscos de violação de direitos e liberdades individuais são elevados. Ainda, o mau uso dos dados, quando as finalidades do processamento estão no âmbito da segurança pública, geram efeitos mais gravosos, já que o direito penal é *ultima ratio* e é prerrogativa do Estado contra atitudes extremas dos cidadãos.

A situação se agrava considerando que a tecnologia tem vieses que fazem com que pessoas negras sejam mais suscetíveis a erros de identificação do que pessoas brancas, o que revela uma **tendência racista** desses sistemas. Além disso, seu uso no Brasil com fundamento em bases de dados de indivíduos procurados pela Justiça acaba por reproduzir ainda mais o histórico de seletividade do sistema penal no Brasil, que historicamente encarcera mais pessoas negras do que brancas[48].

Isso sem contar em como o uso de reconhecimento facial também afeta os direitos de **pessoas transgênero e não-binárias**. Essa tecnologia, ao classificar pessoas como pertencentes somente a dois gêneros, masculino ou feminino, reforça a exclusão e o estigma desses indivíduos, conflitando com a auto-identificação de gênero[49], acirrando violências e reiterando o cerceamento de direitos às pessoas transgênero e não-binárias.

Dessa forma, **os três critérios introduzidos no Anteprojeto de Lei - autorização legislativa e judicial, e atuação apenas para persecução penal - são relevantes para**

---

[47] Nesse sentido, o European Digital Rights, coalização de diversas organizações da sociedade civil que defende direitos humanos e digitais, afirma que uso de tecnologias biométricas para o monitoramento de pessoas em massa não direcionado pelo tratamento de dados pessoais, em particular dados biométricos, em locais públicos, cria sérios riscos de vigilância em massa, para mais detalhes, consulte este link: https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf. Ainda, foi criado o movimento #ReclaimYourFace para a defesa dos direitos humanos digitais pelo banimento de tecnologias de vigilância em massa na Europa, a campanha está veiculada neste link: https://reclaimyourface.eu/the-movement/.

[48] DA SILVA, Rosane Leal & DA SILVA, Fernanda dos Santos Rodrigues. **Reconhecimento Facial e Segurança Pública:** os Perigos do Uso da Tecnologia no Sistema Penal Seletivo Brasileiro. 5º Congresso Internacional de Direito e Contemporaneidade: mídias e direitos da sociedade em rede (2019). Disponível em https://www.ufsm.br/app/uploads/sites/563/2019/09/5.23.pdf. Acesso em: 23 mar. 2021.

[49] CODING RIGHTS. Reconhecimento Facial no Setor Público e Identidades Trans. Disponível em: https://codingrights.org/docs/rec-facial-id-trans.pdf. Acesso em: 28 fev. 2021.

criar parâmetros de um uso razoável da tecnologia sem tornar esses critérios obsoletos com o passar do tempo. Faz-se fundamental o estabelecimento de critérios objetivos no uso de tecnologias que possibilitam a identificação de pessoas, diante do elevado risco a violações de direitos fundamentais e garantias constitucionais sobre o processo penal.

Redação atual

Art. 43. No âmbito de atividades de segurança pública, é vedada a utilização de tecnologias de vigilância diretamente acrescida de técnicas de identificação de pessoas indeterminadas em tempo real e de forma contínua quando não houver a conexão com a atividade de persecução penal individualizada e autorizada por lei e decisão judicial.

Redação sugerida

Manutenção integral do texto do art. 43.

c. Do relatório sobre o uso das tecnologias de monitoramento elaborado pela autoridade supervisora

[art. 44] Previsão de publicação de relatório, pela autoridade supervisora, acerca do uso de tecnologias de monitoramento não mais anualmente, mas a cada seis meses;

O art. 44 do Anteprojeto de Lei pretende estabelecer que uma das atribuições do CNJ, enquanto autoridade supervisora, será o acompanhamento quanto à utilização de tecnologias de vigilância ou o tratamento de dados pessoais que representem elevado risco para direitos, liberdades e garantias dos titulares dos dados. Esse acompanhamento seria concretizado por meio de recomendações, opiniões técnicas, relatórios e auditorias realizadas pelo CNJ. Esses instrumentos,

previstos no Anteprojeto, seriam relevantes para pesquisas sobre a utilidade e eficiência da tecnologia no apoio às forças policiais.

O Anteprojeto de Lei prevê que o CNJ emita relatório anual sobre o uso de tecnologias de monitoramento pelas autoridades competentes em âmbito nacional. No entanto, sugere-se que **a publicação desse documento ocorra semestralmente**, considerando a constante evolução da tecnologia, as peculiaridades regionais brasileiras e a relevância desses relatórios para o acompanhamento da sociedade civil sobre o tratamento de dados para segurança pública e persecução penal.

Redação atual

Art. 44.

(...)

§ 1º O Conselho Nacional de Justiça deverá publicar **relatório anual** acerca do uso de tecnologias de monitoramento pelas autoridades competentes no território nacional.

Redação sugerida

Art. 44.

(...)

§ 1º O Conselho Nacional de Justiça deverá publicar **relatório semestral** acerca do uso de tecnologias de monitoramento pelas autoridades competentes no território nacional.

V - Da transferência internacional de dados

A transferência internacional de dados, conforme definição da LGPD, é a "transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro"[50]. No âmbito da segurança pública e persecução penal, a transferência ganha contornos ainda mais relevantes tanto em relação à natureza dos dados e à repercussão na esfera individual quanto à possibilidade de combate a crimes de maneira internacional. Assim, é necessário que os termos e condições para transferências internacionais estejam claramente definidos.

Este capítulo se divide em: da alternatividade ou cumulação das condições para transferência internacional; da adequação dos termos; dos critérios para análise das garantias em transferências internacionais; e da obrigatoriedade de comunicação ao CNJ de ocorrência de transferência internacional.

a. Da alternatividade ou cumulação das condições para transferência internacional

[arts. 53 e 57] Definição se as condições para a realização de transferências internacionais de dados são cumulativas ou alternativas;

Enquanto o nível de proteção trazido pelo Anteprojeto é satisfatório em uma análise comparativa com o marco legal europeu, tendo sido clara a influência da Diretiva (UE) 2016/680 e da Lei nº 59/2019 de Portugal na sua elaboração, a adoção de alguns termos, redações de dispositivo e dinâmicas de troca de informações merecem ser adaptadas para o contexto brasileiro.

O primeiro ponto se encontra no **art. 53**, que trata das condições exigidas para a execução de uma transferência de dados para outro país ou organização internacional. A leitura do artigo e de seus incisos não deixa claro **se há relação de cumulatividade ou alternatividade entre os incisos, em especial entre o inciso V e VI**. Por isso, não é

[50] Lei nº 13.709/2018, Lei Geral de Proteção de Dados. Art. 5º, XV.

inteligível se é necessário que todas as condições estejam presentes para que haja uma transferência internacional de dados ou se apenas algumas delas. Uma mudança de redação do *caput* para tornar mais claro o funcionamento do artigo é oportuna. Para garantir mais salvaguardas para transferências internacionais, sugere-se a adoção da cumulatividade das condições.

A mesma situação aparece no **art. 57**, que trata das condições necessárias para realização de transferência direta de dados para destinatário que se encontre no exterior. Apesar de o texto do artigo deixar explícita a cumulatividade, não está claro **se os incisos são todos cumulativos entre si ou se apenas entre cada um deles e o inciso V**. Assim, sugere-se alterar sua redação para torná-la mais compreensível.

Redação atual

Art. 53. Sem prejuízo de outras condições exigidas em lei, as autoridades competentes só podem transferir dados pessoais para outro país ou para uma organização internacional, inclusive dados que se destinem a transferências ulteriores para outro país ou outra organização internacional, se:

(...)

Redação sugerida

Art. 53. Sem prejuízo de outras condições exigidas em lei, as autoridades competentes só podem transferir dados pessoais para outro país ou para uma organização internacional, inclusive dados que se destinem a transferências ulteriores para outro país ou outra organização internacional, **se preenchidas, cumulativamente, as seguintes condições:**

(...)

Redação atual

Art. 57. Em derrogação do disposto do inciso III do artigo 53 e sem prejuízo de um acordo internacional tal como definido no §1º deste artigo, autoridade pública com poderes de prevenção, investigação, detecção ou repressão de infrações penais ou de execução de sanções penais, incluindo a prevenção de ameaças à segurança pública, pode, em casos específicos, transferir dados pessoais diretamente a destinatários estabelecidos em outros países desde que, respeitadas as disposições da presente lei, estejam preenchidas as seguintes condições cumulativas:

(...)

Redação sugerida

Art. 57. Em derrogação do disposto do inciso III do artigo 53 e sem prejuízo de um acordo internacional tal como definido no §1º deste artigo, autoridade pública com poderes de prevenção, investigação, detecção ou repressão de infrações penais ou de execução de sanções penais, incluindo a prevenção de ameaças à segurança pública, pode, em casos específicos, transferir dados pessoais diretamente a destinatários estabelecidos em outros países desde que, respeitadas as disposições da presente lei, estejam preenchidas **todas as** seguintes condições, **de forma cumulativa:**

(...)

b. Da adequação dos termos

[arts. 53 e 55] Adequação dos termos que se referem ao controlador do tratamento;

[arts. 56 e 57] Adequação dos termos que se referem à cooperação jurídica internacional, limitando-a apenas ao âmbito penal

[art. 57] Explicitação de quem seria a autoridade de controle

Relativamente aos termos utilizados, tem-se, nos **arts. 53 e 55**, a **utilização do termo "responsável pelo tratamento" onde deveria ser lido "controlador"**, elemento impreciso que se repete em outras partes do Anteprojeto de Lei. Como forma de harmonizar os termos com outros já contidos em legislações vigentes, sugere-se a adoção do termo "controlador", conforme art. 5º, VI, da LGPD.

Outro ponto importante é a necessidade de clarificar alguns termos, como no caso do **art. 56, V, e art. 57, §1º**, que **falam de cooperação jurídica internacional ao invés de cooperação jurídica penal internacional**. Por se tratar de Anteprojeto que visa regular o uso de dados para a segurança pública e investigação criminal, é necessário restringir ao máximo sua aplicabilidade às matérias-alvo. Da forma como está, a redação pode abrir margem para entendimentos que alarguem a aplicabilidade

dos dispositivos para ações de cooperação que vão além do pretendido pelo Anteprojeto.

Além disso, o **§2º do art. 57** se refere apenas à autoridade de controle, não especificando qual órgão seria. Pela leitura sistemática da seção, contudo, infere-se que seja o Conselho Nacional de Justiça. Sugere-se, portanto, a alteração do dispositivo para "autoridade supervisora", de modo a melhor detalhar quem seria essa autoridade de controle.

Redação atual

Art. 53. Sem prejuízo de outras condições exigidas em lei, as autoridades competentes só podem transferir dados pessoais para outro país ou para uma organização internacional, inclusive dados que se destinem a transferências ulteriores para outro país ou outra organização internacional, se:

(...)

Redação sugerida

Art. 53. Sem prejuízo de outras condições exigidas em lei, as autoridades competentes só podem transferir dados pessoais para outro país ou para uma organização internacional, inclusive dados que se destinem a transferências ulteriores para outro país ou outra organização internacional, **se preenchidas, cumulativamente, as seguintes condições:**

(...)

Redação atual

Art. 55.

(...)

II - o **responsável pelo tratamento** tiver avaliado todas as circunstâncias inerentes à transferência de dados pessoais e concluído que existem garantias adequadas no que diz respeito à proteção desses dados.

§ 1º O **responsável pelo tratamento** informará o Conselho Nacional de Justiça sobre as categorias de transferências abrangidas pelo inciso II

Redação sugerida

Art. 55.

(...)

II - o **controlador** tiver avaliado todas as circunstâncias inerentes à transferência de dados pessoais e concluído que existem garantias adequadas no que diz respeito à proteção desses dados.

§ 1º O **controlador** do tratamento informará o Conselho Nacional de Justiça sobre as categorias de transferências abrangidas pelo inciso II

Redação atual

Art. 56.

(...)

V - em casos específicos, para a **cooperação jurídica internacional**, de acordo com regras e instrumentos de direito internacional.

Redação sugerida

Art. 56.

(...)

V - em casos específicos, para a **cooperação jurídica penal internacional**, de acordo com regras e instrumentos de direito internacional.

Redação atual

Art. 57

(...)

§ 1º Para os fins previstos no caput, por acordo internacional entende-se um acordo internacional bilateral ou multilateral em vigor entre o Brasil e o outro país no campo da **cooperação jurídica internacional** ou da cooperação policial.

§ 2º A autoridade competente que efetuar a transferência deve informar a **autoridade de controle** sobre as transferências realizadas na forma deste artigo.

Redação sugerida

Art. 57

(...)

§ 1º Para os fins previstos no caput, por acordo internacional entende-se um acordo internacional bilateral ou multilateral em vigor entre o Brasil e o outro país no campo da **cooperação jurídica penal internacional** ou da cooperação policial.

§ 2º A autoridade competente que efetuar a transferência deve informar ao **Conselho Nacional de Justiça, autoridade de controle**, sobre as transferências realizadas na forma deste artigo.

c. Dos critérios para análise de garantias em transferências internacionais

[art. 55] Inclusão de critérios para análise das garantias adequadas para transferências internacionais de dados

Sugerem-se, ainda, duas alterações na dinâmica de transferência internacional de dados. Uma das exigências para a transferência é que o receptor dos dados assegure nível adequado de proteção; entretanto, se ausente uma decisão que ateste tal adequação, o art. 55 prevê outras duas garantias. No que concerne à garantia prevista no inciso II, cabe dar maior clareza sobre **quais as circunstâncias que o controlador do tratamento terá que levar em conta para entender que foram colocadas em prática todas as garantias adequadas**. Dessa forma, sugere-se a inclusão de tais critérios no corpo do referido artigo.

Redação atual

Art. 55. Na falta de decisão de adequação, os dados pessoais podem ser transferidos para um país estrangeiro ou para uma organização internacional se:

(...)

II - o responsável pelo tratamento tiver avaliado todas as circunstâncias inerentes à transferência de dados pessoais e concluído que existem garantias adequadas no que diz respeito à proteção desses dados.

(...)

Redação sugerida

Art. 55. Na falta de decisão de adequação, os dados pessoais podem ser transferidos para um país estrangeiro ou para uma organização internacional se:

(...)

II - o responsável pelo tratamento tiver avaliado todas as circunstâncias inerentes à transferência de dados pessoais e concluído que existem garantias adequadas no que diz respeito à proteção desses dados.

(...)

§ 3º O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no caput do art. 55 desta Lei será avaliado pela autoridade de controle, que levará em consideração:

I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;

II - a natureza dos dados;

III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;

IV - a adoção de medidas de segurança previstas em regulamento;

V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e

VI - outras circunstâncias específicas relativas à transferência.

d. Da obrigatoriedade de comunicação ao CNJ de ocorrência de transferência internacional

[art. 55] Inclusão de obrigação de comunicação para o Conselho Nacional de Justiça (CNJ) em caso de transferências internacionais

Ainda no art. 55, o §2º determina que as transferências internacionais realizadas sem a decisão de adequação, mas baseadas em outras garantias, só seriam

comunicadas ao Conselho Nacional de Justiça (CNJ) em caso de solicitação deste. Entretanto, é mais compatível com a lógica de proteção de dados pessoais a **comunicação obrigatória da transferência internacional sob esses moldes para o CNJ**, especialmente diante da peculiaridade do contexto em que o dado é tratado, ou seja, em procedimento de investigação criminal ou persecução, bem como do tipo de transferência internacional, sem decisão de adequação.

Redação atual

Art. 55. (...)

II - o responsável pelo tratamento tiver avaliado todas as circunstâncias inerentes à transferência de dados pessoais e concluído que existem garantias adequadas no que diz respeito à proteção desses dados.

(...)

§ 2º As transferências baseadas no inciso II serão documentadas, devendo o responsável pelo tratamento disponibilizar ao Conselho Nacional de Justiça, **a pedido deste**, toda a documentação pertinente, incluindo informações sobre a data e a hora da transferência, a autoridade competente que as recebe, a justificação da transferência e os dados pessoais transferidos.

Redação sugerida

Art. 55. (...)

II - o responsável pelo tratamento tiver avaliado todas as circunstâncias inerentes à transferência de dados pessoais e concluído que existem garantias adequadas no que diz respeito à proteção desses dados, **conforme os critérios previstos no art. 34 da Lei 13.709/18.**

(...)

§ 2º As transferências baseadas no inciso II serão documentadas, devendo o responsável pelo tratamento disponibilizar ao Conselho Nacional de Justiça, **sem necessidade de pedido por parte deste**, toda a documentação pertinente, incluindo informações sobre a data e a hora da transferência, a autoridade competente que as recebe, a justificação da transferência e os dados pessoais transferidos.

VI - Da autoridade de supervisão

A autoridade de supervisão, de acordo com a própria exposição de motivos do Anteprojeto de Lei, seria o órgão responsável pela aplicação, supervisão e monitoramento da futura lei de proteção de dados para segurança pública e investigação penal. Ela seria o equivalente, numa comparação com a LGPD, à Autoridade Nacional de Proteção de Dados (ANPD), mas apenas para o âmbito penal.

Ordenamentos que já possuem uma estrutura de proteção de dados mais consolidada também preveem essa figura, como o sistema da União Europeia (UE). No Anteprojeto, a Comissão de Juristas propôs a criação de uma unidade específica no bojo do Conselho Nacional de Justiça (CNJ), um modelo distinto do adotado na UE. Tal unidade foi denominada de Unidade Especial de Proteção de Dados em Matéria Penal (UPDP).

O presente capítulo se divide em quatro subtítulos: das controvérsias acerca da autonomia da UPDP; das competências da autoridade de supervisão; das hipóteses em que a autoridade de supervisão pode solicitar relatórios de impacto à proteção de dados pessoais; e da relação entre a autoridade de supervisão e órgãos de controle.

a. Das controvérsias acerca da autonomia da Unidade Especial de Proteção de Dados em Matéria Penal (UPDP)

[art. 59] Previsão expressa sobre a não-subordinação hierárquica da Unidade Especial de Proteção de Dados em Matéria Penal (UPDP) em relação ao Plenário do Conselho Nacional de Justiça (CNJ)

[art. 60] Alteração da competência para indicação da Diretoria da UPDP, para ser realizada pela Presidência da República com sabatina no Senado Federal

[art. 60] Previsão expressa de vedação ao exercício de atividades profissionais concomitantes aos ocupantes dos cargos da Diretoria da UPDP

Acerca da sua estrutura, a Unidade Especial de Proteção de Dados em Matéria Penal (UPDP) se encontra dentro do Conselho Nacional de Justiça (CNJ), estando separada da Autoridade Nacional de Proteção de Dados (ANPD). A UPDP é posta como a entidade competente para supervisionar os tratamentos de dados pessoais feitos por autoridades competentes com finalidade de realização de atividades de segurança pública e de persecução penal. Do ponto de vista legal, a medida é possível, já que a LGPD não prescreveu que a ANPD seria competente para supervisionar tratamento de dados pessoais realizados para fins exclusivos de segurança pública. Contudo, sob uma análise de governança, algumas questões surgem diante da posição da UPDP dentro do CNJ.

Primeiramente, **apesar do art. 60, §1º trazer que a UPDP terá autonomia técnica e decisória, sua posição como parte de um órgão superior a torna vulnerável de um ponto de vista legal e de um ponto de vista administrativo**.

A **questão legal** gira em torno de dois eixos. O primeiro diz respeito à **possibilidade de haver recurso das decisões da UPDP ao Plenário do CNJ**, já que a UPDP será parte do Conselho. Os chamados recursos hierárquicos são um mecanismo de revisão das decisões, que pode ser acionado pelas partes de um processo administrativo caso haja uma decisão negando o interesse deles. Diante da inexistência de ressalva sobre a aplicabilidade deste instituto, isso diminuiria a autonomia técnica e decisória da UPDP, pois toda e qualquer decisão poderá ser revisada pelo Plenário do CNJ.

O segundo eixo é a não-submissão do STF ao CNJ, existindo, ao contrário, uma relação de sujeição do CNJ ao STF, como decidido no âmbito da ADI 3.367[51]. Esse precedente **abre caminho para que o STF ignore as regulamentações no âmbito das suas atividades administrativas e**, **no âmbito da sua atuação judicial, modifique as regras criadas pela UPDP**.

[51] Na ADI 3.367, o Supremo Tribunal Federal entendeu que o "Conselho Nacional de Justiça não tem nenhuma competência sobre o Supremo Tribunal Federal, e seus ministros, sendo esse o órgão máximo do Poder Judiciário Nacional, a que aquele está sujeito" (ADI 3.367, Plenário. Min. Relator Cézar Peluso, julgado em 13/04/2005, publicado em 17/03/2006).

Do **ponto de vista administrativo**, a questão que surge é relativa à escolha dos membros da UPDP pelo próprio CNJ. Diferentemente do que é preconizado para a ANPD, cujos membros são escolhidos pela Presidência da República e sabatinados pelo Senado Federal, o que teríamos **com a UPDP seria a escolha de seu diretor diretamente pelo CNJ, sem que haja sabatina pelo Senado**, conforme art. 60, § 2º, do Anteprojeto.

Isto dá um grande poder ao Judiciário na definição da diretoria, já que a composição do CNJ, de acordo com o art. 103-B da Constituição, é feita majoritariamente por juízes, com uma minoria de membros do Ministério Público, advogados e cidadãos, sem representação da Defensoria Pública. Essa composição provavelmente se refletirá na nomeação da diretoria da UPDP, que espelhará mais o interesse do Judiciário do que da sociedade como um todo na estrutura da Unidade.

Em comparação com a Diretiva (UE) 2016/680, vê-se que há diferenças nos pontos levantados, ou seja, legal e administrativamente. O art. 42 da Diretiva prevê que o órgão equivalente à UPDP nos países-membros da UE deve ter independência plena, não podendo sofrer influência ou instrumentos de qualquer outro órgão, de forma direta ou indireta[52]. Nesse sentido, a UPDP poderia ser considerada mais frágil graças a uma possível subordinação ao Pleno do CNJ, como expresso acima. Ademais, a Diretiva dita claramente que a autoridade supervisora terá seu quadro de pessoal e orçamento independente, a fim de garantir maior autonomia.

Além disso, os membros das autoridades nos países europeus devem ser indicados pelo Legislativo, pelo Executivo ou por um órgão independente dos outros poderes. Vê-se que o modelo brasileiro cai exatamente dentro do único modelo não adotado pela Diretiva (UE) 2016/680, ou seja, com indicação por parte do Judiciário. O motivo para tal vedação na normativa europeia é o conflito de interesses que pode existir devido ao estreitamento de relações entre Judiciário e os órgãos de investigação. Ao possibilitar que um representante do Judiciário dite como as investigações policiais poderão ser feitas, abre-se portas para que haja uma

[52] Artigo 42.(...)
2. Os Estados-Membros preveem que os membros das autoridades de controlo, no desempenho das suas funções e no exercício dos poderes nos termos da presente diretiva, não estejam sujeitos a influências externas, diretas ou indiretas, e não solicitem nem recebam instruções de outrem. (...)

interferência do Judiciário na atuação dos órgãos investigativos, colocando em risco o bom funcionamento do sistema acusatório penal.

Por fim, a Diretiva (UE) 2016/680 veda o exercício de atividades profissionais aos ocupantes dos cargos da autoridade supervisora, como nos moldes previstos para os diretores de agências reguladoras no Brasil. Entretanto, este não foi o modelo proposto no Anteprojeto de Lei brasileiro de proteção de dados para a segurança pública e investigação penal.

Portanto, sugere-se que:

1. haja previsão expressa na lei a respeito da não subordinação hierárquica da UPDP em relação ao Pleno do CNJ;
2. os membros da UPDP sejam indicados não pelo próprio CNJ, mas pela Presidência da República e com sabatina no Senado Federal; e
3. seja incluída previsão que vede aos ocupantes dos cargos da autoridade supervisora o exercício de outras atividades profissionais concomitantes ao cargo.

Ressalte-se que, ainda que sejam acolhidas as sugestões trazidas pelo LAPIN, o modelo de autoridade supervisora proposto pelo Anteprojeto de Lei continuará com questões insanáveis. Por fim, **independentemente do modelo adotado pelo legislador para a autoridade de supervisão, as recomendações** dos subcapítulos seguintes - e quaisquer outras que se refiram à autoridade de supervisão nos capítulos anteriores - **devem ser consideradas**.

Redação atual

Art. 59. O Conselho Nacional de Justiça (CNJ), por meio da sua Unidade Especial de Proteção de Dados em Matéria Penal (UPDP), será responsável por zelar, implementar e fiscalizar a presente lei em todo o território nacional.

Redação sugerida

Art. 59. O Conselho Nacional de Justiça (CNJ), por meio da sua Unidade Especial de Proteção de Dados em Matéria Penal (UPDP), será responsável por zelar, implementar e fiscalizar a presente lei em todo o território nacional.

Parágrafo único. A Unidade Especial de Proteção de Dados em Matéria Penal não se subordina hierarquicamente ao Plenário do Conselho Nacional de Justiça.

Redação atual

Art. 60. A diretoria da Unidade Especial de Proteção de Dados em Matéria Penal (UPDP) será composta por 1 (um) Diretor, 3 (três) coordenações especializadas para a aplicação da lei e assessoria técnica.

(...)

§ 2º O Diretor **será escolhido pelo Conselho Nacional de Justiça** dentre brasileiros que tenham reputação ilibada, nível superior de educação e notório saber no campo da proteção de dados ou segurança pública e persecução penal.

(...)

Redação sugerida

Art. 60. A diretoria da Unidade Especial de Proteção de Dados em Matéria Penal (UPDP) será composta por 1 (um) Diretor, 3 (três) coordenações especializadas para a aplicação da lei e assessoria técnica.

(...)

§ 2º O Diretor **será escolhido pelo Presidente da República e por ele nomeado, após aprovação pelo Senado Federal, nos termos da alínea 'f' do inciso III do art. 52 da Constituição Federal**, dentre brasileiros que tenham reputação ilibada, nível superior de educação e notório saber no campo da proteção de dados ou segurança pública e persecução penal.

(...)

§ 5º Fica vedado aos ocupantes de cargos na Diretoria da Unidade Especial de Proteção de Dados em Matéria Penal (UPDP) o exercício de outras atividades profissionais de forma concomitante ao período de ocupação do cargo.

b. Das competências da autoridade de supervisão

[art. 62] Especificação de que a autoridade supervisora será competente para agir sobre todos os tratamentos de dados cuja finalidade é a segurança pública e a persecução penal, independente de quem os realize

[art. 62] Inclusão de competência para o aconselhamento de outros órgãos públicos pela autoridade de supervisão

Relativamente às competências da UPDP, que constam no art. 62, não se observaram sobreposições com o que é de competência da ANPD. Contudo, em alguns incisos, como o VII e o XI, seria prudente uma modificação da redação para tornar claro que os tratamentos referidos são aqueles cuja finalidade é a segurança pública e a persecução penal, independente de quem os realize.

Segundo a LGPD, veda-se a pessoas jurídicas de direito privado a realização de tratamento de dados para segurança pública e investigação penal, "exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional"[53]. Dessa forma, a UPDP seria competente para **supervisionar não apenas as autoridades competentes, mas qualquer pessoa jurídica que realize tratamento de dados para estes fins**. É preciso, portanto, que o texto da futura lei seja claro quanto a essa possibilidade.

Ainda, considerando o papel da autoridade supervisora de instituição especializada, no Estado brasileiro, no tratamento de dados pessoais para fins de segurança pública e persecução penal, cabe incluir, em seu rol de atribuições, o **aconselhamento de outros órgãos públicos na seara desse tipo de tratamento de dados**.

A autoridade de supervisão, como ente que irá regulamentar e fiscalizar os referidos tratamentos, é ator importante e que deve ser ouvido na construção das legislações e na atuação do Executivo, promovendo os direitos dos titulares de dados e a segurança pública. Incluir tal competência garante que esse ecossistema não fique

[53] LGPD. Art.4º, § 2º.

órfão de uma entidade que guie o desenvolvimento desta matéria de forma democrática, com respeito aos direitos fundamentais e à ordem jurídica.

Redação atual

Art. 62. Compete à Unidade Especial de Proteção de Dados em Matéria Penal (UPDP):

(...)

VII - solicitar, a qualquer momento, às **autoridades competentes submetidas a esta lei** informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;

(...)

XI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização sobre o tratamento de dados pessoais **efetuado pelas autoridades competentes**;

Redação sugerida

Art. 62. Compete à Unidade Especial de Proteção de Dados em Matéria Penal (UPDP):

(...)

VII - solicitar, a qualquer momento, **aos controladores que realizam tratamento cuja finalidade é a segurança pública e persecução penal,** informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;

(...)

XI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização sobre o tratamento de dados pessoais **cuja finalidade seja a realização de atividade de segurança pública e persecução penal;**

(...)

XVI - ser consultada e emitir opiniões sobre medidas legislativas e administrativas que versem sobre tratamento de dados pessoais para atividades de segurança pública e de persecução penal;

c. Das hipóteses em que a autoridade de supervisão pode solicitar relatórios de impacto à proteção de dados pessoais

[art. 62] Ampliação das hipóteses em que relatórios de impacto à proteção de dados pessoais (RIDP) podem ser solicitados

Além disso, o **inciso IX do art. 62** estabelece que o relatório de impacto à proteção de dados pessoais (RIPD) só pode ser solicitado pela autoridade supervisora em caso de alto risco aos direitos prescritos na futura lei. Parece prudente que **se amplie o âmbito de situações onde as hipóteses em que o RIPD poderá ser exigido, diante do princípio da prevenção**, previsto no art. 6º, VIII da LGPD e no art. 6º, inciso X deste Anteprojeto de Lei. Isto porque o objeto do referido tratamento de dados, o ramo do direito com que se está se trabalhando e o alto potencial de dano que é inerente à atividade de segurança pública promovida pelo Estado cria uma situação onde é necessário um maior acompanhamento pela UPDP.

Assim, propõe-se que se exclua a condicional de "representação de alto risco aos direitos previstos" na futura lei e se possibilite à autoridade de supervisão solicitar RIPD em qualquer hipótese de tratamento de dados para fins de segurança pública e persecução penal.

Redação atual

Art. 62. Compete à Unidade Especial de Proteção de Dados em Matéria Penal (UPDP):

(...)

IX – solicitar relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento **representar alto risco aos direitos previstos nesta Lei;**

Redação sugerida

Art. 62. Compete à Unidade Especial de Proteção de Dados em Matéria Penal (UPDP):

(...)

IX – solicitar relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento **tenha por finalidade a realização de atividade de segurança pública ou persecução penal;**

d. Da relação entre a autoridade de supervisão e órgãos de controle

[art. 62] Ampliação do âmbito da comunicação para órgãos de controle externo nos casos de descumprimento da futura lei

Outro ponto importante é a alteração do inciso **XIII do art. 62**, para que se **amplie o âmbito da comunicação para os órgãos de controle externo em caso de descumprimento da futura lei.** Tal inciso propõe que a autoridade supervisora comunique apenas a órgãos de controle interno. Entretanto, órgãos de controle externo, como os Tribunais de Contas, podem ser competentes para analisar a adequação das organizações públicas à legislação de proteção de dados. A título de exemplo, o Tribunal de Contas da União já se declarou competente para realizar tal atividade no âmbito da LGPD, podendo expandir tal possibilidade para o âmbito penal.

Redação atual

Art. 62. Compete à Unidade Especial de Proteção de Dados em Matéria Penal (UPDP):

(...)

XIII - comunicar aos **órgãos de controle interno** o descumprimento do disposto nesta Lei pelas autoridades competentes;

Redação sugerida

Art. 62. Compete à Unidade Especial de Proteção de Dados em Matéria Penal (UPDP):

(...)

XIII - comunicar aos **órgãos de controle internos e externos** o descumprimento do disposto nesta Lei pelas autoridades competentes;

VII - Das alterações pontuais, mas necessárias

Além das recomendações apontadas nos capítulos anteriores, sugere-se as seguintes alterações no texto do Anteprojeto de Lei. Por se tratarem de mudanças pontuais, que não necessitam longas explicações, optou-se por reuni-las na tabela abaixo. As justificativas para as sugestões apresentadas variam desde harmonização de termos com outras legislações vigentes até a adoção de salvaguardas capazes de tornar a futura lei mais robusta.

A tabela abaixo está em ordem crescente de artigos e contém três colunas: a primeira com a redação atual do Anteprojeto; a segunda com a redação sugerida por este relatório; e a terceira com o fundamento da alteração.

Redação atual	Redação sugerida	Fundamento
Art. 34. Controladores e operadores devem conservar em sistemas de tratamento automatizado registros cronológicos das seguintes operações de tratamento: de coleta, alteração, consulta, acesso, divulgação, transferências, interconexão, **apagamento**.	Art. 34. Controladores e operadores devem conservar em sistemas de tratamento automatizado registros cronológicos das seguintes operações de tratamento: de coleta, alteração, consulta, acesso, divulgação, transferências, interconexão e eliminação.	Como forma de harmonizar os termos com outros já contidos em legislações vigentes, sugere-se a adoção do termo "eliminação", **conforme art. 5º, XIV, da LGPD**.
Art. 34. (...)	Art. 34 (...) **§ 3º Os registros mencionados no caput apenas podem ser utilizados para as seguintes finalidades:** **I - verificar a legalidade do tratamento;** **II - auxiliar no monitoramento do ciclo de vida dos dados pessoais pelo próprio**	Inspirada na seção 62(4) da Lei de Proteção de Dados do Reino Unido (Data Protection Act 2018), sugere-se a inclusão do mencionado parágrafo. Como os registros mencionados no caput vão inevitavelmente conter dados pessoais, **tais salvaguardas trazem**

	controlador ou, conforme o caso, pelo operador, incluindo para a condução de processos disciplinares internos; **III - garantir a integridade e a segurança dos dados pessoais;** **IV - alcançar os objetivos dos procedimentos criminais.**	**mais segurança e limitação para o seu uso**.
Art. 34. (...) § 1º Os **registos** cronológicos das operações de consulta e de divulgação devem permitir determinar o motivo, a data e a hora dessas operações, a identificação da pessoa que consultou ou divulgou dados pessoais e, sempre que possível, a identidade dos destinatários desses dados pessoais.	Art. 34. (...) § 1º Os **registros** cronológicos das operações de consulta e de divulgação devem permitir determinar o motivo, a data e a hora dessas operações, a identificação da pessoa que consultou ou divulgou dados pessoais e, sempre que possível, a identidade dos destinatários desses dados pessoais.	A grafia "registos" não é **utilizada comumente no Português brasileiro**, por isso sugere-se utilizar a forma "registros".
Art. 34 (...) § 2º Os **registos** cronológicos, cuja integridade e cuja reserva devem ser observadas pelos controladores e operadores, serão mantidos por no mínimo 5 anos e poderão ser utilizados para efeitos de verificação da licitude do tratamento, controle administrativo, exercício do poder disciplinar, garantia da integridade e segurança	Art. 34 (...) § 2º Os **registros** cronológicos, cuja integridade e cuja reserva devem ser observadas pelos controladores e operadores, serão mantidos por no mínimo 5 anos **em base segura e com regras de controle de acesso** e poderão ser utilizados para efeitos de verificação da licitude do tratamento, controle administrativo, exercício do poder disciplinar, garantia da integridade e	A grafia "registos" não é **utilizada comumente no Português brasileiro**, por isso sugere-se utilizar a forma "registros". A salvaguarda tem como fim estabelecer **exigências mínimas quanto à segurança dos registros** mantidos por autoridades competentes, diminuindo

dos dados pessoais, análise pelo Conselho Nacional de Justiça e instrução de processos penais, inclusive a pedido da defesa.	segurança dos dados pessoais, análise pelo Conselho Nacional de Justiça e instrução de processos penais, inclusive a pedido da defesa.	riscos de acesso indevido e vazamento de dados.
Art. 36. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.	Art. 36. (...) **§ 4º As autoridades competentes devem garantir que todo seu corpo de funcionários esteja ciente e cumpra com as medidas de segurança estabelecidas em lei**.	Inspirado no art. 72(2) da Lei de Proteção de Dados irlandesa (Irish Data Protection Act), sugere-se a inclusão de mais um parágrafo ao art. 36 como **forma de reforçar as medidas de segurança no tratamento de dados por autoridades competentes**.
Art. 36. (...) § 3º As medidas de que trata o caput devem ser adotadas com as seguintes finalidades: (...) II - controle de **suporte de dados**: impedir que os **suportes de dados** sejam lidos, copiados, alterados ou retirados sem autorização;	Art. 36. (...) § 3º (...) II - controle de **suporte físico de dados**: impedir que os **suportes físicos de dados** sejam lidos, copiados, alterados ou retirados sem autorização;	O termo utilizado se refere aos *hardwares* ou **dispositivos em que os dados ficam armazenados**, como fitas, CDs e DVDs. De forma a deixar o item mais preciso, sugere-se incluir o termo "físico" à expressão.
Art. 36. (...) § 3º (...) III - controle da conservação: impedir a introdução não autorizada	Art. 36. (...) § 3º (...) III - controle da conservação: impedir a introdução não autorizada de dados pessoais,	Como forma de harmonizar os termos com outros já contidos em legislações vigentes,

de dados pessoais, bem como qualquer inspeção, alteração ou **apagamento** não autorizados de dados pessoais conservados;	bem como qualquer inspeção, alteração ou **eliminação** não autorizados de dados pessoais conservados;	sugere-se a adoção do termo "eliminação", **conforme art. 5º, XIV, da LGPD**.
Art. 36. (...) § 3º (...) VI - controle da comunicação: **assegurar que possa ser verificado e determinado a organismos os dados pessoais que foram ou podem ser transmitidos ou facultados utilizando equipamento de comunicação de dados**;	Art. 36. (...) § 3º (...) VI - controle da comunicação: **assegurar que seja possível verificar e determinar para quais agentes os dados pessoais foram ou podem ser transmitidos ou disponibilizados através de equipamento de comunicação de dados**;	A redação atual é **imprecisa**, portanto, sugere-se a alteração para **torná-la mais inteligível**.
Art. 36. (...) § 3º (...) VII - controle da inserção: assegurar que **possa ser verificado e determinado** a posteriori quais os dados pessoais **introduzidos nos** sistemas de tratamento automatizado, quando e por quem;	Art. 36. (...) § 3º (...) VII - controle da inserção: assegurar que **seja possível verificar e determinar,** a posteriori**,** quais os dados pessoais **tratados no âmbito dos** sistemas de tratamento automatizado, quando e por quem;	A redação atual é **imprecisa**, portanto, sugere-se a alteração para **torná-la mais inteligível**.
Art. 36.(...) § 3º (...) X - assegurar que as funções do sistema funcionem, que os erros de funcionamento sejam assinalados (**fiabilidade**) e que os dados pessoais conservados não possam	Art. 36. (...) § 3º (...) X - **Confiabilidade, integridade e disponibilidade**: assegurar que as funções do sistema funcionem, que os erros de funcionamento sejam assinalados (**confiabilidade**) e que os dados pessoais	Ao contrário dos outros incisos do § 3º, **este não possui título**. Considerando que os três eixos da Tecnologia da Informação (TI) são "confiabilidade", "integridade" e "disponibilidade", sugere-se o título

ser **falseados** por um mau funcionamento do sistema.	conservados não possam ser **corrompidos** por um mau funcionamento do sistema.	mencionado. "Fiabilidade" **não é uma palavra utilizada comumente no Brasil**, especialmente no que se refere a dados. Sugere-se alterá-la por "confiabilidade". "Falseados" **não é uma palavra utilizada comumente no Brasil**, especialmente no que se refere a dados. Sugere-se alterá-la por "corrompidos".
Art. 37. (...) § 2º Os dados pessoais serão **tornados anônimos** ou pseudonimizados o quanto antes, de acordo com a finalidade do processamento.	Art. 37. (...) § 2º Os dados pessoais serão **anonimizados** ou pseudonimizados o quanto antes, de acordo com a finalidade do processamento.	Como forma de harmonizar os termos com outros já contidos em legislações vigentes, sugere-se a adoção do termo "anonimizados", **conforme art. 5º, III e XI, da LGPD**.
Art. 37. (...) § 3º O **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.	Art. 37. (...) § 3º O **controlador** 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.	Como forma de harmonizar os termos com outros já contidos em legislações vigentes, sugere-se a adoção do termo "controlador", **conforme art. 5º, VI, da LGPD**.

Art. 42. (...) § 3º A lei deve estabelecer política de uso que garanta os direitos dos titulares de dados e contenha: (...)	Art. 42. (...) § 3º (...) **IX - definição de prazo razoável para eliminação dos dados coletados**;	Os dados coletados através de tecnologias de monitoramento são, em geral, sensíveis. Portanto, a fim de **assegurar o pleno exercício dos direitos do titular de dados**, é necessário que legislações específicas que autorizem o uso dessas tecnologias prevejam prazo para a eliminação desses dados.

Conclusão

Em novembro de 2020, foi apresentado o **Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Investigação Criminal** à Câmara dos Deputados. Elaborado pela Comissão de Juristas nomeada pela Presidência daquela Casa em novembro de 2019, o texto do Anteprojeto tem por objetivo sanar a lacuna existente no ordenamento brasileiro acerca de legislação específica que balanceie os direitos à proteção de dados pessoais e à segurança pública, ambos previstos constitucionalmente. Além disso, a futura lei decorrente do Anteprojeto cumpriria a exigência prevista no art. 4º, inciso III da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD).

Trata-se de tema essencial ao desenvolvimento democrático brasileiro. Portanto, a presente Nota Técnica objetivou discutir o conteúdo do Anteprojeto e contribuir para o seu aprimoramento através de recomendações a serem incorporadas ao texto. Assim, o LAPIN sugere a análise dos pontos apresentados e a adoção das medidas propostas, de modo a garantir que a futura legislação de proteção de dados para a segurança pública e investigação criminal esteja harmonizada com o ordenamento brasileiro, a evolução das tecnologias e tratamentos de dados e as boas práticas nacionais e internacionais.

Anexo I - Tabela com todas as recomendações

Redação atual	Redação sugerida
Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de defesa nacional e segurança do Estado.	Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de defesa nacional e segurança do Estado. **Parágrafo único. O controlador ou operador de dados que recusar o exercício dos direitos previstos nesta legislação sob a justificativa de defesa nacional e segurança do Estado deverá fundamentar sua decisão, sob pena de nulidade, nos termos do artigo 19, §3º, desta lei.**
Art. 5º Para os fins desta Lei, considera-se: (...)	Art. 5º Para os fins desta Lei, considera-se: (...) XXV - **pseudonimização**: tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro; XXVI - **Perfilização**: qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados para avaliar aspectos pessoais de um titular de dados, nomeadamente para analisar ou prever aspectos relacionados com o seu desempenho profissional, a sua situação econômica, saúde, preferências

	pessoais, interesses, fiabilidade, comportamento, localização ou deslocamentos; XXVII - **Dados biométricos**: dados pessoais resultantes de um tratamento técnico específico, relativos às características físicas, fisiológicas ou comportamentais de um titular de dados, que permitem ou confirmam a sua identificação única, tais como imagens faciais ou dados dactiloscópicos.
Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I – licitude: embasamento do tratamento de dados pessoais em hipótese legal, nos termos do Capítulo II desta Lei; (...) V – proporcionalidade: compatibilidade do tratamento com os objetivos pretendidos, de acordo com o contexto do tratamento;	Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I – licitude: embasamento do tratamento de dados pessoais em hipótese legal, nos termos do Capítulo II desta Lei; (...) V – proporcionalidade: **garantia de limitação de tratamento de dados pessoais somente aos dados que se mostrem adequados, relevantes e estritamente necessários**; (...) **Parágrafo Único: o agente de tratamento deverá descrever os objetivos do tratamento, os dados pessoais tratados e a finalidade do tratamento de maneira acessível aos cidadãos.**

Art. 13. O tratamento de dados pessoais sensíveis somente poderá ser realizado por autoridades competentes se estiver previsto em lei, observadas as salvaguardas desta Lei. Parágrafo único. A autoridade competente responsável pelo tratamento de dados pessoais sensíveis elaborará relatório de impacto à proteção de dados pessoais **e informará ao Conselho Nacional de Justiça**.	Art. 13. O tratamento de dados pessoais sensíveis somente poderá ser realizado por autoridades competentes se estiver previsto em lei, observadas as salvaguardas desta Lei. Parágrafo único. A autoridade competente responsável pelo tratamento de dados pessoais sensíveis elaborará relatório de impacto à proteção de dados pessoais **nos termos dos artigos X e seguintes*.** **Conforme sugestão para o capítulo específico sobre RIPD*
Art. 23. As decisões tomadas com base no tratamento automatizado de dados pessoais, que afetem os interesses do titular, devem ser precedidas de autorização do Conselho Nacional de Justiça **e de publicação de relatório de impacto, que comprove a adoção das garantias adequadas para os direitos e liberdades do titular, incluído o direito de solicitar a revisão da decisão por uma pessoa natural e observado o disposto no artigo 25.** **§1º** O relatório de impacto à proteção de dados pessoais deve ser publicado na página da autoridade competente e enviado ao Conselho Nacional de Justiça, demonstrando as garantias para a proteção dos direitos e liberdades do titular requeridas no caput, que deverão ser adequadas à natureza dos dados tratados. **§2º** O Conselho Nacional de Justiça deverá examinar o relatório de impacto e decidir acerca da possibilidade da	Art. 23. As decisões tomadas com base no tratamento automatizado de dados pessoais, que afetem os interesses do titular, devem ser precedidas de autorização do Conselho Nacional de Justiça e **ser objeto de relatório de impacto nos termos dos artigos X e seguintes*.** *Os **§§1º e 2º** devem ter seu conteúdo remetido ao capítulo específico sobre RIPD, conforme sugestão na tabela seguinte.* §3º O titular será notificado da utilização de decisões automatizadas. §4º As decisões a que se refere o caput deste artigo não podem basear-se em dados sensíveis, com exceção de dados biométricos. **§5º As autorizações de que trata o *caput* serão concedidas de forma individualizada para cada autoridade competente, levando em conta o contexto e a finalidade de sua aplicação**

decisão automatizada com base no tratamento automatizado de dados, à luz das garantias para os direitos e liberdades do titular e dos riscos apresentados. §3º O titular será notificado da utilização de decisões automatizadas. §4º As decisões a que se refere o caput deste artigo não podem basear-se em dados sensíveis, com exceção de dados biométricos.	**específica, sendo vedadas autorizações genéricas referentes a um sistema responsável por decisões automatizadas.** **Conforme sugestão para o capítulo específico sobre RIPD*
Art. 24. (...) § 2º O controlador elaborará relatório de impacto de proteção de dados pessoais à luz das circunstâncias concretas do tratamento em questão. **§ 3º** O Conselho Nacional de Justiça deverá examinar o relatório de impacto e decidir acerca da possibilidade da decisão automatizada com base no tratamento automatizado de dados, à luz das garantias para os direitos e liberdades do titular frente aos riscos apresentados. (...)	Art. 24. (...) § 2º O controlador elaborará relatório de impacto de proteção de dados pessoais à luz das circunstâncias concretas do tratamento em questão, **nos termos dos artigos X e seguintes*.** *O **§ 3º** deve ter seu conteúdo remetido ao capítulo específico sobre RIPD, conforme sugestão na tabela seguinte.* **Conforme sugestão para o capítulo específico sobre RIPD*
Art. 25. Os sistemas responsáveis por decisões automatizadas a que se referem os artigos 23 e 24 devem ser auditáveis, não discriminatórios e passíveis de comprovação acerca de sua precisão e grau de acurácia. (...)	Art. 25. Os sistemas responsáveis por decisões automatizadas a que se referem os artigos 23 e 24 devem ser auditáveis, não discriminatórios e passíveis de comprovação acerca de sua precisão e grau de acurácia. (...) § 3º É garantido ao titular o direito de solicitar a revisão da decisão por uma

§3º É garantido ao titular o direito de solicitar a revisão da decisão por uma pessoa natural.	pessoa natural, **bem como de requerer explicações a respeito do processo de tomada de decisões automatizadas específicas que afetem o exercício de seus direitos ou que possuam fundados indícios de terem sido feitas de forma equivocada.** **§ 5º O pedido de fornecimento de explicações a respeito do processo de tomada de decisões automatizadas específicas será dirigido à autoridade competente para avaliação de seu cabimento, com possibilidade de recurso ao Conselho Nacional de Justiça.** **§ 6º As explicações de decisões automatizadas específicas de que trata o parágrafo anterior poderão ser fornecidas, caso possam afetar a condução de investigação policial, exclusivamente ao Conselho Nacional de Justiça, que avaliará e informará o titular de dados a respeito da compatibilidade de tais explicações com o exercício dos direitos e princípios previstos nesta lei.**
Art. 26. (...)	*O **art. 26 e todos os seus parágrafos** devem ter seu conteúdo remetido ao capítulo específico sobre RIPD, conforme sugestão na tabela seguinte.*
Art. 29. (...)	*O **art. 29 e todos os seus parágrafos** devem ter seu conteúdo remetido ao capítulo específico sobre RIPD, conforme sugestão na tabela seguinte.*
Art. 34. Controladores e operadores devem conservar em sistemas de tratamento automatizado registros cronológicos das seguintes operações de tratamento: de coleta, alteração, consulta, acesso, divulgação,	Art. 34. Controladores e operadores devem conservar em sistemas de tratamento automatizado registros cronológicos das seguintes operações de tratamento: de coleta, alteração, consulta, acesso, divulgação,

transferências, interconexão, **apagamento**.	transferências, interconexão e **eliminação**.
§ 1º Os **registos** cronológicos das operações de consulta e de divulgação devem permitir determinar o motivo, a data e a hora dessas operações, a identificação da pessoa que consultou ou divulgou dados pessoais e, sempre que possível, a identidade dos destinatários desses dados pessoais.	§ 1º Os **registros** cronológicos das operações de consulta e de divulgação devem permitir determinar o motivo, a data e a hora dessas operações, a identificação da pessoa que consultou ou divulgou dados pessoais e, sempre que possível, a identidade dos destinatários desses dados pessoais.
§ 2º Os **registos** cronológicos, cuja integridade e cuja reserva devem ser observadas pelos controladores e operadores, serão mantidos por no mínimo 5 anos e poderão ser utilizados para efeitos de verificação da licitude do tratamento, controle administrativo, exercício do poder disciplinar, garantia da integridade e segurança dos dados pessoais, análise pelo Conselho Nacional de Justiça e instrução de processos penais, inclusive a pedido da defesa.	§ 2º Os **registros** cronológicos, cuja integridade e cuja reserva devem ser observadas pelos controladores e operadores, serão mantidos por no mínimo 5 anos **em base segura e com regras de controle de acesso** e poderão ser utilizados para efeitos de verificação da licitude do tratamento, controle administrativo, exercício do poder disciplinar, garantia da integridade e segurança dos dados pessoais, análise pelo Conselho Nacional de Justiça e instrução de processos penais, inclusive a pedido da defesa. **§ 3º Os registros mencionados no caput apenas podem ser utilizados para as seguintes finalidades:** **I - verificar a legalidade do tratamento;** **II - auxiliar no monitoramento do ciclo de vida dos dados pessoais pelo próprio controlador ou, conforme o caso, pelo operador, incluindo para a condução de processos disciplinares internos;** **III - garantir a integridade e a segurança dos dados pessoais;** **IV - alcançar os objetivos dos procedimentos criminais.**
Art. 36. (...) § 3º As medidas de que trata o caput	Art. 36. (...)

devem ser adotadas com as seguintes finalidades: (...) II - controle de **suporte de dados**: impedir que os **suportes de dados** sejam lidos, copiados, alterados ou retirados sem autorização; III - controle da conservação: impedir a introdução não autorizada de dados pessoais, bem como qualquer inspeção, alteração ou **apagamento** não autorizados de dados pessoais conservados; (...) VI - controle da comunicação: **assegurar que possa ser verificado e determinado a organismos os dados pessoais que foram ou podem ser transmitidos ou facultados utilizando equipamento de comunicação de dados**; VII - controle da inserção: assegurar que **possa ser verificado e determinado** a posteriori quais os dados pessoais **introduzidos nos** sistemas de tratamento automatizado, quando e por quem; (...) X - assegurar que as funções do sistema funcionem, que os erros de funcionamento sejam assinalados (**fiabilidade**) e que os dados pessoais conservados não possam ser **falseados** por um mau funcionamento do sistema.	§ 3º (...) II - controle de **suporte de dados**: impedir que os **suportes de dados** sejam lidos, copiados, alterados ou retirados sem autorização; III - controle da conservação: impedir a introdução não autorizada de dados pessoais, bem como qualquer inspeção, alteração ou **eliminação** não autorizados de dados pessoais conservados; (...) VI - controle da comunicação: **assegurar que seja possível verificar e determinar para quais agentes os dados pessoais foram ou podem ser transmitidos ou disponibilizados através de equipamento de comunicação de dados**; VII - controle da inserção: assegurar que **seja possível verificar e determinar,** a posteriori**,** quais os dados pessoais **tratados no âmbito dos** sistemas de tratamento automatizado, quando e por quem; (...) X - **Confiabilidade, integridade e disponibilidade**: assegurar que as funções do sistema funcionem, que os erros de funcionamento sejam assinalados (**confiabilidade**) e que os dados pessoais conservados não possam ser **corrompidos** por um mau funcionamento do sistema. **§ 4º As autoridades competentes devem garantir que todo seu corpo de funcionários esteja ciente e cumpra com as medidas de segurança estabelecidas**

	em lei.
Art. 37. (...) § 2º Os dados pessoais serão **tornados anônimos** ou pseudonimizados o quanto antes, de acordo com a finalidade do processamento. § 3º O **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.	Art. 37. (...) § 2º Os dados pessoais serão **anonimizados** ou pseudonimizados o quanto antes, de acordo com a finalidade do processamento. § 3º O **controlador** 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.
Art. 42. (...) § 2º O processo legislativo será instruído de análise de impacto regulatório que contenha: (...) § 3º (...)	Art. 42. (...) § 2º O processo legislativo será instruído de análise de impacto regulatório que contenha: (...) **VII - identificação do problema que se pretende solucionar, com a apresentação de suas causas e sua extensão;** **VIII – descrição das alternativas possíveis ao enfrentamento do problema identificado, consideradas as opções de não ação, de soluções dependam de normas e de, sempre que possível, soluções não normativas;** **IX – exposição dos possíveis impactos das alternativas identificadas, inclusive quanto aos seus custos;** **X - opinião emitida pela autoridade supervisora sobre a adequação da tecnologia a esta lei.** § 3º (...)

	IX - definição de prazo razoável para eliminação dos dados coletados;
Art. 43. No âmbito de atividades de segurança pública, é vedada a utilização de tecnologias de vigilância diretamente acrescida de técnicas de identificação de pessoas indeterminadas em tempo real e de forma contínua quando não houver a conexão com a atividade de persecução penal individualizada e autorizada por lei e decisão judicial.	**Manutenção integral do texto do art. 43.**
Art. 44. (...) § 1º O Conselho Nacional de Justiça deverá publicar **relatório anual** acerca do uso de tecnologias de monitoramento pelas autoridades competentes no território nacional.	Art. 44. (...) § 1º O Conselho Nacional de Justiça deverá publicar **relatório semestral** acerca do uso de tecnologias de monitoramento pelas autoridades competentes no território nacional.
Art. 53. Sem prejuízo de outras condições exigidas em lei, as autoridades competentes só podem transferir dados pessoais para outro país ou para uma organização internacional, inclusive dados que se destinem a transferências ulteriores para outro país ou outra organização internacional, se: (...) III - os dados pessoais forem transferidos para **agente responsável** no outro país ou na organização internacional competente para fins de atividades de segurança pública ou persecução penal, sem prejuízo do disposto no artigo 57;	Art. 53. Sem prejuízo de outras condições exigidas em lei, as autoridades competentes só podem transferir dados pessoais para outro país ou para uma organização internacional, inclusive dados que se destinem a transferências ulteriores para outro país ou outra organização internacional, se **preenchidas, cumulativamente, as seguintes condições**: (...) III - os dados pessoais forem transferidos para **controlador** no outro país ou na organização internacional competente para fins de atividades de segurança pública ou persecução penal, sem prejuízo do disposto no artigo 57;

Art. 55. (...) II - o **responsável pelo tratamento** tiver avaliado todas as circunstâncias inerentes à transferência de dados pessoais e concluído que existem garantias adequadas no que diz respeito à proteção desses dados. § 1º O **responsável pelo tratamento** informará o Conselho Nacional de Justiça sobre as categorias de transferências abrangidas pelo inciso II. § 2º As transferências baseadas no inciso II serão documentadas, devendo o responsável pelo tratamento disponibilizar ao Conselho Nacional de Justiça, **a pedido deste**, toda a documentação pertinente, incluindo informações sobre a data e a hora da transferência, a autoridade competente que as recebe, a justificação da transferência e os dados pessoais transferidos.	Art. 55. (...) II - o **controlador** tiver avaliado todas as circunstâncias inerentes à transferência de dados pessoais e concluído que existem garantias adequadas no que diz respeito à proteção desses dados, **conforme os critérios previstos no art. 34 da Lei 13.709/18**. § 1º O **controlador** do tratamento informará o Conselho Nacional de Justiça sobre as categorias de transferências abrangidas pelo inciso II. § 2º As transferências baseadas no inciso II serão documentadas, devendo o responsável pelo tratamento disponibilizar ao Conselho Nacional de Justiça, **sem necessidade de pedido por parte deste**, toda a documentação pertinente, incluindo informações sobre a data e a hora da transferência, a autoridade competente que as recebe, a justificação da transferência e os dados pessoais transferidos.
Art. 56. (...) V - em casos específicos, para a **cooperação jurídica internacional**, de acordo com regras e instrumentos de direito internacional.	Art. 56. (...) V - em casos específicos, para a **cooperação jurídica penal internacional**, de acordo com regras e instrumentos de direito internacional.

Art. 57. Em derrogação do disposto do inciso III do artigo 53 e sem prejuízo de um acordo internacional tal como definido no §1º deste artigo, autoridade pública com poderes de prevenção, investigação, detecção ou repressão de infrações penais ou de execução de sanções penais, incluindo a prevenção de ameaças à segurança pública, pode, em casos específicos, transferir dados pessoais diretamente a destinatários estabelecidos em outros países desde que, respeitadas as disposições da presente lei, estejam preenchidas as seguintes condições cumulativas:	Art. 57. Em derrogação do disposto do inciso III do artigo 53 e sem prejuízo de um acordo internacional tal como definido no §1º deste artigo, autoridade pública com poderes de prevenção, investigação, detecção ou repressão de infrações penais ou de execução de sanções penais, incluindo a prevenção de ameaças à segurança pública, pode, em casos específicos, transferir dados pessoais diretamente a destinatários estabelecidos em outros países desde que, respeitadas as disposições da presente lei, estejam preenchidas **todas as** seguintes condições, **de forma cumulativa**:
(...)	(...)
§ 1º Para os fins previstos no caput, por acordo internacional entende-se um acordo internacional bilateral ou multilateral em vigor entre o Brasil e o outro país no campo da **cooperação jurídica internacional** ou da cooperação policial.	§ 1º Para os fins previstos no caput, por acordo internacional entende-se um acordo internacional bilateral ou multilateral em vigor entre o Brasil e o outro país no campo da **cooperação jurídica penal internacional** ou da cooperação policial.
§ 2º A autoridade competente que efetuar a transferência deve informar a **autoridade de controle** sobre as transferências realizadas na forma deste artigo.	§ 2º A autoridade competente que efetuar a transferência deve informar **ao Conselho Nacional de Justiça, autoridade de controle,** sobre as transferências realizadas na forma deste artigo.

Art. 59. O Conselho Nacional de Justiça (CNJ), por meio da sua Unidade Especial de Proteção de Dados em Matéria Penal (UPDP), será responsável por zelar, implementar e fiscalizar a presente lei em todo o território nacional.	Art. 59. O Conselho Nacional de Justiça (CNJ), por meio da sua Unidade Especial de Proteção de Dados em Matéria Penal (UPDP), será responsável por zelar, implementar e fiscalizar a presente lei em todo o território nacional. **Parágrafo único. A Unidade Especial de Proteção de Dados em Matéria Penal não se subordina hierarquicamente ao Plenário do Conselho Nacional de Justiça.**
Art. 60. A diretoria da Unidade Especial de Proteção de Dados em Matéria Penal (UPDP) será composta por 1 (um) Diretor, 3 (três) coordenações especializadas para a aplicação da lei e assessoria técnica. (...) § 2º O Diretor **será escolhido pelo Conselho Nacional de Justiça** dentre brasileiros que tenham reputação ilibada, nível superior de educação e notório saber no campo da proteção de dados ou segurança pública e persecução penal. (...)	Art. 60. A diretoria da Unidade Especial de Proteção de Dados em Matéria Penal (UPDP) será composta por 1 (um) Diretor, 3 (três) coordenações especializadas para a aplicação da lei e assessoria técnica. (...) § 2º O Diretor **será escolhido pelo Presidente da República e por ele nomeado, após aprovação pelo Senado Federal, nos termos da alínea 'f' do inciso III do art. 52 da Constituição Federal**, dentre brasileiros que tenham reputação ilibada, nível superior de educação e notório saber no campo da proteção de dados ou segurança pública e persecução penal. (...) **§ 5º Fica vedado aos ocupantes de cargos na Diretoria da Unidade Especial de Proteção de Dados em Matéria Penal (UPDP) o exercício de outras atividades profissionais de forma concomitante ao período de ocupação do cargo.**

Art. 62. Compete à Unidade Especial de Proteção de Dados em Matéria Penal (UPDP):	Art. 62. Compete à Unidade Especial de Proteção de Dados em Matéria Penal (UPDP):
(...)	(...)
VII - solicitar, a qualquer momento, às **autoridades competentes submetidas a esta lei** informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;	VII - solicitar, a qualquer momento, **aos controladores que realizam tratamento cuja finalidade é a segurança pública e persecução penal**, informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;
(...)	(...)
IX – solicitar relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento **representar alto risco aos direitos previstos nesta Lei;**	IX – solicitar relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento **tenha por finalidade a realização de atividade de segurança pública ou persecução penal;**
(...)	(...)
XI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização sobre o tratamento de dados pessoais **efetuado pelas autoridades competentes**;	XI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização sobre o tratamento de dados pessoais **cuja finalidade seja a realização de atividade de segurança pública e persecução penal**;
(...)	(...)
XIII - comunicar aos **órgãos de controle interno** o descumprimento do disposto nesta Lei pelas autoridades competentes;	XIII - comunicar aos **órgãos de controle internos e externos** o descumprimento do disposto nesta Lei pelas autoridades competentes;
	(...)
	XVI - ser consultada e emitir opiniões sobre medidas legislativas e administrativas que versem sobre

	tratamento de dados pessoais para atividades de segurança pública e de persecução penal;

Capítulo específico para o relatório de impacto à proteção de dados pessoais (RIPD)	
Redação atual	**Redação sugerida**
Sem equivalente no Anteprojeto de Lei	CAPÍTULO ( ) DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS *Inclusão de capítulo específico sobre o relatório de impacto à proteção dos dados pessoais.*
Art. 29. É obrigatória a elaboração de relatório de impacto à proteção de dados pessoais para tratamento de dados pessoais sensíveis, sigilosos, ou em operações que apresentem elevado risco aos direitos, liberdades e garantias dos titulares de dados. § 1º **O Conselho Nacional de Justiça poderá** determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, referente a suas operações de tratamento de dados. § 2º A elaboração e apresentação de relatório de impacto à proteção de dados pessoais também poderá ser requisitada pelo Ministério Público e pela Defensoria Pública na defesa de direitos individuais ou coletivos, quando cabível no exercício de suas atribuições. § 3º Observado o disposto no caput deste artigo, o relatório deverá conter, no	**Art. X.** É obrigatória a elaboração de relatório de impacto à proteção de dados pessoais para tratamento de dados pessoais sensíveis, sigilosos, ou em operações que apresentem elevado risco aos direitos, liberdades e garantias dos titulares de dados**, incluindo, mas não se limitando a, tratamento de dados que:** **I. Envolva decisões tomadas com base em tratamento automatizado que afete os interesses dos titulares;** **II.Envolva o uso de tecnologias de monitoramento** **III. Envolva o uso de novas tecnologias** § 1º **A autoridade supervisora poderá, a qualquer momento e independente dos critérios descritos no caput,** determinar ao controlador que elabore **e publique** relatório de impacto à proteção de dados pessoais, referente a quaisquer das suas operações de tratamento de dados.

mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.	§ 2º A elaboração e apresentação de relatório de impacto à proteção de dados pessoais também poderá ser requisitada pelo Ministério Público e pela Defensoria Pública na defesa de direitos individuais ou coletivos, quando cabível no exercício de suas atribuições. **§ 3º. Os relatórios de impacto elaborados por autoridades competentes responsáveis por tratamento de dados pessoais, cuja finalidade seja a realização de atividades de segurança pública e de persecução penal, deverão ser enviados à autoridade supervisora.** **§ 4º. Observado o disposto no caput deste artigo, o relatório de impacto à proteção de dados deve ser atualizado:** **I - anualmente;** **II - quando da ocorrência de modificações substanciais na forma de realização de tratamento de dados, se comparados com o descrito no relatório de impacto anterior;** **III - após detecção de incidentes de segurança; e** **IV - quando solicitado pela autoridade competente, sob devida justificativa.** **§ 5º.** Observado o disposto no caput deste artigo, o relatório de impacto a proteção de dados deverá conter, no mínimo: I - a descrição da natureza dos dados pessoais tratados; II - as finalidades específicas do tratamento; III - a metodologia utilizada para a coleta e para a garantia da segurança das

	informações IV - **os agentes** de tratamento de dados envolvidos; V - a quantidade de titulares de dados potencialmente atingidos; VI - se houver, informação sobre nova utilização de algum tipo tecnologia; VII - informação sobre a possibilidade de tratamento discriminatório; VIII - as expectativas legítimas do titular de dados; IX - a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados; e **X - com quem são compartilhados os dados advindos do tratamento.**
Art. 26. O relatório de impacto à proteção de dados **que fundamentar decisões automatizadas nos termos desta lei** verificará, entre outros, as medidas tomadas para a garantia da não-discriminação e transparência. § 1º Os parâmetros para verificação da natureza discriminatória contemplarão o peso de dados pessoais, incluindo aqueles referentes à situação socioeconômica e os dados demográficos relacionados à residência ou os demais, sejam potencialmente capazes de revelar informações sensíveis. § 2º Os sistemas responsáveis por decisões automatizadas conforme o caput devem ser auditáveis nos termos a serem determinados pelo Conselho Nacional de Justiça, que não serão restringidos pelo segredo industrial e comercial.	**Art. X+1. O relatório de impacto à proteção de dados verificará, entre outros,** as medidas tomadas para a garantia da não-discriminação e transparência. § 1º Os parâmetros para verificação da natureza discriminatória contemplarão o peso de dados pessoais, incluindo aqueles referentes à situação socioeconômica e os dados demográficos relacionados ao local de residência ou os demais, sejam potencialmente capazes de revelar informações sensíveis. § 2º No caso de relatório de impacto que fundamente decisões automatizadas, os sistemas responsáveis pelas decisões devem ser auditáveis nos termos a serem determinados pela autoridade supervisora, que não serão restringidos pelo segredo industrial e comercial.

§ 3º Os parâmetros a serem considerados na auditoria prevista no § 2º contemplarão, entre outros: I - a precisão, incluindo a taxa de falsos positivos ou falsos negativos; II - a reprodutibilidade e disponibilidade de documentação acerca do seu funcionamento.	§ 3º Os parâmetros a serem considerados na auditoria prevista no § 2º contemplarão, entre outros: I - a precisão, incluindo a taxa de falsos positivos ou falsos negativos; II - a reprodutibilidade e disponibilidade de documentação acerca do seu funcionamento; **III - o grau de interpretabilidade do sistema, de modo a permitir à auditoria a compreensão dos critérios e dos procedimentos utilizados para a realização de uma decisão automatizada.**
Art. 23. (...) §2º O Conselho Nacional de Justiça deverá examinar o relatório de impacto e decidir acerca da possibilidade da decisão automatizada com base no tratamento automatizado de dados, à luz das garantias para os direitos e liberdades do titular e dos riscos apresentados. — Art. 24. (...) § 3º O Conselho Nacional de Justiça deverá examinar o relatório de impacto e decidir acerca da possibilidade da decisão automatizada com base no tratamento automatizado de dados, às luz das garantias para os direitos e liberdades do titular frente aos riscos apresentados.	**Art. X+2. O relatório de impacto referente ao tratamento de dados de elevado risco ou que utilize tecnologias de monitoramento deve conter, além dos requisitos do §5º do art. X, no mínimo:** I - uma descrição do escopo do tratamento e das capacidades da tecnologia de monitoramento; II - testes ou relatórios relativos aos efeitos do tratamento e da tecnologia de monitoramento na saúde e na segurança de pessoas; III – descrição dos impactos potencialmente díspares do tratamento de dados e da tecnologia de monitoramento ou de sua política de uso em quaisquer populações específicas; IV - as medidas previstas para fazer frente aos riscos mencionados nos incisos anteriores; V - as garantias, as medidas de segurança e os mecanismos para

	assegurar a proteção dos dados pessoais e demonstrar a conformidade do tratamento com a presente lei; e VI - a política de uso e as garantias dos direitos dos titulares. **Parágrafo único - Dentre outras, considera-se atividade de tratamento de dados de elevado risco:** **I - definição do risco de envolvimento em infração penal ou de reincidência do titular do dado pessoal por meio do uso de sistemas de decisões automatizadas;** **II – criação de perfil comportamental do titular do dado;** **III - controle sistemático de áreas de grande circulação pública;** **IV - tratamento em larga escala de dados sensíveis;** **V - tratamento em larga escala de dados sigilosos.**
Art. 23. (...) §1º O relatório de impacto à proteção de dados pessoais deve ser publicado na página da autoridade competente e enviado ao Conselho Nacional de Justiça, demonstrando as garantias para a proteção dos direitos e liberdades do titular requeridas no caput, que deverão ser adequadas à natureza dos dados tratados.	**Art. X+3. As autoridades competentes responsáveis pelo tratamento de dados pessoais deverão publicar os relatórios de impacto em seu site oficial.** **Parágrafo único. A autoridade supervisora poderá prever exceções ao disposto no caput.**

Anexo II - Lista de abreviaturas e siglas

AIR	Análise de Impacto Regulatório
ANPD	Autoridade Nacional de Proteção de Dados
CNJ	Conselho Nacional de Justiça
LGPD	Lei Geral de Proteção de Dados
RGPD	Regulamento Geral de Proteção de Dados
RIPD	Relatório de Impacto à Proteção de Dados Pessoais
STF	Supremo Tribunal Federal
TRF	Tecnologia de Reconhecimento Facial
UE	União Europeia
UPDP	Unidade Especial de Proteção de Dados em Matéria Penal

Anexo III - Glossário

Agente de tratamento	De acordo com o art. 5º, IX, da LGPD, controlador e operador são considerados agentes de tratamento.
Autoridade competente	De acordo com a exposição de motivos do Anteprojeto de Lei, a autoridade competente é "a autoridade pública à qual está atribuída a responsabilidade para o exercício de atividades atinentes" à segurança pública e persecução penal, "inclusive a execução de políticas públicas relacionadas à segurança pública".
Autoridade de supervisão	É o órgão responsável pela aplicação, supervisão e monitoramento da legislação referente à proteção de dados para fins de segurança pública e persecução penal em todo o território nacional.
Controlador	De acordo com o art. 5º, VI, da LGPD, o controlador é a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".
Diretiva (UE) 680/2016	É a legislação da União Europeia equivalente à futura lei que o Anteprojeto discute. Diz respeito à "proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados".
Operador	De acordo com o art. 5º, VII, da LGPD, o operador é a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".