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.

DataPrivacyBR

PREFÁCIO

Historicamente, o Brasil tem falhado na formulação de uma política pública eficaz no campo da segurança pública[1] e da persecução penal. Dentre os vários diagnósticos, destacam-se a ausência de um diálogo institucional das diversas entidades – e nos mais diferentes níveis da federação –, a falta de produção de dados confiáveis a instruir a discussão no país e, também, de um quadro jurídico cuja racionalidade foi forjada com base em uma realidade sociotécnica do século passado. O cenário agrava-se, ainda mais, com a introdução de novas tecnologias que, se não modificam por completo, ao menos alteram significativamente os métodos de policiamento e investigação. Nesse contexto, uma lei que governe o tratamento de dados pessoais para fins de segurança pública e persecução criminal apresenta-se como uma das várias ferramentas para mudar tal quadro jurídico-institucional.

No intuito de compreender quais devem ser o conteúdo e a estrutura normativa de uma lei geral sobre tratamento de dados pessoais para fins de segurança pública e investigação criminal – de forma alinhada à LGPD e às práticas internacionais –, a Associação Data Privacy Brasil de Pesquisa produziu o presente documento que comporta: i) nota técnica elaborada pela equipe do Projeto "Novas Fronteiras de Direitos Digitais" do Data Privacy Brasil e encaminhada à Comissão de Juristas designada à elaboração do anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal, bem como ii) parecer intitulado "A esfera protegida dos dados pessoais e as intervenções informacionais do Estado: A dogmática constitucional aplicada ao tratamento de dados na Segurança Pública e no Processo Penal", desenvolvido por uma equipe de consultores contratada especialmente para o aprofundamento dogmático, a fim de melhor embasar a construção das sugestões de dispositivos formuladas pela nota técnica, a partir de diretrizes técnicas para a regulação da proteção de dados nos específicos setores.

O parecer, elaborado por Eduardo Viana, Lucas Montenegro e Orlandino Gleizer, explora o paradigma da ordem jurídica alemã e do direito comunitário da União Europeia e confere parâmetros para o levantamento de dados para atividades de segurança pública e de persecução criminal balizados na proteção ideal da autodeterminação informacional, observadas as apartadas finalidades de tais atividades e as particularidades locais que impedem a transposição automática de modelos internacionais. Possibilita, ainda, a reflexão quanto às atividades restritivas, as reservas de lei e parlamentares, principalmente no âmbito das normas autorizativas de intervenção informacional. Explora aspectos como o bem protegido (segurança pública), o perigo (objeto material da ação estatal) e os destinatários (objeto pessoal da ação estatal) na esfera do direito de segurança pública para, então, embasado no princípio da separação informacional, desenvolver a dogmática da intervenção em direitos fundamentais. Suscitam exemplos como a norma de autorização da identificação eletrônica de veículos automotivos e de telecomunicações e sustentam que os requisitos de uma norma de autorização demandariam mais que a mera referência à segurança pública como bem protegido, sendo o perigo concreto ou abstrato – e, em sendo abstrato, sendo exigido o motivo fundado para a medida interventiva, tal como o requisito formal de licitude.

Enfim, a diretiva anunciada pelos consultores é no sentido: a) do reconhecimento da autodeterminação informacional culminar no dever de abstenção geral do Estado em relação a qualquer dado pessoal; b) da autodeterminação informacional somada a outros direitos que protejam o livre desenvolvimento da personalidade como sendo importantes para a contenção da sensação de vigilância; e

1 VARGAS, Daniel. ***Segurança Pública:*** um projeto para o Brasil. São Paulo: Editora Contracorrente, 2020; SOARES, Luiz Eduardo. ***Desmilitarizar:*** Segurança pública e direitos humanos. São Paulo: Boitempo, 2019.

c) das reservas de lei e parlamentar e da proporcionalidade como exigências para garantir o livre desenvolvimento da personalidade e limitar os acessos irrestrito de dados pessoais, com a consequente necessidade de revisão completa das legislações aplicadas aos setores.

Considerando a conclusão do parecer, a nota técnica busca consolidar sugestões de redação de dispositivos que permitam a aplicabilidade robusta dos princípios da reserva de lei, por meio de uma perspectiva que garanta o amplo direito fundamental à autodeterminação informacional e o livre desenvolvimento da personalidade humana, sob uma compreensão de justiça procedimental para a máxima garantia da ampla defesa e do contraditório. Além disso, explora os princípios do devido processo (informacional e penal), da responsabilização e prestação de contas, do livre acesso, da transparência, do ***accountability*** e da separação dos poderes informacionais.

Dessa forma, na Seção I da nota técnica, sugere-se que, diferentemente do que fez a Lei 13.709/2018, a futura lei procedimentalize, minimamente, a ferramenta de avaliação de impacto. A partir de uma técnica legislativa mais prescritiva que enuncie os critérios para a identificação de quando uma atividade de tratamento de dados será de alto risco, bem como os elementos que deveriam compor tal avaliação. Além disso, recomenda-se a bipartição de dois instrumentos de avaliação de impacto, direcionados para diferentes sujeitos passivos e compreendidos enquanto documentações autônomas, combinando avaliações ***ex ante*** e ***ex post.*** Os relatórios de impacto à proteção de dados – concebidos como documentação "viva" produzida pelo controlador que deve anteceder a atividade de tratamento de dados específica e ser atualizada constantemente – estariam em uma lógica de complementariedade aos de vigilância[2] – arquitetados como documentações capazes de instruir o processo legislativo antes da criação ou da alteração de medidas interventivas informacionais, com a obrigação de considerar a produção de relatórios por parte dos agentes de tratamento de dados, da Autoridade de Proteção de Dados e do que viria ser a nossa sugestão (Seção III) de um "Conselho Nacional de Proteção de Dados na Segurança Pública".

Na Seção II, exploram-se as medidas de transparência e de ***accountability***, no intuito de maior garantia de controle de uma gestão **pública** transparente, responsável e que prime pela justeza procedimental nas atividades de ***law enforcement*** e compliance. Sugere-se a adoção de relatórios estatísticos de transparência que contemplem o devido escrutínio dos componentes do dever de informação e do princípio de transparência, além de fazer referência expressa **à Lei de Acesso à Informação, principalmente no que diz respeito às** medidas ativas de transparência. Recomenda-se a previsão de um procedimento escalonado de auditoria e de ***accountability***, assim como a previsão de portaria de política de vigilância pormenorizada, publicizada e acessível. Sugere-se, ainda, a previsão normativa do conceito de "perfil comportamental" como chave na tomada de decisão automatizada.

Na Seção III, recomenda-se a formação do "Conselho Nacional de Proteção de Dados na Segurança Pública", um órgão multissetorial de atribuições consultiva, deliberativa e de fiscalização (***soft power***) para atuar sobre as questões de tratamento de dados específicos aos campos de atuação da segurança pública e persecução criminal. A criação desse novo conselho – diferente daquele previsto no artigo 58-A da Lei Geral de Proteção – é necessário para que seus representantes possam quebrar o que foi chamado de "isolacionismo institucional" no campo da segurança pública. Daí porque uma composição quadripartite, com articulação da União, dos Estados e Municípios, bem como de representantes do sistema de justiça e da sociedade civil com expertise nesse campo em específico.

A nota técnica possui importantes anexos que ilustram, na forma de quadros comparativos, sistematizações legais e fluxogramas, comparações das legislações estrangeiras e normativas internacionais

2 Compreende-se, da leitura do anteprojeto, a equivalência do relatório de vigilância à avaliação de impacto regulatório.

que foram fruto das pesquisas realizadas pela equipe para embasar as sugestões de redação de dispositivos a serem incorporados ao anteprojeto.

Por fim, é importante ressaltar que a Associação Data Privacy Brasil de Pesquisa tem colaborado com a comissão de juristas, encarregada da elaboração do anteprojeto de lei proteção de dados na segurança pública e persecução criminal, desde o início do ano. Além de ter participado no seminário organizado pela Câmara dos Deputados[3], a primeira versão dessa nota técnica foi encaminhada ao secretariado da comissão, no dia 02 de novembro de 2020.

Bruno Bioni

Daniela Dora Eilberg

3 No dia 08 de julho de 2020, Bruno Bioni, Fundador e Diretor do Data Privacy, participou do seminário internacional sobre proteção de dados pessoais, organizado pela Câmara de Deputados. Disponível em: <https://www.youtube.com/watch?v=f9VRTtlBlaY&feature=youtu.be&t=3568>. Acesso em: 17 nov. 2020.

SOBRE O DATA PRIVACY BRASIL

O Data Privacy Brasil é um espaço de intersecção entre a escola Data Privacy Ensino e a entidade civil Associação Data Privacy Brasil de Pesquisa. Este relatório foi produzido exclusivamente pela Associação.

A Associação Data Privacy Brasil de Pesquisa é uma entidade civil sem fins lucrativos sediada em São Paulo. A organização dedica-se à interface entre proteção de dados pessoais, tecnologia e direitos fundamentais, produzindo pesquisas e ações de incidência perante o sistema de Justiça, órgãos legislativos e governo. A partir de uma Política de Financiamento Ético e Transparência, a associação desenvolve projetos estratégicos de pesquisa em proteção de dados pessoais, mobilizando conhecimentos que podem ajudar reguladores, juízes e profissionais do direito a lidar com questões complexas que exigem conhecimento profundo sobre como tecnologias e sistemas sócio-técnicos afetam os direitos fundamentais. A Associação possui financiamento de filantropias internacionais como Ford Foundation, Open Society Foundations e AccessNow.

Para mais informações, visite www.dataprivacybr.org

Diretores | Bruno Bioni e Rafael Zanatta

Líder de projetos | Mariana Rielli

Coordenadora de incidências | Bruna Martins dos Santos

Coordenadoras de pesquisa | Daniela Dora Eilberg e Izabel Nuñez

Pesquisadores e jornalistas | Aline Hercocivi, Aiuri Rebello, Brenda Cunha, Eduardo Goulart, Gabriela Vergili, João Paulo Vicente, Júlia Mendonça, Helena Secaf, Iasmine Favaro, Marcelo Soares, Marina Kitayama, Pedro Saliba, Thais Aguiar.

Autores | Bruno Bioni, Daniela Dora Eilberg, Brenda Cunha, Pedro Saliba e Gabriela Vergili

Revisores | Mariana Rielli, Rafael Zanatta e Bruna Martins dos Santos.

Arte e diagramação | Júlio Araújo

Como citar este documento |

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.

PROJETO NOVAS FRONTEIRAS DOS DIREITOS DIGITAIS

02 DE NOVEMBRO DE 2020

À COMISSÃO DE JURISTAS DA CÂMARA DE DEPUTADOS RESPONSÁVEL PELA ELABORAÇÃO DO ANTEPROJETO PARA TRATAMENTO DE DADOS PESSOAIS POR ÓRGÃOS DE SEGURANÇA PÚBLICA E PARA FINS DE PERSECUÇÃO CRIMINAL.

ASSUNTO: NOTA TÉCNICA

SUMÁRIO:

SEÇÃO I: AVALIAÇÃO DE IMPACTO 8

A. PANO DE FUNDO, OBJETIVO E RACIONALIDADE. 9

B. COMPLEMENTARIDADE DE RELATÓRIOS DE IMPACTO À PROTEÇÃO DE DADOS E DE VIGILÂNCIA ENQUANTO DOCUMENTAÇÕES AUTÔNOMAS: ANÁLISES EX ANTE E EX POST E UMA MELHOR DELIMITAÇÃO DE QUEM É O SUJEITO PASSIVO 11

SUGESTÕES DE REDAÇÃO 11

SEÇÃO II: MEDIDAS DE TRANSPARÊNCIA E ACCOUNTABILITY: PARA ALÉM DO CONTROLE INDIVIDUAL E A PRODUÇÃO DE ESTATÍSTICAS 16

A. RELATÓRIOS ESTATÍSTICOS DE TRANSPARÊNCIA 17

SUGESTÃO DE REDAÇÃO 18

B. PORTARIAS DE POLÍTICAS DE TECNOLOGIA: AUDITORIA, COMPLIANCE E REFORÇO À LAI 20

SUGESTÕES DE REDAÇÃO 21

C. TOMADA DE DECISÃO AUTOMATIZADA E "PERFIL COMPORTAMENTAL" COMO CONCEITO-CHAVE 22

SUGESTÃO DE REDAÇÃO 23

SEÇÃO III: CONSELHO NACIONAL DE PROTEÇÃO DE DADOS NA SEGURANÇA PÚBLICA E NA PERSECUÇÃO PENAL 24

SUGESTÃO DE REDAÇÃO 26

ANEXO I – LEGISLAÇÕES ESTRANGEIRAS DE RIPDP/PIA - QUADRO COMPARATIVO 30

ANEXO II – RELATÓRIO DE IMPACTO À VIGILÂNCIA - DEFINIÇÃO E SISTEMATIZAÇÃO LEGAL 34

ANEXO III – FLUXOGRAMA RIPDP E AIV E DEVIDO PROCESSO INFORMACIONAL 37

ANEXO IV – QUADRO COMPARATIVO 39

ANEXO V – A ESFERA PROTEGIDA DOS DADOS 45

SEÇÃO I
AVALIAÇÕES DE IMPACTO

I. A. PANO DE FUNDO, OBJETIVO E RACIONALIDADE

Atualmente, o principal ponto de inflexão é fazer com que as avaliações de impacto – do campo ambiental ao da proteção de dados – desencadeiem um circuito em que todas as partes interessadas possam entender e influir em um determinado processo de tomada de decisão. Trata-se de uma questão de **justiça procedimental**[4], sendo que o que está em jogo não diz respeito apenas ao resultado justo, mas, também, que o caminho percorrido para chegar nele também o seja. No campo penal, isso implica a compreensão de um ***devido processo*** "procedimental"[5], bem como uma "justeza procedimental" que conceba a obediência normativa[6] e garanta, assim, a legitimidade de um sistema por meio da conformidade legal e da transparência na tomada de decisão[7].

Nesse sentido, um dos pontos criticáveis da Lei Geral de Proteção de Dados foi não indicar procedimentos mínimos para a confecção do relatório de impacto à proteção de dados[8] (uma das espécies de avaliação de impacto que serão tratadas na nota), que hoje é uma das principais ferramentas de governança em diferentes ordenamentos jurídicos[9]. E, mesmo nos casos em que o legislador adotou uma técnica mais prescritiva, como foi o caso Europeu, na GDPR, ainda existem muitas disputas interpretativas sobre como extrair uma normatividade que desengatilhe uma proteção robusta para os titulares dos dados[10].

Ao fim e ao cabo, avaliações de impacto são tributárias do que se convencionou chamar de **devido processo informacional**[11]. Isto é, assegurar que haja não apenas medidas de transparência, mas de contenção sobre uma decisão que afetará liberdades públicas e individuais[12], além de garantir sua conformidade legal. Com isso, em última análise, garante-se **contraditório e ampla defesa, o que ganha relevo ainda maior na seara penal, uma vez que as decisões ali tomadas impactam** um dos bens jurídicos cuja perda é de maior gravidade: a liberdade de locomoção. Em poucas palavras, tão importante quanto enunciar o devido processo como um dos fundamentos ou princípios da futura

4 DARIUSZ, Kloza. ***Privacy Impact Assessment as a Means to Achieve the Objectives of Procedural Justice***, Jusletter IT. Die Zeitschrift für IT und Recht, disponível em: <https://cris.vub.be/files/49868387/Kloza_2014_PIA_as_a_Means_to_Achieve_the_Objectives_of_Procedural_Justice.pdf>,.

5 GOMES, Luiz Flávio. ***Novo CPP e o devido processo legal, constitucional e internacional (3/4)***. Disponível em: https://professorlfg.jusbrasil.com.br/artigos/121918040/novo-cpp-e-o-devido-processo-legal-constitucional-e-internacional-3-4. Acesso em: 31 out. 2020.

6 OLIVEIRA, Thiago R.; ZANETIC, André; NATAL, Ariadne. Preditores e Impactos da Legitimidade Policial: Testando a Teoria da Justeza Procedimental em São Paulo. Dados, Rio de Janeiro, v. 63, n. 1, e20170159, 2020. Disponível em: <https://nev.prp.usp.br/wp-content/uploads/2020/05/preditores-e-impactos-da-Legitimidade-policial-testando-a-teoria-da-Justeza-procedimental-em-s%C3%A3o-paulo.pdf>. Acesso em: 31 out. 2020. Página 7-40.

7 JOHNSTON, Rachel et al. ***A Study of Procedural Justice & Criminal Justice System Legitimacy:*** ensuring a high quality of justice for all and increasing New Yorkers' trust and confidence in the justice system. The Justice Collaboratory, Yale Law School. Disponível em: https://law.yale.edu/sites/default/files/19yal_mocj_summary_0709_2.pdf. Acesso em: 31 out. 2020.

8 BIONI, Bruno Ricardo; ZANATTA, Rafael A. F.; RIELLI, Mariana Marques. ***Contribuição à Consulta Pública da Estratégia Brasileira de Inteligência Artificial***, Data Privacy Brasil Research, disponível em: <https://www.dataprivacybr.org/wp-content/uploads/2020/06/E-BOOK-CONTRIBUIC%CC%A7A%CC%83O-DPBR-INTELIGE%CC%82NCIA-ARTIFICIAL-FINAL.pdf>,.

9 WRIGHT, David; HERT, Paul De, ***Privacy Impact Assessment***, Países Baixos: Springer Netherlands, 2012.

10 A Associação Data Privacy Brasil de Pesquisa formou uma parceria com o D.PIA.Lab com a finalidade de traduzir alguns de seus textos, de modo a tornar o conteúdo mais acessível no Brasil. Dentre elas está o policy paper: KLOZA, Dariusz, et. al. ***Avaliações de impacto sobre a proteção de dados na União Europeia:*** complementando o novo regime jurídico em direção a uma proteção mais robusta dos indivíduos. D.PIA.Lab, 2020. As traduções mencionadas encontram-se como anexos da: BIONI, Bruno Ricardo; ZANATTA, Rafael A. F.; RIELLI, Mariana Marques. ***Contribuição à Consulta Pública da Estratégia Brasileira de Inteligência Artificial***, Data Privacy Brasil Research, disponível em: <https://www.dataprivacybr.org/wp-content/uploads/2020/06/E-BOOK-CONTRIBUIC%CC%A7A%CC%83O-DPBR-INTELIGE%CC%82NCIA-ARTIFICIAL-FINAL.pdf>.

11 CITRON, Danielle, PASQUALE, Frank. The Scored Society: Due Process for Automated Predictions. Washington Law Review, Vol. 89, 2014.

12 MENDES, Gilmar. ***STF - Voto - Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.389 Distrito Federal - Ministro Gilmar Mendes***. Conjur. Disponível em:<https://www.conjur.com.br/dl/pandemia-reforca-necessidade-protecao.pdf>. "O quadro fático contemporâneo deve ser internalizado na leitura e aplicação da Constituição Federal de 1988. Aliás, ousaria a dizer que nunca foi estranha à jurisdição constitucional a ideia de que os parâmetros de proteção dos direitos fundamentais devem ser permanentemente abertos à evolução tecnológica".

lei, é articular medidas para a sua concreção. A esse respeito, um dos principais gargalos é um capítulo que procedimentalize avaliações de impacto.

A partir desse pano de fundo, é essencial que o anteprojeto de lei arquitete elementos que:

a) definam as **hipóteses de obrigatoriedade** da elaboração de avaliações de impacto e quem é o seu respectivo sujeito passivo;

I. No caso do relatório de impacto como obrigação direcionada aos agentes de tratamento de dados, o elemento disparador deve ser o risco. Isto é, depois que haja uma previsão legal acerca da medida interventiva informacional, ainda assim os agentes de tratamento de dados devem elaborar avaliações de impacto. O que se busca nesse momento é um **juízo de valor** concreto levando em consideração a tecnologia específica contratada ou desenvolvida e o tratamento de dados para fins de persecução criminal ou segurança pública;

II. Como uma medida de reforço ao princípio da reserva legal, a elaboração de avaliação de impacto deve ser direcionada não apenas aos agentes de tratamento de dados por meio dos relatórios de impacto à proteção de dados, mas, também, ao legislador quando autorizar medidas interventivas. Tal documentação deverá instruir o processo legislativo, de modo a considerar quais são as medidas de salvaguardas para que tal interferência seja proporcional. Por ser uma **análise em abstrato**, o risco não deve ser o elemento disparador da obrigatoriedade de tal avaliação de impacto. É uma proposta que se inspira no que se convencionou chamar de relatório de impacto legislativo[13], para que a elaboração de leis seja baseada em evidências, ainda mais quando interfere em um direito fundamental. Nessa proposta, a denominação para essa avaliação é relatório de impacto de vigilância.

b) apontem quais os **componentes ou a estrutura mínima** que tal documentação deve observar, considerando as particularidades de cada sujeito passivo (e.g., legislador vs. agentes de tratamento de dados) de tal obrigação e a função das espécies de avaliações de impacto (relatório de impacto e relatório de impacto de vigilância);

c) assegurem **participação das partes afetadas**, de modo que a decisão tomada não seja fruto de um juízo de valor apenas por alguns atores, o que pode desencadear decisões enviesadas. Deve-se pensar em arranjos de co-deliberação, como ocorre em algumas leis estrangeiras (e.g., São Francisco para reconhecimento facial[14]).

13 EUROPEAN COMMISSION. ***Impact Assessments.*** Disponível em: <https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/impact-assessments_en>. Acesso em: 31/10/2020. "Impact assessments examine whether there is a need for EU action and analyse the possible impacts of available solutions. These are carried out during the preparation phase, before the Commission finalises a proposal for a new law. They provide evidence to inform and support the decision-making process".

14 BIONI, Bruno; LUCIANO, Maria; RIELLI, Mariana. ***Regulação de reconhecimento facial em São Francisco.*** JOTA, 2020. Disponível em: <https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/regulacao-de-reconhecimento-facial-em-sao-francisco-25062019>

I. B. COMPLEMENTARIDADE DE RELATÓRIOS DE IMPACTO À PROTEÇÃO DE DADOS E DE VIGILÂNCIA ENQUANTO DOCUMENTAÇÕES AUTÔNOMAS: ANÁLISES *EX ANTE E EX POST* E UMA MELHOR DELIMITAÇÃO DE QUEM É O SUJEITO PASSIVO

Avaliações de impacto surgiram como parte do movimento de políticas públicas baseadas em evidência[15], de modo a reduzir a discricionariedade dos agentes estatais. Ao longo desse processo, notou-se cada vez mais a necessidade de que o **exercício de motivação**, contido em tais avaliações, **fosse revisado e atualizado**. Dito de outra forma, tal documentação não deveria ser produzida apenas antes de uma tomada de decisão, mas, também, depois dela, com o objetivo de garantir sua própria manutenção ou mesmo deflagar a sua descontinuação[16].

A partir desse histórico, é importante ressaltar que avaliação de impacto é o gênero de uma série de medidas criadas, ao longo do tempo, com o objetivo de especificar esse exercício de motivação. Nesse sentido, uma possível sistematização de tipos de avaliação de impacto seria considerar que tais espécies reduziram a assimetria de informação de forma *ex ante* e *ex post*:

a) relatórios de vigilância representam uma **documentação capaz de instruir o processo legislativo**, de modo que as prerrogativas legais de tratamento de dados para fins de persecução penal e segurança pública sejam um processo informado que considere outras documentações a serem produzidas pelos agentes de tratamento de dados, pela Autoridade Nacional de Proteção de Dados e pelo Conselho Nacional de Proteção de Dados na Segurança Pública;

b) relatórios de impacto são **uma documentação produzida pelo controlador,** que deve antecipar uma atividade de tratamento de dados específica, para fins de persecução penal e segurança pública, e ser atualizada ao longo do seu desenvolvimento;

SUGESTÃO DE REDAÇÃO 1	
DEFINIÇÃO DE RELATÓRIO DE IMPACTO DE VIGILÂNCIA	**COMENTÁRIOS**
relatório de impacto de vigilância: documentação que instruirá o processo legislativo que autorizará o tratamento de dados pessoais para fins de persecução penal e segurança pública. Implica elevado risco às liberdades civis e aos direitos fundamentais. Deve conter sua descrição e das respectivas medidas de salvaguardas e mecanismos de mitigação de riscos.	Uma vez que o legislador não se enquadra na figura de controlador *strictu sensu*, é necessário então criar uma hipótese em que se explicite sua posição de sujeito passivo da obrigação de produção de um relatório de impacto específico.
TOPOGRAFIA Dispositivo a ser incluído na parte conceitual ou de definição da lei	

15 BIONI, Bruno; LUCIANO, Maria. *O Princípio da Precaução na Regulação de Inteligência Artificial:* Seriam as Leis de Proteção de Dados o seu Portal de Entrada? In: Inteligência Artificial e Direito- Ética, Regulação e Responsabilidade. São Paulo: Thomson Reuters, 2019, p. 207-231.

16 Gomes, Maria Cecília Oliveira. Relatório De Impacto à Proteção De Dados Pessoais: Uma Breve Análise Da Sua Definição e Papel Na LGPD. *Revista da AASP*, n. 144, 2019, p. 6-15. Disponível em: <https://www.academia.edu/41160034/Relat%C3%B3rio_de_Impacto_a_Prote%C3%A7%C3%A3o_de_Dados_Pessoais_uma_breve_an%C3%A1lise_da_sua_defini%C3%A7%C3%A3o_e_papel_na_LGPD>

SUGESTÃO DE REDAÇÃO 2	
DEFINIÇÃO DE RELATÓRIO IMPACTO À PROTEÇÃO DE DADOS	**COMENTÁRIOS**
relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como as medidas, salvaguardas e mecanismos de mitigação de risco.	Com o objetivo de assegurar um paralelismo entre a LGPD e a futura lei, poderia ser adotada a mesma definição da Lei 13.709/2018.
TOPOGRAFIA Dispositivo a ser incluído na parte conceitual ou de definição da lei	

SUGESTÃO DE REDAÇÃO 3	
SEÇÃO DE ELEVADO RISCO	**COMENTÁRIOS**
(S/N) Quando um tratamento de dados resultar em alto risco para os direitos e liberdades fundamentais do titular dos dados, deverá ser antecedido de uma avaliação de impacto nos termos dos artigos S/N e S/N. §1º - Para fins de avaliação do risco, deve-se considerar: I - a natureza dos dados pessoais; II - as finalidades do tratamento de dados; III - a quantidade de agentes de tratamento de dados envolvidos; IV – a quantidade de titulares de dados potencialmente atingidos e; V - se é utilizado algum tipo de nova tecnologia; §2º - Dentre outras, considera-se como atividade de tratamento de dados de elevado risco: I - processo de decisões automatizadas para definir o risco de envolvimento em infração penal ou de reincidência do titular do dado pessoal ou; II – criação de perfil comportamental do titular do dado ou;	Em havendo a bipartição de dois instrumentos de avaliação de impacto e direcionados para diferentes sujeitos passivos, uma boa técnica legislativa seria uma seção que explicite e defina os critérios de uma atividade de alto risco, bem como um rol exemplificativo de tais atividades.

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;	

TOPOGRAFIA

Dispositivos de uma seção do capítulo de Avaliações de Impacto

SUGESTÃO DE REDAÇÃO 4	
SEÇÃO DE RELATÓRIO DE IMPACTO DE VIGILÂNCIA	**COMENTÁRIOS**
(S/N) O tratamento de dados pessoais de elevado risco para direitos, liberdades e garantias dos titulares dos dados dependerá de previsão legal específica, cujo processo legislativo deverá ser instruído por relatório de impacto de vigilância: §1º. O relatório de impacto de vigilância deve considerar e conter: I – os relatórios estatísticos previstos no artigo (S/N - vide sugestão vide sugestão de redação 1 da Seção II.A); II - os relatórios anuais da Autoridade Nacional de Proteção de dados Pessoais acerca do uso de tecnologias de vigilância pelas autoridades competentes no território nacional; III - Os relatórios anuais da Autoridade Nacional de Proteção de dados Pessoais; nos termos do artigo 55-J, XII da Lei No 13.709/2018; IV - os relatórios anuais do Conselho Nacional de Proteção de Dados na Segurança Pública; V - os relatórios anuais do Conselho Nacional de Proteção de Dados, nos termos do artigo 58-B, II da Lei No 13.709/2018; VI - os riscos às liberdades civis e aos direitos fundamentais, com as respectivas medidas de salvaguardas e mecanismos de mitigação de riscos §2º. No processo legislativo, o relatório de impacto de vigilância deverá ser submeti-	A obrigação de produção de relatórios (e.g., estatísticos) por parte dos agentes de tratamento de dados, da Autoridade Nacional de Proteção de Dados e do Conselho Nacional de Proteção de Dados na Segurança Pública deve, necessariamente, instruir o processo legislativo que dará lastro às intervenções informacionais para fins de persecução penal e segurança pública. Com isso, cria-se um processo de tomada de decisão possivelmente informado por evidências empíricas acerca dos acertos e das falhas do estado da arte das atividades de tratamento de dados em questão. Trata-se de uma lógica que combina avaliações *ex ante* e *ex post.*

do à consulta pública e ampla participação social e com a oitiva da: I - Autoridade Nacional de Proteção de Dados; II - Conselho Nacional de Proteção de Dados na Segurança Pública;	

TOPOGRAFIA
Dispositivos de uma seção do capítulo de Avaliações de Impacto

SUGESTÃO DE REDAÇÃO 5	
SEÇÃO DE RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS	**COMENTÁRIOS**
(S/N). O controlador deve elaborar relatório de impacto à proteção de dados pessoais para tratamento de dados de elevado risco aos direitos, liberdades e garantias dos titulares de dados. §1º O relatório deverá conter, no mínimo: I - descrição: a) dos tipos de dados coletados; b) das finalidades do tratamento e das capacidades da tecnologia de vigilância; c) de quaisquer testes ou relatórios relativos aos efeitos do tratamento e da tecnologia de vigilância na saúde e na segurança de pessoas; d) de quaisquer impactos potencialmente díspares do tratamento de dados; e) do envolvimento e da recomendação de encarregado; f) das garantias, das medidas de segurança e dos mecanismos para assegurar a proteção dos dados pessoais e demonstrar a conformidade do tratamento com a presente lei; e g) de auditoria interna e mecanismos de supervisão para garantir a conformidade das atividades de tratamento de dados.	Procedimentalizar minimamente quais os elementos a compor os Relatórios de Impacto à Proteção de Dados para garantir um nível de aplicação robusto dos princípios em questão.

II - políticas:

a) de uso e as garantias dos direitos dos titulares, conforme o disposto no S/N (considerando que haverá artigos a esse respeito);

b) de segurança e sigilo nos termos do capítulo S/N (considerando que haverá um capítulo a esse respeito);

c) de retenção, acesso e uso dos dados tratados;

d) das hipóteses de uso compartilhado, nos termos artigo S/N (considerando que haverá artigos a esse respeito);

e) de treinamento dos indivíduos que realizarão o tratamento, utilizarão a tecnologia de vigilância ou terão acesso aos bancos de dados e;

f) de atualização e revisão do relatório de impacto à proteção de dados

VII – metodologia utilizada para:

a) coleta e o tratamento de dados, especialmente se for automatizado;

b) criação de perfil comportamental dos titulares de dados;

c) identificação e classificação dos riscos;

d)medidas adotadas de salvaguardas e mecanismos de mitigação de risco, especialmente acerca da sua eficácia nos termos do S/N (princípio da responsabilização e prestação de contas).

§2º Consideradas as diretrizes do Conselho Nacional de Proteção de Dados na Segurança Pública, a autoridade nacional emitirá;

I - opiniões técnicas sobre as exceções e quais elementos do relatório de impacto à proteção de dados não devem ser públicos;

II - recomendações sobre consultas públicas e o envolvimento de representantes dos titulares de dados na elaboração de relatórios de impacto à proteção de dados;

TOPOGRAFIA

Dispositivos de uma seção do capítulo de Avaliações de Impacto

SEÇÃO II
MEDIDAS DE TRANSPARÊNCIA E *ACCOUNTABILITY*: PARA ALÉM DO CONTROLE INDIVIDUAL E A PRODUÇÃO ESTATÍSTICAS

II.A. RELATÓRIOS ESTATÍSTICOS DE TRANSPARÊNCIA

Tão importante quanto assegurar direitos ao titular do dado para redução da assimetria de informação é arquitetar deveres por parte dos atores no campo da segurança pública e da persecução criminal que permitam controle social sobre suas atividades. A necessidade de uma Lei Geral de Proteção de Dados penal embasada em transparência e ***accountability*** perfaz a aquisição de dados de pessoas investigadas e daquelas que sequer são alvo de investigação criminal e têm seus dados colhidos – seja no cotidiano das atividades dos órgãos de segurança pública ou por reflexo de investigações com coleta massiva de dados[17]. Portanto, não se trata apenas da cadeia de custódia da prova digital – que de fato, é essencial para um processo penal democrático e está relacionada ao ciclo de vida do dado na forma como a LGPD a dispõe –, mas do controle transparente e responsável de quais dados são colhidos, por quais órgãos, para quais órgãos são transmitidos e por quê, sendo o controle desse caminho percorrido imprescindível para o exercício de um Estado Democrático de Direito.

Além disso, considerando o fato de que a etapa inicial de grande parte das investigações de crimes por meio das tecnologias implica a coleta de evidências armazenadas de provedores de serviços terceirizados[18], o que se busca é o controle das aquisições de fonte de provas digitais[19]. A transparência dos dados e da construção metodológica desses dados, assim como o ***accountability*** são inerentes ao controle e à gestão pública legítima e, nesse sentido, seria de extrema valia que o anteprojeto dispusesse sobre relatórios estatísticos de transparência[20] que, de forma qualificada, contemplem:

- Metodologia dos dados (cobertura e qualidade técnica);
- Número de pedidos sobre conteúdo e metadados com o registro do órgão;
- Número de consultas (autorizações) sobre conteúdo e metadados com fundamentação criterizada e registro do órgão;
- Auditorias de controladores;
- Número de transferência e compartilhamento de dados entre órgãos;
- Procedimentos de minimização detalhando os requisitos para adquirir, armazenar e compartilhar os dados;
- Análises de compliance referente aos procedimentos de minimização do ano anterior e a cada um dos órgãos;
- Procedimentos de anonimização dos dados para garantia da privacidade de vítimas;
- Falhas relatadas com o tratamento dos dados e procedimentos de correção em curso

Não sendo a transparência um fim em si mesmo, mas um caminho à inteligibilidade[21], a necessidade de algoritmos responsáveis também é uma aposta urgente, sendo viável divulgar informações sobre

17 Como recentemente vimos com a decisão da Terceira Seção do STJ que, por 8 votos a 1, manteve a ordem para que o Google entregue dados para embasar a investigação dos assassinatos de Marielle Franco e Anderson Gomes.

18 KERR, Orin. Digital evidence and the new criminal procedure. ***Columbia Law Review***, v. 105, n. 279, 2005. pp. 279-318.

19 Aqui compreendidas as inúmeras modalidades em que uma informação no formato eletrônico pode ser produzida, armazenada ou transmitida. In: MARTÍN, Joaquín Delgado. ***Investigación tecnológica y prueba digital en todas las jurisdicciones.*** 2 ed. Wolters Kluwer, 2018.

20 Quanto ao ponto, inclusive, é com base no ***Principles of Intelligence Transparency da Intelligence Community (IC) que até mesmo o Foreign Intelligence Surveillance Act of 1978 (FISA)*** prevê a elaboração de um relatório estatístico de transparência, nos termos do 50 U.S.C. § 1873(a). Outro exemplo observado para fins de desenvolver o que deveria ser contemplado disponível em: https://data.police.uk/about.

21 PASQUALE, Frank. Restoring transparency to automated authority. ***J. on Telecomm. & High Tech. L.***, v. 9, p. 235, 2011. CITRON, Danielle Keats; PASQUALE, Frank. Network accountability for the domestic intelligence apparatus. ***Hastings Law Journal***, v. 62, p. 1441, 2010.

algoritmos em termos de prestação judicial sem divulgar o código-fonte[22]. A transparência ativa requer que o cumprimento do art. 5º, XXXIII, da CF se faça de forma publicizada, ainda que não solicitada[23], ressalvados os amparos legais de sigilo e não identificação. Portanto, a publicização de pesquisas de diagnóstico interno corrobora com a teoria da justeza social e com a legitimidade do sistema.

SUGESTÃO DE REDAÇÃO 1	
CAPÍTULO DE TRANSPARÊNCIA E ACESSO À INFORMAÇÃO	**COMENTÁRIOS**
(S/N). As autoridades competentes informarão as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a base legal, a finalidade, os objetivos específicos, os procedimentos e as práticas utilizadas para a execução dessas atividades. §1º. As informações a que se refere este artigo serão detalhadas em lei ou regulamento; § 2º. As informações sobre o tratamento de dados devem ser disponibilizadas em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos, de forma clara, adequada e ostensiva, devendo incluir, entre outros, elementos previstos em regulamentação para o atendimento do princípio do livre acesso, sobre: I - finalidade específica do tratamento; II - forma, escopo e duração do tratamento; III - políticas de retenção, descarte e acesso; IV- identificação do controlador; V - informações de contato do controlador; VI - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VII - responsabilidades dos agentes que realizarão o tratamento; e	Historicamente, o fio condutor das leis de proteção de dados é um controle individual por parte do próprio titular dos dados. Contudo, fica cada vez mais evidente a necessidade de uma virada na direção de um controle social. Esse é, também, um dos sentidos do termo contravigilância, em que se busca evidenciar as atividades de vigilância sobre escrutínio, especialmente para que as entidades de direitos difusos e coletivos possam não só ter acesso, mas, também, julgar a prestação de contas das - uma dos eixos principais do princípio de *accountability* - atividades de *law enforcement*. Nesse sentido, há uma janela de oportunidade para um capítulo que: a) detalhe quais são os componentes do dever de informação e, em última análise, do princípio da transparência e; b) faça deferência à Lei de Acesso à Informação, especialmente sobre medidas ativas de transparência.

22 KROLL, Joshua A. et al. Accountable Algorithms, *University of Pennsylvania Law Review*, pp 633-705. p.

23 RIO GRANDE DO SUL. Assembleia Legislativa. Projeto de Lei nº 82/2019. Dispõe sobre a transparência dos registros da área da segurança pública e dá outras providências. Disponível em: http://www.al.rs.gov.br/legislativo/ExibeProposicao/tabid/325/SiglaTipo/PL/NroProposicao/82/AnoProposicao/2019/Default.aspx?Dod=13/10/2020. Acesso em: 31 out. 2020.

VIII - direitos do titular, com menção explícita aos direitos contidos no art. 20 desta Lei;

IX - auditorias dos agentes de tratamento de dados;

X- procedimentos de minimização detalhando os requisitos para adquirir, armazenar e compartilhar os dados;

XI - incidentes de segurança nos termos do art. S/N;

XII - procedimentos de anonimização dos dados para garantia da privacidade de vítimas

§2º. A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento, especialmente tendo em vista a garantia da segurança pública e atividades de repressão, investigação e persecução de infrações penais e execução da pena.

(S/N). A autoridade máxima de cada autoridade competente publicará, anualmente, em seu sítio na internet, relatórios estatísticos de requisição de dados pessoais para atividades de persecução penal e segurança pública, contendo:

I - o número de pedidos realizados sobre:

a) dados sigilosos;

b) dados pessoais sensíveis e;

c)dados pessoais, especialmente de registros de conexão e aplicação nos termos do artigo 5º, VI e VIII, da Lei 12.965/2014

II - a natureza dos dados solicitados;

III - a listagem das pessoas jurídicas de direito privado aos quais os dados foram requeridos;

IV - o número de pedidos deferidos e indeferidos judicialmente; e

V - o número de titulares afetados por tais solicitações.

(S/N). Os prazos e procedimentos para exercício dos direitos do titular observarão o disposto em legislação específica, em

especial as disposições constantes da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), em especial o artigo 8º.	

TOPOGRAFIA

Dispositivo que consiste em um capítulo da APL

II.B. PORTARIAS DE POLÍTICAS DE TECNOLOGIA: AUDITORIA, *COMPLIANCE* E REFORÇO À LAI

No que tange à transparência das atividades dos agentes de tratamento de dados, é necessária a previsão das contratações por meio de determinadas políticas de tecnologia de vigilância e publicizá-las na forma de **Portaria de Política de Tecnologia de Vigilância**[24], com descrição de produtos e serviços, das finalidades, das políticas de usos e regras, das salvaguardas precisas, de transparência robusta, dos formatos de armazenamento e acesso aos dados, com as autorizações de acesso, das salvaguardas gerais, do prazo de retenção das informações, dos treinamentos, dos casos específicos em que há compartilhamento com o Ministério Público, dos procedimentos implantados para o devido *compliance* e da responsabilização pelo mau uso[25].

Sendo assim, quando o tratamento de dados tiver finalidade relacionada à persecução criminal ou segurança pública, o controlador, como figura competente para a tomada de decisão sobre o tratamento de dados, apenas poderá ser uma entidade pública que corresponda à autoridade competente. Dentre suas obrigações, é importante que audite anualmente o uso de equipamentos ou serviços de tecnologia de vigilância e a conformidade de tal uso com uma respectiva portaria de política de tecnologia de vigilância aprovada e de auditoria (previsão na seção I).

Desse modo, empresas privadas somente poderão ocupar a posição de co-controlador ou operador de dados – devendo sempre uma entidade pública figurar como controladora na cadeia de tratamento de dados. Quando a atividade de tratamento de dados demandar segunda contratação (e.g. empresa privada contratada para organizar dados em um banco de dados, mas precisa terceirizar o serviço de armazenamento), deverá ser executada por meio de autorização expressa do controlador. Além disso, é importante reiterar que a formalização deve ser registrada, auditada e publicizada nos Portais de Transparência.

Não bastam as exigências de medidas de transparência e de informe sobre o tratamento de dados à Autoridade Nacional de Proteção de Dados, tampouco a divulgação de tais operações em veículos de fácil acesso, já que há a possibilidade de que tais informações fiquem dispersas e fragmentadas, dificultando o controle e fiscalização pela sociedade civil ou pelo próprio poder público. É por essa razão que se sugere que **toda e qualquer operação que faça uso de tecnologias de vigilância em ações de segurança pública deva:** i) **ser submetida**, primeiramente, **a um processo de avaliação e autorização por autoridade competente**; ii) ser a **autorização procedimentalizada,** exigindo-se que a solicitação a ser pleiteada junto à autoridade inclua finalidade e resultados previstos/almejados a partir do uso dessa tecnologia, no intuito de mensurar se a finalidade é coerente com a perspectiva de eficiência/eficácia na segurança pública**;** iii) compor **um registro nacional de acesso público,**

24 Inspirada na regulação de reconhecimento facial de São Francisco, Disponível em: https://sfgov.legistar.com/LegislationDetail.aspx?ID=3850006&GUID=12FC5DF6-AAC9-4F4E-8553-8F0CD0EBD3F6

25 Assim o faz a regulação mencionada na nota anterior.

onde estão inseridas as informações detalhadas do objeto em questão: os atores envolvidos, o prazo de execução, o tratamento, a eliminação, além das salvaguardas já previstas no anteprojeto.

SUGESTÃO DE REDAÇÃO 2	
SEÇÃO DE ELEVADO RISCO	**COMENTÁRIOS**
(S/N). As decisões sobre a autorização e a maneira como devem ser financiadas, adquiridas ou utilizadas as tecnologias de vigilância, bem como a forma como devem ou não ser compartilhados os dados delas provenientes dependem de um procedimento escalonado de auditorias. (S/N). Durante a vigência da contratação, a auditoria deve ser em conformidade com as medidas técnicas, organizativas e previsões legais, devendo as políticas em matéria de proteção de dados pelo controlador ser devidamente aplicadas em conformidade com cada finalidade específica de tratamento;	A necessidade de um procedimento escalonado de auditoria e de *accountability*, bem como o registro em uma portaria de política de vigilância são imprescindíveis para as decisões sobre como devem ser financiadas, adquiridas ou utilizadas as tecnologias de vigilância.
TOPOGRAFIA Dispositivos de uma seção do capítulo de Avaliações de Impacto	

SUGESTÃO DE REDAÇÃO 3	
PORTARIA DE POLÍTICA DE VIGILÂNCIA	**COMENTÁRIOS**
(S/N). A portaria de política de tecnologia de vigilância deve, além de exigir o relatório de impacto de vigilância, determinar a composição das autoridades competentes da auditoria e a descrição: I - dos produtos e serviços de tecnologias de vigilância adotados; II - das finalidades do uso da tecnologia e detalhamentos dos dados que podem ser adquiridos; III - das políticas de usos e regras das tecnologias; IV - dos formatos de armazenamento, transmissão e acesso dos dados; V - das salvaguardas precisas de proteção da informação que não pode ser acessada, tais como mecanismos de controle de	A previsão das contratações e o detalhamento das descrições devem se dar por meio de portaria de política de tecnologia de vigilância publicizada e acessível.

acesso e criptografia e a expressa previsão de quem estaria autorizado a acessar; VI - do prazo estipulado e limitado para o armazenamento dos dados colhidos e procedimento para o seu descarte; VII - das previsões expressa das possibilidades de transmissão; VIII - dos procedimentos implantados para o devido compliance e da responsabilização pelo mau uso. (S/N). A portaria de política de tecnologia de vigilância deve ser tornada publicamente acessível pela internet e em formato interoperável. (S/N). O Registro Nacional de Portarias de Política de Tecnologia de Vigilância deverá ser mantido pelo Ministério da Justiça e Segurança Pública e será regulamentado por normas específicas. (S/N). O Registro Nacional de Portarias de Política de Tecnologia de Vigilância deverá ser mantido pelo Ministério da Justiça e Segurança Pública e será regulamentado por normas específicas.	
TOPOGRAFIA Dispositivo a ser incluído na Seção de Transparência	

II.C TOMADA DE DECISÃO AUTOMATIZADA E "PERFIL COMPORTAMENTAL" COMO CONCEITO-CHAVE

Quando se criam inferências a respeito de preferências pessoais por tecnologias de informação e comunicação/TICs – que têm capacidade de extrair informações de uma pessoa natural de diversas fontes, especialmente dos seus rastros digitais – evidencia-se a prática da denominada "perfilização". Devido ao alto risco de tal prática reforçar desigualdades e vieses já existentes[26], leis gerais de proteção de dados têm calibrado de forma mais intensa obrigações por encarar tal tipo de tratamento de dados como sendo de alto risco[27].

26 Pesquisas científicas como a de Cathy O'Neil e Virginia Eubanks demonstram como algoritmos e sistemas de análise de big data podem causar consequências socioeconômicas para milhares de pessoas a partir da reprodução de desigualdades já existentes, tanto na esfera pública como na esfera privada. O'NEIL, Cathy. ***Weapons of math destruction:*** How big data increases inequality and threatens democracy. Broadway Books, 2016. EUBANKS, Virginia. ***Automating inequality:*** How high-tech tools profile, police, and punish the poor. Nova Iorque: St. Martin's Press, 2018.

27 ZANATTA, Rafael; A. F.; SOUZA, Michel R. O. A tutela coletiva na proteção de dados pessoais: tendências e desafios, In: DE LUCCA, Newton; ROSA, Cíntia. ***Direito & Internet.*** IV: Proteção de Dados Pessoais. São Paulo: Quartier Latin, 2019. ISBN: 9788574538389. ZANATTA, Rafael. ***Proteção de dados pessoais como regulação de risco: uma nova moldura teórica?***1. I Encontro da Rede de Pesquisa em Governança da Internet, Novembro de 2017. Disponível em: <http://www.redegovernanca.net.br/public/conferences/1/anais/ZANATTA,%20Rafael_2017.pdf>. Acesso em: 31 out. 2020.

Nesse sentido, deveres de informação, explicação, revisão e elaboração de relatórios de impacto à proteção de dados pessoais são medidas de contenção[28] que muitas vezes são ativados quando o perfilamento instrumentaliza um processo de tomada decisão. Portanto, é um conceito que, via de regra, é um elemento normativo que atravessa vários dos eixos de uma lei de proteção de dados. Por exemplo, a Lei Geral de Proteção de Dados fia-se ao: a) termo perfil comportamental para considerar: em quais hipóteses dados anonimizados podem ser considerados dados pessoais (art. 12, §2º); b) termo perfil pessoal para delimitar quando o titular tem direito à revisão de decisões automatizadas (art. 20, caput).

Além de não uniformizar tal terminologia, a LGPD não enunciou um conceito para perfil comportamental, o que tende a dificultar o seu processo de aplicação e interpretação. Diferentemente, a GDPR prescreveu uma definição para tal conceito jurídico e a ele faz referência ao longo de todo o seu corpo normativo. Recomenda-se, por isso, que o anteprojeto de lei estabeleça tal estratégia para que se evita dubiedade hermenêutica.

SUGESTÃO DE REDAÇÃO 4	
SEÇÃO DE ELEVADO RISCO	**COMENTÁRIOS**
(S/N). – Perfil comportamental: qualquer forma de tratamento parcial ou automatizado de dados para avaliar certos aspectos pessoais de uma pessoa natural, especialmente com relação ao seu desempenho profissional, a sua situação econômica, saúde, preferências pessoais, interesses, localização.	Ao prescrever tal definição, deve-se uniformizar a terminologia do restante dos dispositivos e utilizá-la como gatilho para reforçar deveres de informação, revisão, explicação e como critério para mensuração se uma atividade de tratamento de dados é de alto risco
TOPOGRAFIA Dispositivo a ser incluído na parte conceitual ou de definição da lei	

28 Bennett Moses, Lyria; de Koker, Louis. ***Open Secrets:*** Balancing Operational Secrecy and Transparency in the Collection and Use of Data by National Security and Law Enforcement Agencies", MelbULawRw, n. 32, v. 41 (2), Melbourne University Law Review, 2017.

SEÇÃO III
CONSELHO NACIONAL DE PROTEÇÃO DE DADOS NA SEGURANÇA PÚBLICA E NA PERSECUÇÃO PENAL

A formação de um conselho nacional como órgão consultivo, deliberativo e de fiscalização ***soft-power*** para atuar sobre as questões de tratamento de dados específicos aos campos de atuação da segurança pública e persecução criminal tem como um de seus fundamentos suprir parte das demandas decorrentes do quadro de fragmentação do sistema de segurança pública. Isso se conecta a um debate maior sobre a "arquitetura institucional da segurança pública", que pode ser entendida como "as instituições que atuam no campo da segurança pública, em todo o país, e o arranjo formal que limita, impõe e dita os termos de suas inter-relações, estabelecendo também as condições nas quais dar-se-ão as conexões entre elas e as instituições que pertencem ao campo específico da segurança pública"[29].

Em seu recente livro "Segurança Pública: um projeto para o Brasil"[30], Daniel Vargas aponta que o principal problema desta importante política pública é o isolacionismo institucional. Seria necessário pensar em um paradigma cooperativo através de três eixos:

> i. vertical, para que houvesse coordenação entre os diferentes níveis da federação, o que deveria ser com base em dados – não em achismos –, com horizontes claros – metas e parâmetros de avaliação;
>
> ii. horizontal, para que municípios e estados pudessem dialogar com polícia, ministério público, judiciário e sistema penitenciário- i.e., todo o ecossistema da segurança pública; e
>
> iii. transversal, cujo foco de colaboração seria a antessala da criminalidade, de modo que advogados, defensores públicos e outras ferramentas de não criminalização – educação e cultura – também pudessem dialogar;

Em meio à discussão de uma lei geral de proteção de dados para fins de segurança pública e persecução penal, há uma janela de oportunidade para quebrar, pelo menos parte do mencionado ruído de comunicação e cooperação dos atores do ecossistema da Segurança Pública. Tal como fez a Lei Geral de Proteção de Dados Pessoais com a previsão de um conselho multissetorial (artigo 58-A), propõe-se a criação de um novo conselho que possa estimular a "descentralização com integração sistêmica e unidade axiológica"[31], em um arranjo cooperativo e de descentralização federativa. A criação de um novo conselho faz-se necessária justamente para que o seu perfil seja composto por representantes com expertise no campo de proteção de dados e se constitua como um ***policy paper***[32] para articulação institucional no campo da segurança pública.

Sugere-se a institucionalização desse espaço na forma de um modelo quadripartite, isto é, composto por representantes: a) da União; b) dos Estados e Municípios; c) do Sistema de Justiça; e d) da sociedade civil (academia, terceiro setor e setor privado). Essa composição fortaleceria as experiências de participação de âmbito e alcance nacional e interlocução de atores e, ao mesmo tempo, permitiria multiplicar as formas de vocalização e agregação dos interesses presentes nesse ecossistema. Além disso, contribuiria para a elaboração de diagnósticos e políticas mais abrangentes relacionadas às questões que emergem do tratamento de dados na segurança pública e chamaria atenção à "centralidade da participação na gestão pública como fator de constituição dos direitos fundamentais,

---

29 SOARES, Luiz Eduardo. "Glossário de Segurança Pública". In: ***Desmilitarizar***. São Paulo: Boitempo, 2019, p. 273

30 VARGAS, Daniel. ***Segurança Pública: um projeto para o Brasil.*** São Paulo: Editora Contracorrente, 2020.

31 SOARES, Luiz Eduardo. "Glossário de Segurança Pública". In: ***Desmilitarizar***. São Paulo: Boitempo, 2019, p. 274.

32 DERY, David. Policy by the Way: When Policy is Incidental to Making Other Policies. ***Journal of Public Policy***, v. 18, n.2, 1998, pp. 163-176. DOI:10.1017/S0143814X98000087. Disponível em: https://www.cambridge.org/core/journals/journal-of-public-policy/article/policy-by-the-way-when-policy-is-incidental-to-making-other-policies/D00B31A6FCD898442B55FBBF150C14EC. Acesso em: 31 out. 2020.

entre os quais, o direito à segurança"[33]. Ao fim e ao cabo, haveria um solo, a ser germinado, para "inovação institucional e parceria entre estado, mercado e sociedade civil" para um novo horizonte para a segurança pública[34].

As atribuições do conselho se distribuiriam dentro de três grupos principais: (i) atribuições consultivas; (ii) atribuições deliberativas; e (iii) atribuições de fiscalização. Com relação ao aspecto consultivo das atribuições, espera-se que o conselho forneça recursos técnicos, com base na produção de estudos, tanto para a ANPD quanto para o público geral, em relação a questões de proteção de dados no âmbito da segurança pública. Em seu aspecto deliberativo/sugestivo, ilustrativamente, o conselho poderá sugerir ações a serem tomadas pela ANPD, bem como incentivar a criação de leis específicas.[35] Como mencionado, o conselho também cumpriria o papel na fiscalização da atuação das atividades de tratamento de dados por agentes de segurança pública ou persecução criminal, podendo ser um canal para acionar a ANPD para que fiscalize de forma mais aprofundada certos processos de tratamento. Além disso, ainda no âmbito fiscalizatório, produzirá relatórios anuais sobre a implementação da Política Nacional de Proteção de Dados Pessoais e da Privacidade na Segurança.

SUGESTÃO DE REDAÇÃO 3	
CONSELHO NACIONAL DE PROTEÇÃO DE DADOS NA SEGURANÇA PÚBLICA E NA PERSECUÇÃO PENAL COMENTÁRIOS	
COMPOSIÇÃO DO CONSELHO	**COMENTÁRIOS**
(S/N) O Conselho Nacional de Proteção de Dados Pessoais na Segurança Pública e na Persecução Penal composto de 23 (vinte e três) representantes, titulares e suplentes, dos seguintes órgãos: I - os seguintes representantes da União: a) o Ministro de Estado da Justiça e Segurança Pública, que o presidirá; b) o Secretário-Executivo do Ministério da Justiça e Segurança Pública, que exercerá a vice-presidência e substituirá o Presidente em suas ausências e em seus impedimentos; c) o Diretor-Geral da Polícia Federal; d) o Diretor-Geral da Polícia Rodoviária Federal; e) o Diretor-Geral do Departamento Penitenciário Nacional; f) o Secretário Nacional de Segurança Pública; g) o Secretário de Direitos Humanos II - os seguintes representantes dos Estados e dos Municípios: a) um representante das polícias civis, indicado pelo Conselho Nacional de Chefes de Polícia Civil;	A previsão das contratações e o detalhamento das descrições devem se dar por meio de portaria de política de tecnologia de vigilância publicizada e acessível.

33 LIMA, R. S.; SOUZA, L. G.; SANTOS, T.. A participação social no campo da segurança pública. Desigualdade & Diversidade (PUCRJ), v. 1, p. 23-48, 2012.

34 VARGAS, Daniel. Segurança Pública: um projeto para o Brasil. São Paulo: Editora Contracorrente, 2020. Posição 105, Edição Kindle.

35 Evidentemente, sugestões de novos projetos de lei teriam como público-alvo o poder Executivo e o poder Legislativo e não a Autoridade Nacional de Proteção de Dados Pessoais, que não possui tal função de formulação de leis.

b) um representante das polícias militares, indicado pelo Conselho Nacional de Comandantes Gerais;

c) 05 (cinco) representantes das secretarias de segurança pública ou de órgãos congêneres das 05 (cinco) regiões do país, indicados pelo Colégio Nacional dos Secretários de Segurança Pública;

d) um representante dos institutos oficiais de criminalística, medicina legal e identificação, indicado pelo Conselho Nacional de Perícia Criminal

III - os seguintes representantes do sistema de justiça:

a) um representante do Poder Judiciário, indicado pelo Conselho Nacional de Justiça;

b) um representante do Ministério Público, indicado pelo Conselho Nacional do Ministério Público;

c) um representante da Defensoria Pública, indicado pelo Colégio Nacional de Defensores Públicos Gerais;

d) um representante da Ordem dos Advogados do Brasil, indicado pelo Conselho Federal da Ordem dos Advogados do Brasil;

IV - os seguintes representantes da sociedade civil:

a) 2 (dois) de entidades da sociedade civil com atuação relacionada a proteção de dados pessoais, eleitos nos termos do disposto no S/N;

b) 2 (dois) de entidades da sociedade civil relacionadas com políticas de segurança pública e defesa social, eleitos nos termos do disposto no S/N;

c) 2 (dois) representantes de entidades de profissionais de segurança pública, eleitos nos termos do disposto no S/N;

d) 3 (três) de instituições científicas, tecnológicas e de inovação, eleitos nos termos do disposto no S/N;

e) 2 (dois) de entidades representativas do setor empresarial relacionado à área de tecnologias de vigilância e segurança pública eleitos nos termos do disposto no S/N;

§ 1º Cada representante titular terá um representante suplente para substituí-lo em suas ausências e seus impedimentos.

§ 2º Os representantes a que se referem das alíneas “i”, “j” e “k” do inciso II do caput serão escolhidos por meio de processo aberto que manifestem interesse em participar do Conselho.

§ 3º O processo a que se refere o § 3º será precedido de convocação pública, cujos termos serão aprovados na primeira reunião deliberativa do Conselho, observados o requisito de representatividade e os critérios objetivos definidos também na primeira reunião.

§ 4º O mandato dos representantes a que se referem o inciso II será de dois anos, admitida uma recondução.

§ 5º A participação no CNSP será considerada prestação de serviço público relevante, não remunerada.

(S/N) Compete ao Conselho Nacional de Proteção de Dados Pessoais na Segurança Pública e na Persecução Penal:

I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade em Segurança Pública e Persecução Criminal para a atuação da ANPD;

II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade na Segurança;

III - sugerir ações a serem realizadas pela ANPD;

IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade em Segurança;

V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população em geral;

VI - convocar e coordenar conferências nacionais organizadas em parceria com entidades da sociedade civil por meio de comissões, fóruns ou grupos de trabalho para elaboração de diretrizes de natureza administrativa e legislativa;

VII - empreender os melhores esforços para que as demandas apresentadas nas conferências nacionais convertam-se em políticas, promovendo a sua execução e seu monitoramento, zelando, assim, pela efetividade das suas deliberações;

VIII - estudar, analisar e sugerir alterações na legislação pertinente;

IX - traçar ações para promover a integração entre órgãos de segurança pública federais, estaduais, distritais e municipais acerca de políticas e procedimentos em matéria de tratamento e compartilhamento de dados e tecnologias de vigilância;

X - auxiliar a ANPD na proposição de diretrizes para elaboração dos relatórios de impacto à proteção de dados e de Vigilância;

XI - auxiliar a ANPD na proposição diretrizes para aquisição das tecnologias de segurança;

XII - auxiliar a ANPD e ter acesso aos números e relatórios dos informes encaminhados à ANPD pelos agentes de tratamento para as atividades de requisição e compartilhamento de dados;

XIII - auxiliar a ANPD e ter acesso aos números e relatórios dos informes encaminhados à ANPD de registro de aquisição de tecnologias de vigilância por parte das autoridades da segurança.

XIV - auxiliar a ANPD no relatório anual acerca dos relatórios de impacto à proteção de dados pelas autoridades competentes no território nacional.

ANEXO I
LEGISLAÇÕES ESTRANGEIRAS DA RIPDP/PIA
QUADRO COMPARATIVO

SUGESTÃO DE REDAÇÃO 2					
PAÍS E LEGISLAÇÃO	EIXOS TEMÁTICOS DE ANÁLISE				COMENTÁRIOS
	CRITÉRIOS OBRIGATÓRIOS	ELEMENTOS E ESTRUTURA MÍNIMA	ARRANJOS DE CO-DELIBERAÇÃO E ESCRUTÍNIO PÚBLICO	AVALIAÇÃO *EX ANTE* E *EX POST*	
Estados Unidos E-Government Act of 2002	Conforme a seção 208 (1) (A) e (B), do E-Government Act, o relatório de impacto é necessário para agências que pretendem desenvolver tecnologias da informação que envolvam o tratamento de informações que identificam alguém; ou que iniciem uma coleta de dados (i) utilizando tecnologias da informação ou (ii) que envolve informações que tornam um indivíduo identificável permitindo contato físico ou virtual.	De acordo com o item (2) (B) (ii), da mesma seção, o conteúdo de um PIA é (i) o tipo de informação coletada; (ii) a razão para a coleta (finalidade); (iii) o uso pretendido pela agência; (vi) com quem a informação será compartilhada; (v) em que momentos poderá ser solicitado o consentimento do titular para a coleta; e (vi) como a informação será protegida.	Há necessidade de revisão dentro do governo e publicização, sem deliberação e escrutínio público evidentes.	Exigência *ex ante*, em relação à atividade de tratamento de dados, de elaboração de PIA. No entanto, conforme artigo 3, C da seção 208, o Diretor da Agência pode exigir a execução de um PIA após início da atividade de tratamento.	Regulamenta Privacy Impact Assessment - (Section 208 - Privacy Provisions). A seção tem como objetivo exigir das agências governamentais que sejam implementadas medidas para garantir a privacidade das informações pessoais dos cidadãos. Estas medidas envolvem a elaboração de um relatório de impacto à privacidade.
Canadá Interim Directive on Privacy Impact Assessment	O dispositivo 6.1, da Diretiva, estabelece a responsabilidade de chefes de instituições governamentais de estabelecer um processo de PIA. E conforme o dispositivo 6.3, cabe aos oficiais ou executivos sênior aderir ao processo de PIA para conclusão do documento. O processo deve ser iniciado quando um programa ou atividade (i) utilizar ou pretender utilizar informações pessoais para tomada de decisões que impactam indivíduos; (ii) que utiliza informações pessoais for alterado com finalidades administrativas; e (iii) for transferido para outro nível governamental ou entidade do setor privado implicando em mudanças substanciais no programa ou atividade (6.3.1).	O conteúdo mínimo do PIA está descrito no Apêndice C. O texto indica que o PIA deverá ter oito seções. A primeira seção trata da visão geral e introdução do PIA, em que são apresentados os órgãos e agentes responsáveis, e descrição geral do projeto. A segunda seção trata da categorização do risco. A terceira e quarta tratam da análise das informações pessoais necessárias e procedimentos de uso e fluxo de informação. A quinta abrange medidas de *compliance* em relação ao *Privacy Act* canadense. Entre a sexta e a oitava encontra-se a conclusão, há um resumo das análises e recomendações, lista de anexos e indicação de aprovação formal do PIA.	De acordo com o dispositivo F)6.3.16, a visão geral e a introdução (*initiation*) do PIA, bem como a seção em que é identificado o risco e sua categorização, deverão ser publicizadas.	Conforme o dispositivo 6.3.1, o processo do PIA será iniciado no começo da implementação de uma atividade ou programa que faça uso de dados pessoais, no entanto, será necessário refazer quando tal atividade sofrer alteração substancial. Ainda assim, não há menção específica à uma análise posterior à atividade.	A Diretiva apresenta designação de responsabilidades para agentes quanto à elaboração do PIA, bem como define claramente o que nele deverá ser contido. Ainda assim, não há clara previsão de escrutínio público, apenas sendo exigida a publicização.

PAÍS E LEGISLAÇÃO	EIXOS TEMÁTICOS DE ANÁLISE				COMENTÁRIOS
	CRITÉRIOS OBRIGATÓRIOS	ELEMENTOS E ESTRUTURA MÍNIMA	ARRANJOS DE CO-DELIBERAÇÃO E ESCRUTÍNIO PÚBLICO	AVALIAÇÃO *EX ANTE* E *EX POST*	
Reino Unido *Data Protection Act* 2018Data Protection, Privacyb and Electronic	Conforme o *Data Protection Act*, artigo 64, o RIPDP é exigido quando a atividade de tratamento de dados pode resultar em alto risco aos direitos e liberdades individuais, sendo um dever do controlador.	Nos termos do art. 64 (3), do Data Protection Act, o conteúdo mínimo do RIPDP é: (i) descrição geral da atividade pretendida; (ii) identificação de risco e previsão de medidas de minimização; e (iii) salvaguardas e mecanismos de segurança a serem implementados.	Não foram encontrados, na legislação, dispositivos que determinem o escrutínio público.	A princípio, a determinação para elaboração de RIPDP seria antes da implementação de atividade de tratamento de dados.	O Reino Unido não apresenta legislação nacional que esclareça todos os procedimentos para o desenvolvimento de um RIPDP. Ainda assim, segue o modelo definido na GDPR e se baseia nas instruções de sua autoridade.
França La loi Informatique et Libertés-Le décret d'application RIPDP: Guidelines CNIL	Conforme o artigo 62 da Lei de Liberdade da Informação, antes da implementação de uma atividade de tratamento de dados, o controlador deve executar o PIA, considerando artigo 35 da Regulação EU 2016/697. Nos termos do artigo 90, da Lei francesa, quando houver alto risco à direitos e liberdades naturais, o controlador deverá executar um RIPDP.	Conforme o Decreto de Aplicação, artigo 130, III, o PIA/RIPDP, previsto no artigo 90, deverá conter ao menos a descrição geral da atividade de tratamento de dados, indicação de riscos e medidas para sua minimização, salvaguardas e mecanismos de segurança.	Não foram encontrados dispositivos que tratem sobre deliberação envolvendo o público.	A princípio há apenas determinações de avaliações anteriores à atividade de tratamento de dados.	A França não possui legislação que defina claramente os procedimentos para elaboração do PIA, dependendo de decisões/diretrizes da Autoridade francesa. Quanto ao RIPDP, a França segue as determinações da GDPR, sendo que a CNIL se manifesta especificamente sobre alguns pontos para detalhá-los.
Portugal Lei 59/2019	A Autoridade portuguesa, na Lei 59/2019, em seu artigo 29º, trata das avaliações de impacto. A obrigatoriedade da elaboração da avaliação é marcada pela possibilidade da operação de tratamento de dados representar um alto risco aos direitos de liberdades dos indivíduos.	Como conteúdos mínimos para a avaliação, o artigo 29º, prevê que deve haver uma descrição geral das operações de tratamento, avaliação dos potenciais riscos, indicação de medidas para gerenciar tais riscos e definição de garantias e medidas de segurança para assegurar os direitos dos titulares.	Não há determinação da legislação nacional que exija o escrutínio público.	As avaliações de impacto seriam executadas antes das atividades de tratamento de dados que podem representar um alto risco ao titular	A legislação portuguesa é bem superficial quanto aos procedimentos para se desenvolver um RIPDP. Ainda assim, nota-se que seguem o padrão da Diretiva 2016/680 e GDPR. Além disso, dependem muito das instruções da autoridade, sem utilizar atos normativos.
Austrália (I) Privacy Act 1988 A Autoridade Nacional possui um guia para a sua elaboração: Guide to undertaking	Segundo o dispositivo 33D (1), do *Privacy Act* australiano, o Comissário pode exigir a execução de um PIA quando (i) uma agência iniciar atividade que use informações pessoais; e (ii) o Comissário considerar que a atividade pode	Quanto ao conteúdo mínimo, o Privacy Act aponta que o PIA identifica o impacto que a atividade pode ter sobre a privacidade dos indivíduos e recomendações para	Não é mencionada deliberação e escrutínio público	Não é mencionada execução posterior à atividade.	A legislação em si não é muito detalhista quanto aos procedimentos de elaboração do PIA. No entanto, o Guia da Autoridade australiana fornece a complementação necessária para mais detalhes sobre o conteúdo do PIA, sobre a execução de consultas públicas e sobre a

privacy impact assessments	impactar significativamente a privacidade de indivíduos	minimizar tal impacto (33D (3)).	Não há determinação da legislação nacional que exija o escrutínio público.	As avaliações de impacto seriam executadas antes das atividades de tratamento de dados que podem representar um alto risco ao titular	necessidade de refazer, revisar ou atualizar o documento.
Austrália (II) Guide to undertaking privacy impact assessments	O Guia recomenda que sempre que uma entidade de utilizar dados pessoais, ela deveria considerar a elaboração de um PIA. Assim, seria uma etapa a ser iniciada ainda no começo do desenvolvimento do projeto para que ele seja planejado considerando a contenção de riscos e proteção dos titulares.	Segundo o Guia da Autoridade, o PIA deveria descrever o fluxo dos dados ao longo da atividade, analisar possíveis impactos, identificar e recomendar medidas protetivas, apresentar considerações de privacy by design.	Segundo o Guia, poderão existir consultas públicas no processo de elaboração do PIA. No Guia, é apontado como algo a se inserir no planejamento da elaboração do PIA a definição da extensão e momento para execução de consultas com stakeholder e com o público. Esta é uma forma de comunicar e endereçar os assuntos relacionados à privacidade. Esta consulta serve também para que se considere as expectativas do público quanto à preservação do seu direito à privacidade e para conscientizar a população sobre a implementação.	O Guia define que o PIA precisa ser revisitado e atualizado quando houver alterações, e até mesmo refazê-lo (é identificado como conteúdo do PIA o esclarecimento sobre se é uma atividade nova ou se refere-se a uma modificação de atividade pré-existente). A revisão do PIA pode ser feita por entidade independente (auditoria externa), o que não impede uma revisão interna. De todo modo, a revisão é uma ferramenta útil para verificar se as recomendações do PIA foram devidamente implementadas. E a atualização serve para abarcar as mudanças feitas ao longo do percurso de implementação e execução do projeto.	O Guia, ainda que não traga muitas imposições como faria um ato normativo, possibilita o detalhamento dos procedimentos esperados e amplia os dispositivos legais, recomendando formas de melhorar o PIA e porque implementá-las é benéfico. Exemplos deste tipo de ampliação seria a sugestão para elaborar um PIA em qualquer tipo de atividade que envolva tratamento de dados, traz detalhamento de outros conteúdos para além do mínimo que poderiam estar no PIA, além de pormenorizar sua estrutura. Outro ponto que vai além da legislação é a identificação das consultas públicas como parte do processo de elaboração de um PIA, bem como sua revisão e atualização.

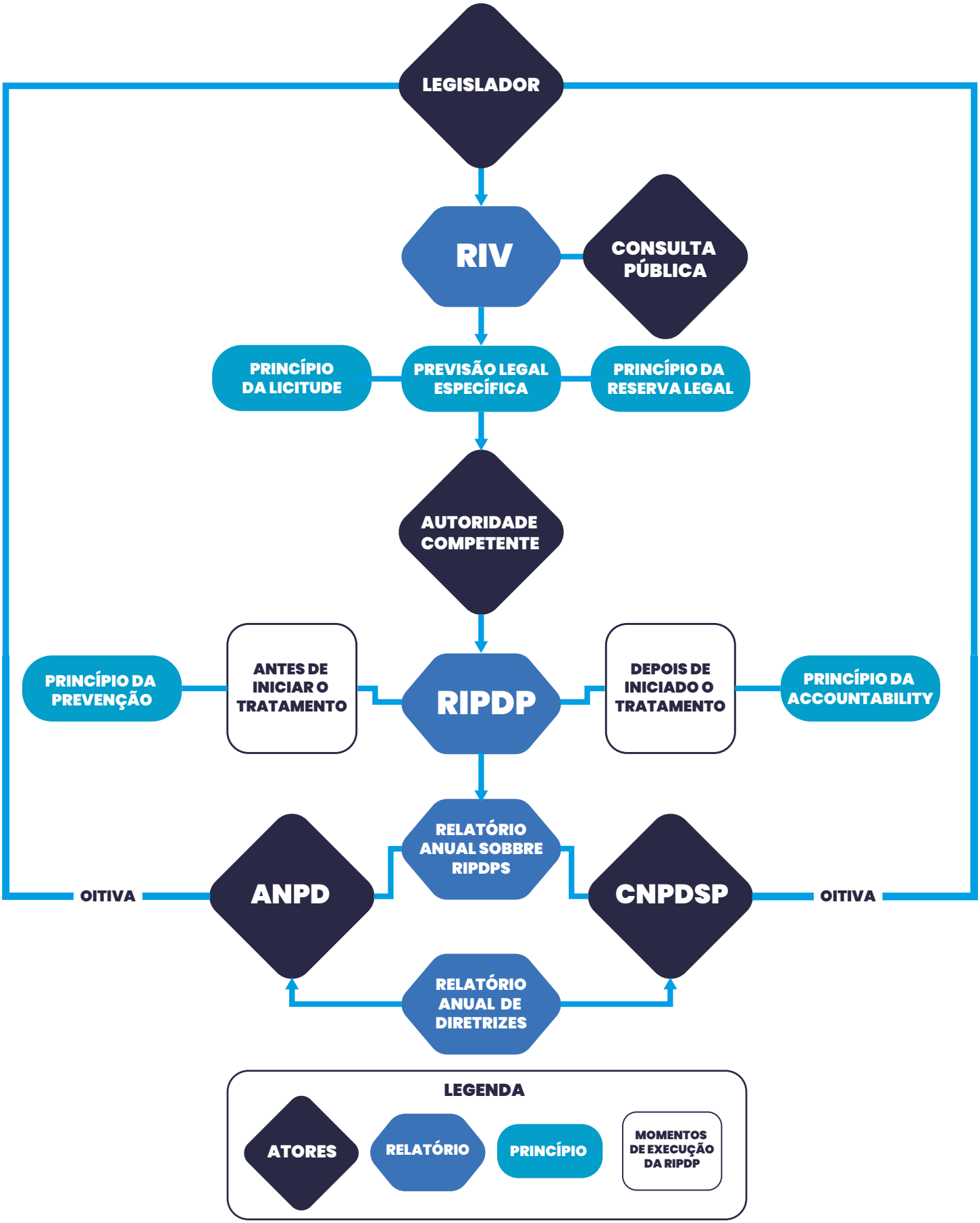
ANEXO II
RELATÓRIO DE IMPACTO À VIGILÂNCIA – DEFINIÇÃO E SISTEMATIZAÇÃO LEGAL

PAÍS	COMENTÁRIOS	LEGISLAÇÃO E REFERÊNCIAS
Austrália	A legislação federal australiana menciona apenas o relatório de impacto sobre dados pessoais - *Privacy Impact Assessment*. O artigo 33D, 1, b, *do Privacy Act 1998* fala em impacto significativo na privacidade de indivíduos (*"significant impact on the privacy of individuals"*), termo que a autoridade nacional australiana (*Office of the Australian Information Commissioner*) inclui atividades de vigilância. Não há previsão de relatório de impacto de vigilância.	• Privacy Act 1988 • Australian Privacy Principles • Guide to undertaking privacy impact assessments
Canadá	Não foi localizado nos dispositivos legais ao lado um relatório específico para vigilância, somente o Privacy Impact Assessment (PIA). O outro relatório mencionado é Threat Risk Assessment (TRA), focado em segurança da informação. Na diretiva provisória para o PIA, há menção às tecnologias de vigilância, mas sem indicar necessariamente um documento específico para este fim.	• Personal Information Protection and Electronic Documents Act ('PIPEDA') • Personal Information Protection Act ('PIPA Alberta') • Personal Information Protection Act ('PIPA BC') • An Act Respecting the Protection of Personal Information in the Private Sector ('Quebec Privacy Act'), (collectively, 'Canadian Privacy Statutes') • Interim Directive on Privacy Impact Assessment
Estados Unidos	A Câmara Municipal de Seattle aprovou a necessidade de um Relatório de Impacto de Vigilância – *Surveillance Impact Report (SIR), Ordinance 125376, subsection 14.18.040.B* – sempre que houver aquisição de tecnologias de vigilância pelo poder público municipal. Exige a descrição das tecnologias de vigilância, tipo de dados que é capaz de produzir, finalidade do uso, política de tratamento dos dados e outros requisitos, como o compartilhamento de dados. A legislação determina que seja divulgada uma Avaliação de Impacto em Equidade (*Equity Impact Assessment, subsection 14.18.050*), bem como uma publicação anual a respeito do uso de tecnologias de vigilância. Vigente desde 2017, já foram produzidos e disponibilizados relatórios de vigilância sobre câmeras de segurança, gravador de logs e outras tecnologias. A cidade de São Francisco aprovou em 2019 a Ordinance 107-19, definindo regras para aquisição de tecnologias de vigilância pelo poder público municipal. A seção 19B exige que um relatório de impacto de vigilância (*surveillance impact report*) seja submetido para aprovação pelo Conselho de Supervisão (*Board of Supervisors*) especialmente designado para a tarefa. Dentre os requisitos, é preciso demonstrar que as tecnologias adquiridas respeitem a privacidade dos cidadãos. A norma define o que são tecnologias de vigilância e exige a publicização de relatório anual a respeito do uso destas pelos departamentos municipais (*Annual Surveillance Report*), com inventário das tecnologias e suas finalidades.	• Seattle - Surveillance Ordinance (Ordinance 125376) • Surveillance Technology Community Equity Impact Assessment and Policy Guidance Report (2019) • San Francisco - Acquisition of Surveillance Technology - Ordinance 107-19 • E-Government Act of 2002

Estados Unidos	O E-Government Act of 2002 exige que agências governamentais dos EUA implementem medidas para proteção da privacidade de cidadãos através de um Privacy Impact Assessment, mas não especifica a necessidade de relatório de impacto de vigilância.	
França	A legislação trata especificamente do relatório de análise de impacto sobre dados pessoais – *analyse d'impact relative à la protection des données* (AIPD), mas não há previsão de relatório de impacto de vigilância.	• La Loi Informatique et Libertés • Le décret d'application • Règlement intérieur de la CNIL • Fonctionnement en urgence sanitaire
Portugal	Não há menção específica a relatórios de vigilância, tampouco impactos de vigilância, apenas "Avaliação de Impacto". A Lei nº 58/2019, ao delimitar competências e atribuições da Comissão Nacional de Proteção de Dados, elenca a Unidade de Informática como responsável por estudos sobre novas tecnologias com impacto no tratamento de dados pessoais, mas sem critérios específicos (Art. 26, i).	• Lei da Proteção de Dados Pessoais • Decreto Lei nº 35/2004 - Atividade de segurança privada • Código do Trabalho • Lei nº 58/2019 • Lei nº 59/2019 • Princípios sobre o tratamento de videovigilância
Reino Unido	Não existe previsão para um relatório de impacto de vigilância, apenas orientações e princípios específicos para a videovigilância (CCTV). A legislação ao lado menciona apenas relatórios de impacto em privacidade - *Data Protection Impact Assessment* (DPIA).	• Data Protection Act 2018 • Data Protection, Privacy and Electronic Communications • Recomendações do Information Commissioner's Office (ICO) a respeito de setores da polícia, justiça e vigilância • Data protection code of practice for surveillance cameras and personal information

ANEXO III
FLUXOGRAMA RIV E RIPDP E DEVIDO PROCESSO INFORMACIONAL

FLUXOGRAMA RIPDP E RIV COMO MEDIDAS DE DEVIDO PROCESSO INFORMACIONAL



ANEXO IV
QUADRO COMPARATIVO

CONSELHO NACIONAL DE PROTEÇÃO DE DADOS E PRIVACIDADE DECRETO Nº 10.474, DE 26 DE AGOSTO DE 2020		CONASP DECRETO Nº 7.t413, DE 30 DE DEZEMBRO DE 2010		CNSP DECRETO Nº 9.489, DE 30 DE AGOSTO DE 2018 (Cap. V)	
COMPOSIÇÃO		**COMPOSIÇÃO**		**COMPOSIÇÃO**	
FORMATO:	**COLEGIADO**	**FORMATO:**	**COLEGIADO**	**FORMATO:**	**COLEGIADO**
MEMBROS:	**23 TITULARES**	**MEMBROS:**	**39 TITULARES**	**MEMBROS:**	**40 TITULARES**
MEMBROS POR SETOR		**MEMBROS POR SETOR**		**MEMBROS POR SETOR**	
I - um da Casa Civil da Presidência da República, que o presidirá; II - um do Ministério da Justiça e Segurança Púbica; III - um do Ministério da Economia; IV - um do Ministério da Ciência, Tecnologia e Inovações; V - um do Gabinete de Segurança Institucional da Presidência da República; VI - um do Senado Federal; VII - um da Câmara dos Deputados; VIII - um do Conselho Nacional de Justiça; IX - um do Conselho Nacional do Ministério Público; X - um do Comitê Gestor da Internet no Brasil; XI - três de organizações da sociedade civil com atuação comprovada em proteção de dados pessoais; XII - três de instituições científicas, tecnológicas e de inovação;		I - nove representantes governamentais dos governos federal, estadual, do Distrito Federal e municipal, além do comando ou direção das forças policiais; II - nove representantes de entidades representativas de trabalhadores da área de segurança pública; e III - doze representantes de entidades e organizações da sociedade civil cuja finalidade seja relacionada com as políticas de segurança publica.		I - o Ministro de Estado da Justiça e Segurança Pública, que o presidirá II - o Secretário-Executivo do Ministério da Justiça e Segurança Pública, que exercerá a vice-presidência e substituirá o Presidente em suas ausências e seus impedimentos; III - o Diretor-Geral da Polícia Federal; IV - o Diretor-Geral da Polícia Rodoviária Federal; V - o Diretor-Geral do Departamento Penitenciário Nacional; VI - o Secretário Nacional de Segurança Pública; VII - o Secretário Nacional de Proteção e Defesa Civil; VIII - o Secretário Nacional de Políticas sobre Drogas; IX - os seguintes representantes da administração pública federal, indicados pelo Ministro de Estado correspondente: a) um representante da Casa Civil da Presidência da República; b) um representante do Ministério da Defesa; c) um representante do Ministério da Mulher, da Família e dos Direitos Humanos d) um representante do Gabinete de Segurança Institucional da Presidência da República; X - os seguintes representantes estaduais e distrital:	

XIII - três de confederações sindicais representativas das categorias econômicas do setor produtivo; XIV - dois de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; e XV - dois de entidades representativas do setor laboral.		a) um representante das polícias civis, indicado pelo Conselho Nacional de Chefes de Polícia Civil; b) um representante das polícias militares, indicado pelo Conselho Nacional de Comandantes Gerais; c) um representante dos corpos de bombeiros militares, indicado pelo Conselho Nacional dos Corpos de Bombeiros Militares do Brasil; d) um representante das secretarias de segurança pública ou de órgãos congêneres, indicado pelo Colégio Nacional dos Secretários de Segurança Pública; e) um representante dos institutos oficiais de criminalística, medicina legal e identificação, indicado pelo Conselho Nacional de Perícia Criminal; e f) um representante dos agentes penitenciários, indicado por conselho nacional devidamente constituído; XI - um representante dos agentes de trânsito, indicado por conselho nacional devidamente constituído; XII - um representante das guardas municipais, indicado por conselho nacional devidamente constituído; XIII - um representante da Guarda Portuária, indicado por conselho nacional devidamente constituído; XIV - um representante do Poder Judiciário, indicado pelo Conselho Nacional de Justiça; XV - um representante do Ministério Público, indicado pelo Conselho Nacional do Ministério Público; XVI - um representante da Defensoria Pública, indicado pelo Colégio Nacional de Defensores Públicos Gerais; XVII - um representante da Ordem dos Advogados do Brasil, indicado pelo Conselho Federal da Ordem dos Advogados do Brasil; XVIII - dois representantes de entidades da sociedade civil organizada cuja finalidade esteja relacionada com políticas de segurança pública e defesa social, eleitos nos termos do disposto no § 3º;

		XIX - dois representantes de entidades de profissionais de segurança pública, eleitos nos termos do disposto no § 3º; e XX - os seguintes indicados, de livre escolha e designação pelo Ministro de Estado da Justiça e Segurança Pública: a) um representante do Poder Judiciário; b) um representante do Ministério Público; e c) até oito representantes com notórios conhecimentos na área de políticas de segurança pública e defesa social e com reputação ilibada. XXI - o Secretário de Operações Integradas do Ministério da Justiça e Segurança Pública.
MEMBROS POR SETOR	**MEMBROS POR SETOR**	**MEMBROS POR SETOR**
I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; III - sugerir ações a serem realizadas pela ANPD; IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população em geral.	I - atuar, como órgão normativo, na formulação de estratégias e no controle de execução da Política Nacional de Segurança Pública; II - estimular a modernização institucional para o desenvolvimento e a promoção intersetorial das políticas de segurança pública; III - desenvolver estudos e ações visando a aumentar a eficiência da execução da Política Nacional de Segurança Pública; IV - estabelecer diretrizes para as ações da Política Nacional de Segurança Pública e acompanhar a destinação e aplicação dos recursos a elas vinculados; V - convocar e coordenar as Conferências Nacionais de Segurança Pública e zelar pela efetividade das suas deliberações; VI - articular e apoiar, sistematicamente, os Conselhos Estaduais, do Distrito Federal e Municipais de Segurança Pública, visando a formulação e realização de diretrizes básicas comuns e a potencialização do exercício das suas atribuições legais e regulamentares; VII - estudar, analisar e sugerir alterações na legislação pertinente; e	O CNSP, órgão colegiado permanente, integrante estratégico do Susp, tem competência consultiva, sugestiva e de acompanhamento social das atividades de segurança pública e defesa social, respeitadas as instâncias decisórias e as normas de organização da administração pública. Parágrafo único. O CNSP exercerá o acompanhamento dos integrantes operacionais do Susp, a que se refere o § 2º do art. 9º da Lei nº 13.675, de 2018 , e poderá recomendar providências legais às autoridades competentes, de modo a considerar, entre outros definidos em regimento interno ou em norma específica, os seguintes aspectos: I - as condições de trabalho, a valorização e o respeito pela integridade física e moral de seus integrantes; II - o cumprimento das metas definidas de acordo com o disposto na Lei nº 13.675, de 2018, para a consecução dos objetivos do órgão; III - o resultado célere na apuração das denúncias em tramitação nas corregedorias; e IV - o grau de confiabilidade e aceitabilidade do órgão pela população por ele atendida.

	VIII - promover a integração entre órgãos de segurança pública federais, estaduais, distritais e municipais.	Art. 41. Compete, ainda, ao CNSP: I - propor diretrizes para políticas públicas relacionadas com segurança pública e defesa social, com vistas à prevenção e à repressão da violência e da criminalidade e à satisfação de princípios, diretrizes, objetivos, estratégias, meios e instrumentos da Política Nacional de Segurança Pública e Defesa Social, estabelecidos no art. 4º ao art. 8º da Lei nº 13.675, de 2018 ; II - apreciar o Plano Nacional de Segurança Pública e Defesa Social e, quando necessário, fazer recomendações relativamente aos objetivos, às ações estratégicas, às metas, às prioridades, aos indicadores e às formas de financiamento e gestão das políticas de segurança pública e defesa social nele estabelecidos; III - propor ao Ministério da Segurança Pública e aos integrantes do Susp a definição anual de metas de excelência com vistas à prevenção e à repressão das infrações penais e administrativas e à prevenção de desastres, por meio de indicadores públicos que demonstrem, de forma objetiva, os resultados pretendidos; III - propor ao Ministério da Justiça e Segurança Pública e aos integrantes do Susp a definição anual de metas de excelência com vistas à prevenção e à repressão das infrações penais e administrativas e à prevenção de desastres, por meio de indicadores públicos que demonstrem, de forma objetiva, os resultados pretendidos; (Redação dada pelo Decreto nº 9.876, de 2019) IV - contribuir para a integração e a interoperabilidade de informações e dados eletrônicos sobre segurança pública e defesa social, prisionais e sobre drogas, e para a unidade de registro das ocorrências policiais; V - propor a criação de grupos de trabalho com o objetivo de produzir e publicar estudos e diagnósticos para a formulação e a avaliação de políticas públicas relacionadas com segurança pública e defesa social;

		VI - prestar apoio e articular-se, sistematicamente, com os conselhos estaduais, distrital e municipais de segurança pública e defesa social, com vistas à formulação de diretrizes básicas comuns e à potencialização do exercício de suas atribuições legais e regulamentares; VII - estudar, analisar e sugerir alterações na legislação pertinente; e VIII - promover a articulação entre os órgãos que integram o Susp e a sociedade civil. Parágrafo único. O CNSP divulgará anualmente e, de forma extraordinária, quando necessário, as avaliações e as recomendações que emitir a respeito das matérias de sua competência. Art. 41-A. As convocações para as reuniões do CNSP, do Conselho Gestor do Sinesp e da Comissão Permanente do Sinaped especificarão o horário de início das atividades e previsão para seu término. (Incluído pelo Decreto nº 9.876, de 2019) § 1º. Na hipótese de reunião ordinária com duração superior a duas horas, deverá ser especificado período para votação, que não poderá ser superior a duas horas. (Incluído pelo Decreto nº 9.876, de 2019) § 2º. É vedada a divulgação de discussões em curso nos colegiados sem a prévia anuência do Ministro de Estado da Justiça e Segurança Pública. (Incluído pelo Decreto nº 9.876, de 2019) Art. 41-B. A participação nos colegiados e nos subcolegiados de que trata este Decreto será considerada prestação de serviços públicos relevante, não remunerada. (Incluído pelo Decreto nº 9.876, de 2019) Art. 41-C. Os regimentos internos dos colegiados serão elaborados no prazo de noventa dias, contado da data de publicação deste Decreto. (Incluído pelo Decreto nº 9.876, de 2019) Parágrafo único. Os regimentos internos de que trata o caput serão aprovados por maioria simples.

ANEXO IV
A ESFERA PROTEGIDA DOS DADOS

Consulta

A esfera protegida dos dados pessoais e as intervenções informacionais do Estado

A dogmática constitucional aplicada ao tratamento de dados na Segurança Pública e no Processo Penal

– Diretrizes técnicas para subsidiar *Policy Paper* –

Consulente:

Data Privacy Brasil

Consultados:

Eduardo Viana, Lucas Montenegro e Orlandino Gleizer

Novembro/2020

Sumário

Lista de abreviaturas 1
A. Objeto da Consulta 2
B. A dogmática constitucional da proteção de dados 6
I. A reserva de lei e a reserva parlamentar: o conteúdo das normas autorizativas de intervenção informacional 7
II. Regramento específico para as distintas atividades estatais e o princípio da separação informacional 11
III. A dogmática da intervenção em direitos fundamentais 12
C. Algumas precauções em relação à Diretiva 2016/680 (DPD): a importância da legislação nacional no contexto europeu 16
D. Intervenções informacionais para fins de segurança pública 20
I. A garantia da segurança pública 20
II. Aspectos centrais de um direito de segurança pública: bem protegido, perigo e destinatários 21
1. Bem protegido: a segurança pública 22
2. Objeto material da ação estatal: o perigo 23
3. Objeto pessoal da ação estatal: os destinatários 24
II. Um exemplo de norma de autorização: a identificação eletrônica de veículos automotivos 25
E. Intervenções informacionais para o fim de persecução criminal 29
I. Considerações gerais 30
1. O princípio da publicidade do processo e a proteção da personalidade 30
2. A presunção de inocência e os níveis de suspeita do fato 33
3. Formas de tratamento de dados no processo penal 33
II. Medidas de investigação na persecução penal 34
1. Critérios para regras especiais de autorização 36
2. Um exemplo de norma de autorização: o monitoramento de telecomunicações 39
III. Demais formas de tratamento de dados pessoais no processo penal 42
F. O compartilhamento de dados entre órgãos de segurança pública e persecução penal 44
I. Licitude formal: o modelo das duas portas 44
II. Licitude material: a vinculação ao fim e o critério do levantamento hipotético 45
Síntese e Parecer 47

Lista de abreviaturas

Abs. – *Absatz* (parágrafo ou subparágrafo)
art. – artigo
Art. – *Artikel*
BGH – *Bundesgerichtshof* (Corte de Justiça Federal alemã, competente para a interpretação da lei federal)
BGHSt – *Sammlung der Entscheidungen des Bundesgerichtshofs in Strafsachen* (repositório oficial de jurisprudência do BGH em matéria penal)
BVerfG – *Bundesverfassungsgericht* (Tribunal Constitucional Federal alemão)
BVerfGE - *Die Entscheidungen des Bundesverfassungsgerichts* (repositório oficial de jurisprudência do BVerfG)
Cap. – Capítulo
CF – Constituição Federal brasileira
Cf. - Conferir
Cons. - Consideração
CP – Código Penal brasileiro
CPP – Código de Processo Penal brasileiro
CR – *Computer und Recht* (revista jurídica)
DPD – Diretiva 2016/680 (DPD) da União Europeia.
EuGRZ – *Europäische Grundrechte-Zeitschrift* (revista jurídica)
FS – *Festschrift* (coletânea de artigos em homenagem)
GA – *Goldtammer's Archiv für Strafrecht* (revista jurídica)
GG – *Grundgesetz* (Constituição Federal alemã)
GVG – *Gerichtsverfassungsgesetz* (Lei de Organização Judiciária alemã)
LGPD – Lei Geral de Proteção de Dados brasileira (Lei 13.709/2018)
LIT – Lei de Interceptação Telefônicas (9.296/96)
MDR – *Monatsschrift für Deutsches Recht* (revista jurídica)
NJW – *Neue Juristische Wochenschrift* (revista jurídica)
nm. – número marginal
nr. (nota de rodapé)
Orgs. - Organizadores
p. – página
pp. – páginas
RBDPP – Revista Brasileira de Direito Processual Penal, Porto Alegre (volume/número, p.)
REC – Revista de Estudos Criminais (volume/número, p.)
RGPD – Regulamento Geral de Proteção de Dados da União Europeia (2016/679)
s. – e seguinte
S. – *Satz* (frase em uma Abs.)
SK-StPO – *Systematischer Kommentar zur Strafprozessordnung* (comentário ao StPO)
ss. – e seguintes
STF – Supremo Tribunal Federal
STJ – Superior Tribunal de Justiça
StPO – *Strafprozessordnung* (código de processo penal alemão)

Brasil/Alemanha, 1º de novembro de 2020

A. Objeto da Consulta

Um fato curiosamente ocorrido em 1983, às vésperas do fatídico ano 1984, escolhido por *George Orwell* como cenário e nome de seu romance distópico[1], representou paulatinamente, em grande parte do mundo, uma mudança de paradigma na proteção do indivíduo contra o poder informacional do Estado.[2] Em dezembro daquele ano, portanto no apagar das luzes para o "profético" ano representativo da "vigilância total", a Corte Constitucional Federal alemã (BVerfG) decidiu que, "diante das condições do processamento automático de dados, não mais haveria dados [pessoais] irrelevantes"[3].

É preciso atentar, por enquanto, para as exatas palavras do BVerfG proferidas àquela altura, a fim de que se possa compreender um detalhe fundamental dessa mudança de paradigma. Em primeiro lugar, ela se impunha em razão de certa contingência: o surgimento do processamento automático de dados. Em segundo lugar, é preciso compreender o que de fato mudou: um amplo espectro de dados pessoais, até então considerados irrelevantes, adquiriu relevância. Aquela decisão certamente não inaugurou a proteção da privacidade[4] e de dados pessoais, e com isso os interesses individuais contra a tomada de conhecimento de suas informações por parte do Estado. Já havia dados individuais relevantes e, portanto, protegidos pelos direitos de *sigilo*[5]. Um exemplo disso são as informações trocadas por cartas ou por telefone, que já eram protegidas constitucionalmente (Art. 10 GG). No entanto, com o processamento automático de dados, até mesmo dados tipicamente menos significativos, ou seja, aqueles que, a princípio, não revelariam informações pertinentes a um âmbito íntimo da vida privada, poderiam, se combinados e comparados a outros – possibilidade que surgia com o processamento automático –, servir para adquirir informações relevantes e sensíveis, e até mesmo para formar perfis de personalidade sobre os indivíduos em questão. Assim, no entender do Tribunal cuja missão institucional é a salvaguarda de direitos fundamentais do cidadão, era necessário submeter qualquer dado individual à proteção de um direito fundamental.

---

[1] *Orwell*, George. 1984, Secker and Warburg: Londres, 1. ed., 1949.
[2] A decisão abordou apenas as questões relacionadas ao processamento de dados *estatal*.
[3] BVerfGE 65, 1 (45) - Volkszählungsurteil: "insoweit gibt es unter der Bedingungen der automatischen Datenverarbeitung kein "belangloses" Datum mehr".
[4] Para uma breve história da evolução do direito geral de personalidade, cf. *Bull*, Netzpolitik: Freiheit und Rechtsschutz im Internet, 2013, pp. 51 ss.
[5] A esse respeito, cf. *Lewinski*, Die Matrix des Datenschutzes, 2014, pp. 31 ss.

Essa visão imporia, gradualmente, uma radical mudança de paradigma tanto na ordem jurídica alemã quanto no plano do direito comunitário da União Europeia e, como agora se vê, até mesmo em países da América Latina, a exemplo do Brasil.

Passados mais de 30 anos daquela decisão alemã e seguindo os primeiros passos já dados no sentido de uma proteção brasileira de dados pessoais, foram estes subscritores procurados pela Data Privacy Brasil, para que oferecessem seu Parecer sobre as *diretrizes técnicas para a regulação da proteção de dados nos específicos setores da Segurança Pública e do Processo Penal*. A finalidade desse Parecer é a de instruir *Policy Paper* endereçado à Comissão de Juristas, atualmente instalada na Câmara dos Deputados Federal, que formula anteprojeto de lei para a regulação da matéria

A questão que nos coloca a Consulente é da maior relevância. Antecipando-se à realidade com que somos confrontados atualmente, o BVerfG parece ter profetizado o surgimento de uma sociedade digital, que, por meio do uso massivo de técnicas eletrônicas de informação e comunicação, alcançou "possibilidades inacreditáveis de levantamento, valoração e uso de dados"[6]. Essas técnicas trouxeram consigo, usando palavras mais recentes do BVerfG, um "sentimento difusamente ameaçador de vigilância"[7], que perturba um dos pressupostos fundamentais para o livre desenvolvimento humano: a sensação de inexistência de espaços livres de observação. Sentir-se observado pode afetar a forma humana mais pura da espontaneidade, atributo fundamental para o desenvolvimento da personalidade. Por essas razões, é necessário criar e garantir o amplo direito fundamental à autodeterminação informacional, de modo que o indivíduo, tendo um controle ideal das informações que lhe digam respeito, tenha condições de configurar seu próprio destino e determinar sua própria identidade.[8]

O direito de proteção de dados não pode significar apenas proteção *dos* dados, deve implicar também proteção *contra* os dados,[9] ou seja, contra os efeitos das informações que contêm para seus titulares. Sendo assim, a regulação da proteção de dados no setor público deve ser a resultante entre os legítimos interesses individuais e os efeitos estatais pretendidos com o tratamento de dados pessoais. É preciso incluir, portanto, nessa ponderação as *pretensões* do Estado no exercício de suas atividades próprias. Não há âmbitos onde essas pretensões têm efeitos mais relevantes para a esfera do titular de dados do que no das atividades de segurança pública e persecução de crimes. As informações pessoais levantadas pelo Estado podem ensejar, no exercício dessas

[6] *Bull*, Sinn und Unsinn des Datenschutzes, 2015, p. 4,
[7] BVerfGE 125, 260 (320).
[8] Para mais detalhes, cf. *Kingreen/Poscher*, Grundrechte Staatsrecht II, 35. ed., p. 122 nm. 441 ss.; *Tinnefeld et al.*, Einführung in das Datenschutzrecht, 7. Aufl, 2020, pp. 107 ss.
[9] Assim, já *Lewinski,* Die Matrix des Datenschutzes, 2014, p.4; no mesmo sentido, *Bull* (nr. **6**), p. 9.

atividades, as intervenções mais severas do ordenamento jurídico: o indivíduo pode até ser preso com base em informações obtidas a partir de seus dados pessoais.

Essa particular componente do problema enseja, assim, um aspecto especial do objeto da Consulta: a impossibilidade da mera transposição de algum modelo específico presente em âmbito internacional que não tenha em conta as particularidades da organização da segurança pública e do processo penal no Brasil. Afinal, a forma como cada Estado soberano melhor organiza suas atividades de segurança interna e persecução de crimes é matéria sensível e complexa, jamais passível de solução uniforme. Por isso, a resposta à Consulta exige não apenas conhecimento das questões específicas do processamento automatizado de dados, mas também daquelas atinentes ao exercício interventivo das forças estatais brasileiras na esfera individual protegida por direitos fundamentais, e isso sobretudo nos âmbitos mais interventivos, quais sejam, os da segurança pública e do processo penal. Assim, parece recomendável formular, no lugar de precisas respostas, critérios e considerações para uso no debate nacional sobre a conformação dessas atividades a uma proteção ideal da autodeterminação informacional. E isso segundo a convicção de que não basta proteger o indivíduo contra usos ilegítimos de seus dados, é necessário ao mesmo tempo garantir que o Estado brasileiro possa, em certas hipóteses, usá-los de forma legítima também contra o mesmo indivíduo, de modo que, ao final, essa relação seja *compatível* com as condições necessárias para que o indivíduo possa autodeterminar-se suficientemente enquanto o Estado age.

A resposta de nossa Consulta parte, portanto, da formulação de um controle *ideal* por parte do indivíduo em relação às suas informações pessoais. Esse controle ideal começa na proteção constitucional dos dados pessoais: o indivíduo deve poder determinar "quem sabe o que sobre ele, quando e em que circunstância"[10]. Mas ali não se esgota: porque um exagerado autocontrole das informações pessoais, que ameace até mesmo a comunicação interpessoal (outro aspecto essencial do desenvolvimento da personalidade: *comunicação é como respiração*[11]) tampouco é do interesse do indivíduo, que não desenvolve sua personalidade apenas enquanto titular de dados, senão também como usuário de dados alheios. Afinal, é necessário que "outros possam, a partir dos meus comportamentos e das minhas expressões, formar uma imagem a meu respeito"[12]. Assim, o imperativo de resolução dessa questão é o perfeito equilíbrio entre os diversos interesses em ponderação. Encontrar o limite adequado para esse controle ideal é, portanto, o esforço principal destes subscritores, traduzido neste Parecer, cujo objetivo reside em oferecer critérios gerais para normas claras,

[10] BVerfGE 65, 1 (Rn 148).
[11] Assim, *Bull* (nr. 6), p. 5, que faz relevantes considerações a respeito de uma proteção de dados exagerada; cf. também *idem*, Netzpolitik (nr. 4), p. 55.
[12] *Bull* (nr. 6), p. 6.

determinadas e proporcionais que autorizem intervenção estatal legítima no âmbito constitucionalmente protegido do indivíduo, sem afetar seu espaço de controle essencial.

Em um Estado de Direito, cujas ações precisam estar sempre legitimadas pelo povo (art. 1º § único CF), em lei formal e materialmente legítima, todos os agentes estatais agem nos limites de expressas autorizações legais, e isso especialmente quando suas ações atingem um âmbito da vida privada protegido por um direito fundamental. Afinal, ninguém é obrigado a fazer ou deixar que com que ele se faça algo senão em virtude de lei (art. 5º II CF). Por isso, erigir as barreiras próprias de um direito fundamental no entorno dos dados pessoais obriga o Estado, de forma geral, a só adentrar este espaço quando expressamente autorizado a tanto e apenas quando necessário para a realização de suas legítimas funções. Daí dizer que, em relação às informações individuais, cada uma das ramificações estatais (como a polícia, o Ministério Público, os tribunais etc.) só pode levantá-las na medida em que sejam necessárias para, e apenas para, a realização de suas tarefas. E que, tão logo cumpridas essas tarefas, qualquer manutenção das informações levantadas carece de nova fundamentação, tanto formal quanto material. São essas as razões que fundamentam a ideia de vinculação finalística: o uso dos dados (ou seja, das informações nele contidas) está vinculado à finalidade de seu *levantamento*, e qualquer uso para outro fim, que não este inicial, representa, portanto, outra autônoma intervenção do Estado.

Por isso, não é possível falar em proteção de dados na Segurança Pública e no Processo Penal de forma geral, sem uma necessária distinção precisa entre as atuações estatais em cada um desses âmbitos. Elas se orientam por finalidades distintas e com maior ou menor garantia ao indivíduo. É possível estabelecer certas ideias gerais de validade comum a ambos, mas não é possível, por exemplo, estabelecer hipóteses comuns de levantamento de dados pessoais para os dois. Enquanto um está voltado à prevenção de perigos, outro está interessado na punição de crimes. E, diferentemente do que ocorre nas relações cíveis, nas quais os indivíduos trocam seus dados de forma consentida, é no levantamento sem consentimento que reside o ponto crucial de toda a análise a seguir. É a forma como os dados chegam às mãos do Estado, contrariamente à vontade de seus titulares, o que definirá toda a estratégia de equilíbrio entre os interesses postos em ponderação.

É sobre a forma de autorização do levantamento de dados individuais e as posteriores exigências dela advindas, portanto, que se desenvolverá, a seguir, a resposta à consulta que, honrosamente, nos dirigiu a Data Privacy Brasil.

B. A dogmática constitucional da proteção de dados

O termo "*proteção* de dados", embora não seja incorreto, pode induzir a erro quando se pensa em regulação para a segurança pública e o processo penal. O erro em questão consistiria em supor que um regime de proteção de dados se inicia com um conjunto de normas e órgãos que o Estado tem de criar, para que os dados pessoais sejam adequadamente protegidos. Nesse caso, a proteção de dados seria algo semelhante à proteção ao consumidor: um conjunto de normas e órgãos sem os quais o titular dos dados estaria suscetível a toda sorte de abusos. A tarefa do legislador, no que aqui nos interessa, consistiria em garantir esses *standards* de proteção do titular dos dados pessoais para compensar a sua vulnerabilidade; e isso especialmente em razão do advento de novas tecnologias e das possibilidades de tratamento que oferecem aos órgãos de segurança pública e persecução penal. Embora tais normas e órgãos sejam necessários, essa forma de compreender a proteção de dados ignora um aspecto fundamental do problema: o *status* constitucional dos dados pessoais.

Dados pessoais são protegidos por meio dos direitos fundamentais que conformam a garantia ao livre desenvolvimento da personalidade (autodeterminação informacional, sigilo das telecomunicações, garantia de confiabilidade e integridade dos sistemas informáticos, inviolabilidade do domicílio etc.). Isso significa que, assim como vida, liberdade, integridade corporal etc., aqueles direitos se encontram no âmbito de uma esfera protegida em relação à qual o Estado tem um *dever de abstenção* – e isso não no sentido de um mero programa a ser realizado, mas como direitos de *aplicação imediata* (art. 5 § 1º CF). A regra, portanto, é a abstenção: esses referidos direitos fundamentais funcionam, em primeira linha, como direitos de defesa do indivíduo dirigidos *contra* o Estado, fundamentando, apenas em segundas considerações, a proteção ativa daquilo que protegem.[13] Deste modo, o termo *proteção* de dados deve ser compreendido como proteção (constitucional) *dos* dados, e não como proteção (estatal) *aos* dados: não se trata de obrigar o Estado a conferir proteção aos dados, senão de dotar os dados de proteção intrínseca contra a ingerência do Estado.[14] Isso quer dizer que, em regra, o Estado não pode intervir; e que exceções a isso têm de ser especialmente justificadas a título de *intervenções* nessa esfera protegida. É o paradigma da abstenção que deve orientar a proteção de dados nas áreas da segurança pública e do processo penal. Dessa primeira aproximação é possível formular a seguinte orientação: a primeira tarefa de uma legislação da

[13] O direito à autodeterminação informacional (diferentemente dos outros mencionados), por exemplo, esgota-se praticamente em sua função de defesa; exceção é feita ao dever de proteger os interesses do indivíduo de tomar conhecimento das medidas informacionais do Estado que afetem (também outros de) seus direitos fundamentais. Fala-se, aqui, em um *direito à tomada de conhecimento* (Recht auf Kenntnis). Cf. BVerfGE 120, 351, 360 s.

[14] Uma comparação ajuda a esclarecer essa posição: o direito à vida gera duas naturezas de dever ao Estado, de um lado, o dever de se abster (ou de não matar), de outro, o dever de proteger a vida (p.ex., proibindo que se mate).

proteção de dados nessa área consiste em estabelecer quais formas de tratamento de dados pelo Estado – ou seja, quais formas de intervenção – são constitucionalmente legítimas.

Esse é o caminho que consideramos mais adequado para encarar o complexo problema da proteção dos dados. E esse nosso julgamento não decorre apenas de considerações dogmáticas. Isso também está refletido em opções do próprio legislador brasileiro. O regime de proteção de dados foi expressamente inserido em uma moldura constitucional (arts. 1º e 2º LGDP). Dentre os direitos referidos na lei, destaca-se a menção aos direitos ao livre desenvolvimento da personalidade e à autodeterminação informacional. Essa moldura constitucional é o que dá fundamento à opção feita pelo legislador brasileiro não somente pela disciplina unificada dos âmbitos público e privado, mas também pelo tratamento de dados submetido ao denominado *princípio da proibição com reserva de permissão*[15], aplicável também às atividades de segurança pública, persecução criminal e inteligência (art. 4º § 1º LGPD). Esse dispositivo condiciona o tratamento de dados nos referidos âmbitos a legislações específicas, que devem prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público. Se bem entendido, o dispositivo não é outra coisa senão a enunciação de dois princípios fundamentais da dogmática constitucional: o princípio da reserva de lei (todo tratamento de dados pessoais pressupõe autorização em lei) e o princípio da proibição de excesso (intervenções para o atendimento de interesses públicos devem ser proporcionais).

São esses, portanto, os fundamentos que devem reger o tratamento de dados na segurança pública e no processo penal. Sua devida apreensão é imprescindível para a compreensão das diretrizes oferecidas neste Parecer. Por essa razão, seguem algumas breves considerações sobre esses fundamentos constitucionais, naquilo que interessam à proteção de dados pessoais.

I. A reserva de lei e a reserva parlamentar: o conteúdo das normas autorizativas de intervenção informacional

A clássica e primordial função[16] dos direitos fundamentais, enquanto *direitos de defesa*, é exigir atitude *geral* de abstenção do Estado. Eles formam uma barreira contra condutas de agentes estatais que atingem âmbitos protegidos da vida do indivíduo. Por isso, a fim de que se possa saber se uma ação estatal está, a princípio, bloqueada

[15] Sobre esse princípio, que caracteriza o modelo europeu em oposição ao modelo americano, de regulação em parte pontual, ver *Tinnefeld et al.*, Einführung in das Datenschutzrecht, 7. ed. 2019, pp. 239 ss.
[16] Sobre as demais funções, aqui, menos relevantes, cf. por todos *Greco*, Introdução, in: Wolter (org. por Greco). O inviolável e o intocável no direito processual penal, São Paulo: Marcial Pons, 2018, pp. 35 s., com outras referências.

pelo respectivo direito, é importante, em primeiro lugar, estabelecer definições precisas de seu âmbito de proteção. Como cada direito fundamental protege aspectos ou dimensões diferentes da vida, também é natural que cada um esteja dotado de maiores ou menores artefatos defensivos/protetivos. O direito fundamental à vida imporá, por exemplo, altas exigências para que seja autorizada uma ação estatal perigosa para a vida. Já o direito à inviolabilidade do domicílio não protege algo tão essencial como a própria vida, de modo que a entrada de um agente no domicílio pode ser autorizada em situações menos urgentes e perigosas; entretanto, para coibir a banalização da entrada estatal no domicílio do indivíduo, isso será possível uma vez respeitadas algumas outras exigências e tomadas certas precauções. Portanto, como já é possível notar, direitos fundamentais não formam uma barreira intransponível à ingerência do Estado, de modo que a corriqueira afirmação de que esses direitos não são absolutos[17] é, quando não vazia, redundante.

Diante do imperativo jurídico de proteger os indivíduos e a sociedade e de promover os fins que lhe incumbem (por ex., art. 3º CF), o Estado pode ver-se forçado a adentrar, ou seja, a *intervir* nos espaços individuais protegidos pelos direitos fundamentais. Ocorre que, como os direitos fundamentais de liberdade antecedem aos interesses estatais,[18] o Estado necessitará, para tanto, de uma *justificação especial* para sua ação de intervenção. Como cada direito fundamental apresenta distintas barreiras protetivas, essa justificação varia segundo o direito fundamental afetado. Uma ação de intervenção não justificada é, portanto, uma violação do direito fundamental: o Estado, em tal situação, desconsidera as exigências do direito – como as regras preestabelecidas do jogo – e age sem legitimidade. Portanto, é na dogmática dessa justificação especial para uma ação interventiva, fundamentada na atitude geral de abstenção do Estado, que devem ser encontradas as respostas à Consulta que nos fora formulada.

Em um Estado de Direito, como o brasileiro, os direitos fundamentais demandam, dos poderes *executivo* (investigador e acusador) e *judiciário*, atuação, além de *proporcional* no caso concreto, nos *estritos limites da autorização* democrática: é o povo que escolhe o que o *seu* Estado pode ou não fazer no exercício de suas competências. Ou seja, o povo, em sua Constituição, por meio de direitos fundamentais, estabelece o que estaria sob proteção geral, reservando, assim, a si próprio, a posterior decisão sobre exceções que atendam seus eventuais interesses circunstanciais. Daí surge, na dogmática constitucional, o conceito de *normas autorizativas* (art. 5º II CF) – por meio das quais o parlamento autoriza intervenções em direitos fundamentais – em contraponto a normas de competência.[19] A máxima dessa distinção é a ideia de que **de competências**

[17] Essa afirmação costuma negligenciar, muitas vezes, o fato de que alguns direitos fundamentais são, sim, absolutos, por não permitirem qualquer intervenção em seu âmbito de proteção, como o direito de não ser torturado (art. 5º III CF). Neste sentido, o STF: HC 70.389/SP, rel. Min. Celso de Mello, DJ 23.6.1994. Com mesma posição, *Sarlet*. Teoria Geral dos Direitos Fundamentais, em: Sarlet/ Wolfgang/Marinoni/Mitidiero. Curso de Direito Constitucional, 7. ed., São Paulo, 2018, pp. 436 ss., que apresenta outras considerações.

[18] *Wolter* Jürgen. Proteção de dados no processo penal (trad. Alaor Leite), em: Wolter, Jürgen. O inviolável e o intocável no direito processual penal, Luís Greco (Org.), 2018, p. 199.

[19] Normas de competência distribuem as atribuições do Estado entre suas instituições: por exemplo, a este compete investigar, àquele, acusar, ao outro, julgar. Normas autorizativas dão àquelas instituições competentes, por outro lado, o direito de intervir neste ou naquele específico direito individual, a fim de cumprirem esta ou aquela tarefa que lhes competem. A respeito, cf. *Greco* (nr. 16), p. 36 ss.

não se derivam autorizações. O conteúdo dessas autorizações é o limite *dirigido ao poder legislativo*: forma e proporcionalidade. Ou seja, a ideia é que o legislador poderá autorizar intervenções naquele âmbito da vida humana protegido pelo direito fundamental, desde que de forma clara e precisa e respeitando um mínimo conteúdo essencial (intocável[20]), a fim de intervir sem eliminar o direito; para além disso, essa intervenção deverá perseguir um fim constitucionalmente legítimo segundo um ideal de proporcionalidade, que evita o sacrifício desnecessário e inadequado dos direitos do indivíduo. Para fazer uso da construção de *Kingreen* e *Poscher*, "na conexão dos atos legislativos aos direitos fundamentais, a reserva de lei se transforma em reserva de lei proporcional". Ou seja, "com a reserva de lei, os direitos fundamentais repelem e bloqueiam ações interventivas da administração sem base legal, com a reserva de lei proporcional, bloqueiam leis interventivas desproporcionais".[21]

Isso significa que, em princípio, desde que respeitado o núcleo essencial dos direitos fundamentais, em cujo âmbito uma intervenção jamais pode ser justificada, o legislador está autorizado a estabelecer restrições ao exercício de direitos fundamentais em algumas circunstâncias, mas está submetido, ele mesmo, a determinados limites nessa atividade restritiva (ideia conhecida como *restrições a restrições*). Uma das restrições à atividade restritiva é a *reserva parlamentar*, que encontra seu fundamento também na ideia de que o poder legislativo serve como garantia do indivíduo e, portanto, não pode delegar as decisões *essenciais*[22] sobre a intervenção que autoriza, senão ponderá-las e tomá-las ele mesmo.[23]

Outra consequência dos fundamentos da reserva de lei e parlamentar é o fato de que a CF (art. 5º II), assim como grande parte de suas equivalentes estrangeiras, não faz concessões a autorizações por portarias, decretos, regulamentos ou outro ato normativo diferente de lei. Isso porque não há autorização constitucional a agentes não-parlamentares para que decidam, fora do processo democrático, impor restrições a direitos de defesa que valem, principalmente, contra eles. De outra forma, a existência de direitos fundamentais reduz-se a nada, possibilitando que qualquer agente estatal realize juízo próprio sobre a ponderação de seus interesses em relação a direitos alheios. Esse juízo decisivo, enquanto criador de poderes e deveres, está reservado ao povo, que o exerce no parlamento. Assim, a **principal diretriz** para a regulação da proteção de dados nos setores da segurança pública e do processo penal é a defesa intransigente da reserva de lei e da reserva parlamentar na confecção de normas autorizativas de tratamento de dados, enquanto salvaguardas essenciais dos

[20] A respeito, com mais referências, *Greco* (nr. 16), pp. 32 ss.
[21] *Kingreen/Poscher* (nr. 8), p. 94, nm. 325.
[22] A respeito da teoria da essencialidade (*Wesentlichkeitslehre*), cf. *Kingreen/Poscher* (nr. 8), p. 315, que pode, no que interessa, ser reduzida à ideia de que a decisão sobre os pressupostos, as circunstâncias e as consequências das intervenções deve ser tomada pelo legislador e não pode ser delegada à administração ou ao tribunal.
[23] *Kingreen/Poscher* (nr. 8), p. 95, nm. 329.

direitos da personalidade. Não há como juízes, policiais ou órgãos da administração pública superarem a ausência de uma autorização do parlamento, ainda que creiam fortemente fazê-lo por razões justas. Tornando mais claro: o juízo de ponderação sobre a necessidade de uma intervenção no caso concreto não substitui nem se confunde com aquele sobre a possibilidade dessa intervenção, que se traduz em seu fundamento legal.[24] Este último é objeto do debate parlamentar.

Se intervenções (informacionais) precisam estar autorizadas em lei, também é claro que apenas aquilo que se pode compreender da leitura da norma autorizativa pode, de fato, estar autorizado. Por essa razão, é atributo da reserva de lei o chamado *imperativo de determinação e clareza*: é necessário autorizar expressamente a ação naturalística (interceptar, infiltrar, armazenar etc.) em si, ou seja, não bastam previsões gerais do estilo "métodos para obtenção/tratamento de informações". Aqui, é a perspectiva do indivíduo a medida do imperativo: é preciso, substituindo-se a ele, questionar se a ação interventiva era, da leitura da norma, previsível.

Fazem-se exceções com relação às medidas bagatelares, que, por seu baixo grau interventivo, estariam autorizadas por cláusulas gerais contidas em normas de competência. Contudo, justamente em relação às intervenções informacionais por meio de modernas técnicas de vigilância, o legislador alemão, por exemplo, passou a detalhar cada uma das medidas, sobretudo porque instado pelo BVerfG a fazê-lo.[25] Cláusulas gerais de autorização não são boas opções em situações de coleta e armazenamento de dados, pois autorizariam, com poucos limites, imprevisíveis intervenções estatais de diversas naturezas, que, aos poucos, começarão a impor intrincados desafios e a traduzir-se em insegurança jurídica. Essa prática subverteria a ideia de autodeterminação informacional, já que o indivíduo perderia o controle sobre quais de seus dados podem ser levantados, usados e armazenados e, assim, de quem sabe o que a seu respeito; e isso em uma contingência onde, a princípio, "não existem dados irrelevantes". Há variadas razões, portanto, para cautela ao empregar cláusulas gerais na proteção dos dados. Também o parlamento e o conselho da União Europeia impuseram a mesma obrigação (Cons. 33 e art. 8 DPD), exigindo que, em uma intervenção informacional, pelo menos, o objetivo e o propósito do processamento de dados – e de especificamente quais dados – devem ser previsíveis ao indivíduo segundo a norma que o autoriza, "a fim de oferecer garantia suficiente contra perigos de abuso e arbítrio" (Cons. 33 DPD).

[24] Divergindo, Clever *Vasconcellos*. Interceptação telefônica, São Paulo, 2011, p. 60, que não apenas enxerga no próprio art. 5º XII CF (que afirma um direito!) a norma jurídica que determina procedimentos da escuta telefônica, mas [p. 65 s.] chega a questionar também a reserva judicial. Escora-se, para tanto, em errôneas compreensões, tanto das "palavras de Ada Pellegrini Grinover: as liberdade públicas não podem ser entendidas em sentido absoluto"] como do fato de que o sigilo imposto à autoridade policial requerente dos dados de comunicação às empresas telefônicas seria suficiente para garantir a privacidade, ignorando portanto também a autonomia de cada modalidade interventiva e a distinta natureza de ambas as garantias.

[25] *Roxin/Schünemann*, Strafverfahrensrecht, 29. ed. 2018, §9 nm. 19. Cf. Também *Schenke*, Polizei- und Ordnungsrecht, 10. ed., 2018, p. 25, nm. 50: „O levantamento de dados pessoais não pode ter seu fundamento em cláusulas gerais do direito de polícia [ou seja, de normas de competência]. Essa é uma consequência da jurisprudência do BVerfG a respeito do direito à autodeterminação informacional, que exige para essas intervenções regulações específicas a cada âmbito (...)".

II. Regramento específico para as distintas atividades estatais e o princípio da separação informacional

Enquanto direitos de defesa e com seu instrumentário da proporcionalidade, os direitos fundamentais também não podem ser indiferentes aos fundamentos das intervenções contra as quais defendem. Cada ação interventiva baseia-se em um propósito distinto. Em alguns casos, diante de uma base fática sólida e estudada, é possível assumir que a intervenção informacional atingirá a esfera de uma pessoa suspeita de um crime, que, com alguma probabilidade, será condenada. Em outros, como durante uma manifestação popular, a intervenção atingirá, inevitavelmente, muitas pessoas, quando não todas, inocentes, com a finalidade de justamente evitar que crimes ocorram ou que os eventualmente ocorridos não restem impunes. Ambos os fundamentos interventivos podem ser legítimos, mas é evidente que devem ser levadas em conta suas peculiaridades. Fiquemos com dois exemplos: enquanto o levantamento de dados para uso em processo penal pode reduzir riscos de afetação da esfera de terceiros insuspeitos, ele pode incrementar os riscos da tomada de conhecimento das informações (encartadas nos autos) por pessoas não autorizadas; já o levantamento de informações durante uma blitz policial não precisa, se assim indicarem as leituras dos documentos requeridos, ser convertido em um armazenamento, de modo que os dados levantados podem ser eliminados com brevidade. Por essas e outras razões, uma proteção adequada dos dados exige que sejam criadas bases legais para as intervenções informacionais de acordo com o preciso âmbito de atividade para a qual serão utilizadas.

Ocorre que dados não podem ser levantados sem um propósito legítimo (necessário e adequado), e as razões de previsibilidade – que permitem a autodeterminação informacional do indivíduo – impedem que, uma vez levantados, sejam utilizados, de forma indeterminada, para finalidades diversas. Daí falar-se em *vinculação finalística*. É o *levantamento*[26] dos dados – sem exagero – a *pedra angular* da proteção de dados pessoais no âmbito estatal. A forma como o Estado obtém informações pessoais, geralmente sem o consentimento do titular, define todas as regras do posterior processamento da informação (cf. também Art. 4 I b DPD).[27]

[26] Entende-se, neste trabalho, por levantamento toda forma de obtenção de dados. Embora, na discussão brasileira, *coleta* seja uma tradução frenquente (e *recolha*, na portuguesa) e incorporada pela LGPD (art. 5º X), o termo *levantamento* resolve a ambiguidade de que não se trata de uma obtenção de dados seguida de armazenamento. O armazenamento, por si só, é uma intervenção e carece de fundamento próprio. Por essa razão, demos preferência ao segundo termo, que é também o correspondente literal de *Erhebung* na discussão alemã (vide versão alemã da RGPD, art. 4 Nr. 2), em que os conceitos de formas de tratamento, enquanto formas autônomas de intervenção, foram desenvolvidos.

[27] *Johannes/Weinhold*, Das neue Datenschutzrecht bei Polizei und Justiz, 2018, p. 65.

Cada outra forma de processamento – o uso, o armazenamento e o compartilhamento – configura uma intervenção autônoma que estará vinculada ao propósito determinado na norma de levantamento. Por isso, diferencia-se entre determinação da finalidade e vinculação à finalidade. Enquanto autônomas intervenções, cada uma dessas quatro fases do processamento necessita de uma autorização (legislativa) específica, ainda que disciplinada no mesmo dispositivo. É também na vinculação à finalidade, portanto, que se fundamentam as ideias de renúncia a dados desnecessários (*Datenverzicht*), de evitação ou economia de dados (*Datenvermeidung*, *Datensparsamkeit*),[28] e da *proibição de armazenamento em estoque*[29] e do *imperativo de eliminação*[30]: sem clara determinação da finalidade que justifica o armazenamento ou vindo esta a se esgotar, é ilegítimo armazenar dados pessoais.

Alinhando ambas as considerações anteriores, a saber, de um lado, o necessário regramento das intervenções informacionais por área de atividade estatal e, de outro, a consequente vinculação às finalidades do levantamento, justifica-se a defesa da *separação informacional de poderes*[31]. Isso significa que é ilegítima uma base de dados comum a todos os órgãos estatais – nos moldes do Sinesp (art. 35 Lei Nº 13.675/2018), aprovado pelo então presidente Michel Temer – que armazene informações de inteligência e de segurança pública obtidas por autoridades dos mais diversos níveis (polícias, bombeiros, órgãos penitenciários, agentes de trânsito, guardas municipais etc.). Do contrário, não há como efetivar a proteção da autodeterminação informacional, cujo propósito máximo é, justamente, inviabilizar a coleta e o armazenamento indiscriminado de dados neste estilo. Isso só indica, contudo, que o legislador brasileiro parece ter recepcionado a autodeterminação informacional (art. 2º II LGPD) insciente de sua completa incompatibilidade com o banco de dados que aprovara quase que ao mesmo tempo. É de se esperar que esta latente incompatibilidade seja logo desvelada pelos tribunais brasileiros, e que isso se dê em favor da autonomia individual.

III. A dogmática da intervenção em direitos fundamentais

Encontra-se na literatura brasileira, com frequência, o apoio a dois recursos retóricos para fundamentação de intervenções que revelam de uma incompreensão básica da dogmática dos direitos fundamentais.

[28] Assim também *Greco* (nr. 16), p. 45.
[29] BVerfGE 65, 1, 46.
[30] BVerfGE 65, 1, 46; 100, 313, 362; 109, 279, 380.
[31] Cf. *Greco* (nr. 16), p. 45 ss., com várias referências.

O primeiro dos mencionados recursos retóricos é a afirmação, como antecipamos, de que direitos fundamentais não são absolutos. Com algumas exceções, como a proibição de tortura (art. 5º III CF) e de penas indignas (art. 5º XLVII CF), ela é uma das poucas ideias indisputáveis. São as consequências dela advindas que indicam a incompreensão dogmática. O fato de que direitos não são absolutos não significa que possam ser violados. E desse mal-entendido, encontrado volta-e-meia, surge o segundo recurso retórico: o de que o constituinte teria estabelecido inviolabilidades (absolutas) a certos direitos da personalidade.[32] O fato de um direito ser inviolável significa simplesmente que ele só comporta intervenções justificadas. Apenas intervenções *in*justificadas representam o que se conhece por *violações*. Por isso, onde se lê inviolabilidade no texto constitucional, não se deve compreender intangibilidade (intocabilidade)[33].

Para que essa ideia seja compreensível, é necessário conhecer outra diferenciação dogmática: aquela entre direitos submetidos a reserva de lei simples, a reserva de lei qualificada e direitos sem reserva de lei. Algumas normas do art. 5º CF, que estabelece os direitos fundamentais, acompanham-se de cláusulas de reserva de lei simples [basicamente: o legislador poderá autorizar intervenções], como a do direito geral de ação (art. 5º II CF). Outras apresentam uma reserva qualificada [intervenções são legítimas apenas para algumas finalidades ou em algumas circunstâncias], como a do sigilo das comunicações telefônicas (art. 5º XII CF). Há aquelas, por fim, que dão a aparente noção de uma proteção absoluta,[34] quando confrontada com as outras duas, já que, em relação a elas, o constituinte, ao afirmar o direito, silencia quanto à reserva. A esse terceiro grupo, *dos direitos fundamentais sem reserva de lei*, pertencem, por exemplo, o direito à livre manifestação do pensamento e – nesta ocasião, de particular importância – a inviolabilidade do sigilo da correspondência e dos *dados*. Com esses exemplos, é fácil perceber que a ausência de reserva de lei não pode significar, na sistemática constitucional brasileira, proteção absoluta. Fosse assim, seria ilegítimo punir a ofensa à honra (arts. 138 CP ss.), interceptar cartas de presidiários[35] e obter qualquer espécie de dados (o que é necessário admitir ainda que para fins estranhos à persecução penal). É possível abordar a questão de outra maneira, reduzindo o âmbito de proteção do determinado direito, de modo a não abranger os exemplos mencionados acima. Nesse caso, apenas a manifestação do pensamento inofensivo à honra seria livre. O fato de ser livre também a manifestação da ofensa – impassível de censura prévia,[36] embora passível de intervenção por pena dissuasiva – aponta para o fato de que a melhor solução parece ser a que enxerga autorização de certas

[32] *Grinover/Gomes Filho/Fernandes*. As nulidades do processo penal, 11ª ed., São Paulo, 2009, p. 167/168, *Streck*. As interceptações telefônicas e os direitos fundamentais, 2ª ed., Porto Alegre, 2001, p. 46 s.
[33] Explicações detalhadas já em *Greco* (nr. 16), pp. 32 s.
[34] Cf. *Sidi*. A interceptação das comunicações telemáticas, Belo Horizonte, 2016, pp. 219 ss., com outras referências.
[35] STF HC 70814-5/SP, j. em 1.3.1994.
[36] Cf., por exemplo, STF Rcl 38201 AgR/SP, j. em 21.2.2020; STF Rcl 28747 AgR/PR, j. em 5.6.2018.

intervenções também em direitos fundamentais sem reserva. Isso parece ainda mais correto ao não incluir no âmbito de proteção absoluta (do sigilo) certos dados que eventualmente precisem ser levantados. Mais vantajoso e coerente parece ser atribuir-lhes proteção relativa, exigindo justificação para a intervenção. Aceitando, portanto, que direitos fundamentais sem reserva também sejam passíveis de intervenção, estas deveriam ser submetidas, em geral, a duas exigências: "a primeira delas é que essas restrições estejam legalmente fundadas (nesse aspecto, eles não diferem dos direitos submetidos a uma reserva de lei); a segunda, é que esses direitos só possam ser restringidos em razão da tutela de outros valores de hierarquia constitucional"[37]. Com isso, deve ficar claro que autorização legal é fundamento de toda e qualquer intervenção em direito fundamental, e não se confunde com juízo de proporcionalidade. E que direitos sem reserva possuem maior peso na relação de proporcionalidade.

Essas exigências não criam problemas adicionais à regulação da proteção de dados na segurança pública e no processo penal, tendo em vista que o pressuposto que acrescentam à legitimidade da intervenção informacional é que esteja, esta, a cargo de outros valores constitucionais, o que se verifica tanto no caso da segurança pública (Preâmbulo e art. 144 CF) como no da *capacidade de funcionamento da justiça penal*[38] (Funktionstüchtigkeit der Strafrechtspflege)[39]. Ou seja, o direito fundamental à inviolabilidade do sigilo de dados – que, portanto, protege, de forma mais rigorosa, apenas dados em sigilo, e não todo e qualquer dado[40] (cuja proteção é dada pelo direito à autodeterminação informacional), pode comportar intervenções para a tutela de outros valores de hierarquia constitucional,[41] como a segurança pública e o processo penal. Enquanto isso, o direito ao sigilo das comunicações telefônicas, protegido pela reserva qualificada, é impassível de intervenção – por decisão expressa do constituinte – para qualquer fim que não seja a investigação e persecução penal, o que impede a quebra de sigilo telefônico para a atividade de segurança pública e de inteligência.

Como se percebe, essas considerações não estão em perfeita harmonia sistemática. A raiz disso está na (falta de) organicidade do texto constitucional. As soluções interpretativas apresentadas acima podem parecer arbitrárias, mas se justificam na exigência de coerência e permitem, ao mesmo tempo, a solução dos problemas reais com os quais nos deparamos. Dessa forma, dados sob sigilo não seriam absolutamente protegidos, de forma que seria legítimo ao juiz decidir sobre acesso a informações sigilosas (art. 3º-B XI d CPP). Também é possível, no entanto, entender por dados sigilosos apenas aqueles assegurados por cláusula jurídica de sigilo, a exemplo de certas informações reveladas em

---

[37] *Greco* (nr. 16), p. 37, com outras referências do direito alemão. Com menores exigências, *Mendes/Coelho/Branco*. Curso de Direito Constitucional, 2ª ed., São Paulo, 2008, p. 392, aos quais bastaria um juízo de proporcionalidade – dessa forma, estaria o constituinte, com seu silêncio sobre a possibilidade de uma restrição, deixando os específicos direitos mais vulneráveis a intervenções em relação àqueles aos quais afirma essa possibilidade (?); no mesmo sentido, *Cabette*, Interceptação telefônica, 3ª ed., São Paulo, 2015, p. 86.

[38] Preâmbulo CF: "(...) um Estado Democrático, destinado a assegurar o exercício dos direitos sociais e individuais, a liberdade, a segurança, o bem-estar, o desenvolvimento, a igualdade e a *justiça como valores supremos* de uma sociedade fraterna, pluralista e sem preconceitos, fundada na harmonia social e comprometida, na ordem interna e internacional, com a solução pacífica das controvérsias (...)".

[39] BVerfGE 46, 214, 222: "o Estado de Direito só pode realizar-se se houver a garantia de que os criminosos serão, nos limites das leis vigentes, perseguidos, julgados e conduzidos a sua justa punição". Cf. também BVerfGE 33, 367, 383; 38, 105, 115 s.; 38, 312, 321; 39, 156, 163; 41, 246, 250; EuGRZ 1977, 334, 338.

[40] Cf. outras considerações em *Greco/Gleizer,* RBDPP 5-3, 1483, pp. 1497 s.

[41] *Greco* (nr. 16), p. 37.

consulta médica (art. 73 Res. 2217/2018 CFM)[42] ou a defensor criminal (p.ex., art. 448 CPC; art. 207 CPP; art. 34 Lei 8.906/94[43]).[44] Nesse caso, estaria correta a CF em assegurar a proteção absoluta desses dados. Essa é certamente uma opção. Uma apropriada discussão a respeito extrapolaria, no entanto, nosso espaço, razão pela qual será deixada em aberto.

[42] Resolução do CFM, no uso das atribuições conferidas pelo art. 15 *d* da Lei 3268/1957. É importante observar que a imposição de sigilo ético na relação médico-paciente por meio de resolução não viola a reserva de lei, por não se tratar de intervenção, mas antes de proteção ao direito fundamental do indivíduo.

[43] A Lei 8906/84 (Estatuto da Advocacia e da Ordem dos Advogados do Brasil) menciona o sigilo profissional apenas na forma de infração disciplinar. Não se define ali o escopo desse sigilo.

[44] Cf. também *Greco/Gleizer* RBDPP 5-3, 1483, pp. 1505 s, para outras considerações sobre o sigilo profissional.

C. Algumas precauções em relação à Diretiva 2016/680 (DPD): a importância da legislação nacional no contexto europeu

No âmbito da União Europeia, após uma ampla reforma em 2016, a proteção de dados encontra-se regulada, principalmente, por dois diplomas: ao lado do já mencionado RGPD, a Diretiva 2016/680 (DPD) regula a proteção das pessoas naturais no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de *prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados*. Considerando a proximidade do regime de proteção de dados da UE e do Brasil, sedimentada na influência exercida pelo RGPD sobre a nossa LGPD, o caminho natural seria tomar igualmente a DPD como modelo para uma regulação brasileira do tratamento de dados nas áreas de segurança pública e processo penal. Há, no entanto, razões de sobra para desaconselhar esse proceder.

A construção de uma ordem jurídica regional na Europa não avança com a mesma velocidade em todos os âmbitos de atuação estatal. É esse o caso, por exemplo, quanto à segurança pública e ao processo penal, em que os esforços de integração são notadamente mais hesitantes. Razão para isso é que atividades punitivas e policiais integram o núcleo da noção tradicional de soberania nacional, de modo que os Estados se mostram receosos em abdicar delas em nome de uma integração regional. Antes do Tratado de Lisboa, segurança pública e processo penal integravam o chamado "terceiro pilar", em que a integração se restringia a uma cooperação intergovernamental, sem que se reconhecesse uma organização supranacional com competência soberana em relação aos Estados e seus cidadãos. Por essa razão, a proteção de dados nos referidos âmbitos era, antes da DPD, regulada pela Decisão-Quadro 2008/977/JAI, que visava, especificamente, à criação de parâmetros para a transmissão de dados entre Estados-Membros no contexto de cooperação policial e judiciária em matéria penal. Com o Tratado de Lisboa de 2009, o modelo dos três pilares é abolido, e também a cooperação entre polícia e justiça em matérias criminais passa a ter natureza supranacional. Entretanto, como o Tratado previa em relação a esse âmbito um período de transição de cinco anos, isso passou a valer de fato apenas em 2014.[45]

A DPD, que substitui a mencionada Decisão-Quadro 2008/977/JAI, revela ainda, em vários aspectos, essa postura hesitante em relação à integração em matéria policial e jurídico-penal. Já o fato de que se optou por um regramento em separado, paralelo ao regime geral estabelecido pelo RGPD, é revelador dessa hesitação.[46] Enquanto o RGPD, em razão da natureza de *regulamento* na ordem jurídica da EU (Art. 288, 2

[45] Sobre esse desenvolvimento, cf. *Ambos*, Internationales Strafrecht, 5. ed. p. 416 ss.
[46] Nesse sentido, também *Tinnefeld et al.*, Einführung in das Datenschutzrecht, 7. ed. 2019, p. 340; *Rüpke/v. Lewinski/Eckhardt,* Datenschutzrecht, 2018, p. 116.

AEUV), goza de aplicação imediata nos Estados-Membros, compondo parte de suas ordens jurídicas, optou-se, para as matérias ali excetuadas, por uma regulação por meio de simples *diretiva* (Art. 288, 3 AEUV), garantindo, assim, maior liberdade aos Estados-Membros na implementação de suas próprias normas.[47] Isso significa que, enquanto o RGPD é endereçado diretamente ao aplicador do direito, a DPD tem os Estados-Membros como endereçados, que devem aplicá-la.[48] Por fim, muitas regras aprovadas na DPD têm um caráter genérico e perseguem o fim de harmonização mínima da proteção de dados entre os Estados-Membros. Ênfase é dada a definições, princípios gerais, garantias procedimentais para assegurar os direitos do afetado e regras para a transferência internacional de dados. Deixa-se aos Estados-Membros, com isso, amplo espaço de implementação, uma vez que *as formas de tratamento autorizadas não são ali reguladas*.[49] O art. 8º DPD apenas exige que o tratamento de dados ocorra com base no direito da União ou de um Estado-Membro. Com isso, a tarefa mais fundamental de um regime de proteção de dados nos âmbitos de segurança pública e processo penal, qual seja, a de determinar em que circunstâncias e como o Estado pode intervir na esfera protegida dos dados pessoais, *fica a cargo das legislações nacionais*.[50] O legislador europeu pode, por isso, se contentar com esse objetivo modesto, uma vez que a implementação da DPD dá-se paralela e complementarmente às normas já existentes nos Estados-Membros, que regulam, cada um à sua maneira, as formas concretas de tratamento.

Não é esse, entretanto, o cenário brasileiro. Há uma grave deficiência de leis que autorizem e regulem propriamente o tratamento de dados pessoais nos âmbitos da segurança pública e do processo penal, e obviamente não há sentido em se falar em esforços de harmonização mínima, tal como perseguido no contexto europeu, já que não contamos com um processo de integração regional semelhante.

O processo penal brasileiro é deficiente em normas que autorizem e regulem intervenções no âmbito protegido dos dados pessoais. Embora haja, por exemplo, (insatisfatória) regulação em lei para interceptações telefônicas (LIT) ou infiltrações de agentes (arts. 10 ss. Lei 12.850/13), medidas como infiltrações online[51] ou observações prolongadas, dentre tantas outras, não estão autorizadas/reguladas. Veja-se que os exemplos mencionados, os poucos que temos, se referem todos a âmbitos de sigilo, de modo que da proteção de dados não pertinentes a zonas de sigilo pouco se tem notícia. Há, além disso, grave ausência de regulação legal para as demais formas de tratamento: arquivamento, alteração, utilização e, em especial, o compartilhamento. Quanto à segurança pública, a situação é extremamente crítica, pois a ausência de

[47] *Roßnagel*, Geleitwort, in: Johanes/Weinhold, Das neue Datenschutzrecht bei Polizei und Justiz, 2018, pp. 6 ss.
[48] *Johanes/Weinhold*, Das neue Datenschutzrecht bei Polizei und Justiz, 2018, p. 31.
[49] *Gola/Heckmann*, § 45 BDSG nm. 5; *Johanes/Weinhold*, Das neue Datenschutzrecht bei Polizei und Justiz, 2018, p. 68.
[50] *Johanes/Weinhold*, Das neue Datenschutzrecht bei Polizei und Justiz, 2018, p. 69.
[51] A respeito, cf. abaixo em D.I.3.

regras para o tratamento de dados inserem-se no contexto de um problema ainda maior: a inexistência de um direito de segurança pública no Brasil.[52] Controle de identidade, emprego de câmeras de vigilância em espaços públicos ou das denominadas *Body-Cams*, observações prolongadas, levantamento de dados de telecomunicação, criação de bancos de dados etc., para tudo isso há carência de uma adequada regulação em lei. É importante notar, como exposto acima (B.I), que atos normativos supralegais, como decretos, regulamentos, regimentos, portarias etc., não servem para a fundamentação formal de uma ação interventiva estatal, ou seja, uma afetação de esfera individual protegida por um direito fundamental.

Uma forte orientação pela DPD, desprezando a profunda diferença entre os contextos europeu e brasileiro, traria consigo uma série de implicações problemáticas. Ela conduziria, sobretudo, a uma falsa avaliação daquilo que é prioritário em termos de um regime de proteção de dados. É imperioso saber, em primeiro lugar, em que circunstâncias e sob quais requisitos o Estado está autorizado a intervir no direito de autodeterminação informacional e nos demais direitos que protegem dados pessoais. Essa é a pergunta sobre a licitude do tratamento de dados, que, como visto, a DPD não responde (art. 8º DPD), embora esse seja um pressuposto de várias de suas normas. Pode-se dizer que as normas de autorização para o tratamento de dados gozam de uma *prioridade normativa* em relação a outras normas de proteção mais gerais. A DPD prevê, por exemplo, um direito de informação dos titulares de dados, direito este, no entanto, que, se necessário, pode ser parcial ou inteiramente limitado para a realização das atividades de segurança pública e persecução e execução criminais (art. 15 a, b, c DPD). O que determina em que circunstâncias esse direito é limitado são normas sobre a forma concreta de tratamento dos dados. Outro exemplo: a transferência internacional de dados é uma forma de tratamento que decorre, em regra, do levantamento e arquivamento de dados por órgãos da segurança pública. A ilicitude do levantamento e arquivamento tem consequências, no entanto, para a permissibilidade da transferência. E, como afirmado, quais formas de levantamento ou arquivamento são legítimas, e como são legítimas, não é objeto de regulação da DPD.

Tampouco se poderia pensar em um sistema de controle externo e de sanções em razão de tratamento ilícito, se não há regras que especifiquem que formas de tratamento são lícitas. Para a atividade dos órgãos de segurança pública e persecução penal, isso implicaria uma situação de grave insegurança jurídica, diante da ausência de esclarecimento concreto sobre o que é permitido ou não, e com ela a tendência a um

[52] Para uma breve descrição do problema, ver *Estellita/Montenegro/Gleizer*, Por um direito de segurança pública, Estadão, acessível em: https://politica.estadao.com.br/blogs/fausto-macedo/por-um-direito-de-seguranca-publica/; cf. também a monografia de *Filocre*, Direito Policial Moderno - Polícia de Segurança Pública no Direito Administrativo Brasileiro, 2017.

excesso de judicialização. Essa situação incomum de ausência de normas autorizativas claras e precisas, além do mais, não impõe obstáculo somente à segurança jurídica, ela significa, tomada rigorosamente, a verdadeira antítese do direito de proteção de dados: a imprevisibilidade pelo indivíduo quanto ao uso de seus dados.

Por isso, pensam os signatários que as principais diretrizes para a proteção de dados na segurança pública e no processo penal são aquelas atinentes à conformidade das normas autorizativas de tratamento de dados da correspondente legislação brasileira aos princípios e regras gerais do tratamento de dados nesses setores. Esses princípios e regras gerais, voltados às definições conceituais, aos princípios, aos direitos do titular de dados, aos deveres dos controladores e operadores, à segurança dos dados e à transferência de dados pessoais para países estrangeiros ou organizações internacionais – para citar alguns exemplos – já estão expostos na DPD. A sua aplicação concreta, em forma de lei, nos Estados-Membros pode variar em certa medida. A forma como essas normas gerais foi implementada na Alemanha (§ 45 ss. BDSG) pode servir de exemplo para a criação de dispositivos similares na legislação brasileira. A questão mais complicada e fundamental, sobre a qual concentraremos, portanto, nossos esforços em busca de uma real proteção dos direitos informacionais é aquela atinente à conformidade das normas autorizativas de tratamento de dados. Essas não são objeto da DPD.

D. Intervenções informacionais para fins de segurança pública

I. A garantia da segurança pública

Um primeiro grupo de medidas interventivas no âmbito constitucionalmente protegido dos dados pessoais são aquelas realizadas pelo Estado com o fim de *proteção contra perigos para a segurança pública*. Antes de uma exposição concreta das diversas formas de intervenções e seus critérios, são necessárias breves considerações gerais, a fim de que o tratamento de dados para fins de garantia da segurança pública seja compreendido no contexto geral desta atividade estatal e do controle normativo específico que ela pressupõe.[53]

A noção de Estado de Direito é profundamente marcada por uma diferenciação de funções estatais, que vai muito além da conhecida separação dos poderes legislativo, executivo e judiciário[54]. A clara determinação das funções exercidas pela administração pública implica não só maior eficiência da ação estatal, mas também a possibilidade de ponderar corretamente a legitimidade da medida em face do fim perseguido. Para a atividade dos órgãos dedicados à segurança interna, isso implica uma *estrita diferenciação* entre atividade de segurança pública, persecução e punição de delitos e inteligência, ainda que essas atividades sejam realizadas em parte pelos mesmos órgãos e possam estar reunidas sob o escopo geral da segurança interna.[55] Tratando-se de finalidades distintas, há outros pressupostos para a atuação, e o controle normativo tem de ser, consequentemente, específico para cada uma delas. É essa a razão pela qual a RGPD e a DPD se referem de forma explícita e destacada a cada uma dessas atividades (art. 2º I d RGPD; art. 1º DPD).

Em especial quanto ao tema deste tópico, as referidas normas destacam "a salvaguarda e prevenção de ameaças à segurança pública". A ideia de que a atividade de polícia se restringe à proteção contra perigos para a segurança pública está intimamente vinculada ao desenvolvimento do Estado de Direito e surge, na Alemanha, em contraposição a um chamado Estado policial, em que a atividade de polícia abrange

[53] Optou-se aqui por não incorporar o uso do termo "polícia", corrente na Europa para se referir a essa atividade estatal dirigida à proteção contra perigos. No Brasil, o termo está muito vinculado aos órgãos denominados policiais (polícias civis e militares, polícia federal, polícia rodoviária federal etc.), ou seja, a um conceito institucional de polícia. Um conceito material de polícia, no entanto, refere-se a toda atividade voltada à proteção contra perigos para a segurança e ordem públicas, e abrange, com isso, também atividades de outros órgãos, como o corpo de bombeiros ou órgãos de controle de trânsito. Optamos, assim, por falar em garantia de segurança pública e direito de segurança pública, para deixar claro, desde o princípio, do que se trata. Sobre os diferentes conceitos de polícia, ver, p.ex., *Schenke* (nr. 25), § 1 nm. 1 ss; *Guedes Valente*, Teoria Geral do Direito Policial, 6. ed., 2019, pp. 54 ss.

[54] Para os fundamentos, cf. *Lewinski* (nr. 5), p. 55 ss.

[55] Sobre o conceito de segurança interna, cf. *Götz,* Innere Sicherheit, in: Handbuch des Staatsrechts IV, 3. ed. 2006 § 85, p. 673, Rn 3 ss. Para uma análise da segurança como um campo do direito, *Gusy*, Sicherheitsrecht als Rechtsgebiet?, in: Dietricht/Gärditz (org.), Sicherheitsverfassung – Sicherheitsrecht, 2019, pp. 9 ss.

todas as atividades de realização do bem-comum.[56] No Brasil, a doutrina administrativista menciona, de forma genérica e confusa, um poder de polícia[57] e costuma distinguir entre polícia administrativa e polícia judiciária.[58] Há, no entanto, pouca clareza sobre o significado desses termos. Não há uma legislação comparável que regule a atividade da polícia protetiva, tampouco uma disciplina jurídica dedicada ao tema.[59] O próprio texto constitucional não é explícito sobre a quem compete legislar nessa matéria, se União, Estados ou Municípios. Na prática, a atividade de segurança pública é realizada muitas vezes sem amparo legal ou com base em normas do CPP (pensadas e ponderadas para situações distintas), que explicitamente se aplicam aos órgãos de polícia apenas quanto ao fim de apuração das infrações penais e da sua autoria (art. 4º CPP). Há, nisso, resquícios de um Estado policial, para cuja superação o anteprojeto de lei em questão pode, em nosso entender, contribuir. As bases para o desenvolvimento dessa contribuição serão apresentadas a seguir.

II. Aspectos centrais de um direito de segurança pública: bem protegido, perigo e destinatários

Normas de autorização só podem ser avaliadas em sua adequação quando consideradas em relação ao fim estatal específico que se busca realizar. Assim sendo, normas que autorizem o tratamento de dados no âmbito da segurança pública pressupõem a compreensão precisa do que caracteriza essa atividade. Uma vez que um direito de segurança pública é praticamente inexistente no Brasil, impõem-se alguns esclarecimentos sobre aspectos centrais dessa atividade estatal. Trata-se de ações estatais que visam a) à garantia da *segurança pública*, b) eliminando ou prevenindo *perigos*, c) e que afetam determinados *destinatários*, em geral, num âmbito constitucionalmente protegido.

---

[56] Sobre o desenvolvimento histórico do conceito de polícia na Alemanha, ver *Knemeyer*, Polizeibegriffe in Gesetzen des 15. bis 18. Jahrhunderts, AöR 92, 2 Heft, 1967, pp. 153 ss.

[57] Entende-se, em geral, por poder de polícia os poderes da administração pública para restringir direitos individuais em nome de interesses públicos, ver, p.ex., *Di Pietro*, Direito Administrativo, 33. Ed., 2020, capítulo 5. Com razão, *Binenbojm* inclui o chamado poder de polícia dentre os elementos de uma tradição autoritária no direito administrativo brasileiro, cf. *Binenbojm*, Uma Teoria do Direito Administrativo, 3. Ed. 2014, p. 3, pp. 121 ss. Não é correto falar em poder de polícia, simplesmente porque não existe tal poder num sistema que reconhece direitos fundamentais. O que há, ou deveria haver, é uma série de *autorizações legais* para intervenções proporcionais no âmbito de proteção desses direitos. Somente se satisfeitos os pressupostos previstos em normas de autorização, e apenas dentro dos limites impostos, pode-se reconhecer algum espaço de discricionariedade.

[58] Cf. *Bandeira de Mello*, Curso de Direito Administrativo, 32 ed. 2015, pp. 857 ss.; *Di Pietro*, Direito Administrativo, 33. Ed., 2020, capítulo 5.4.

[59] Embora tenha sido desenvolvido como disciplina jurídica, sobretudo, na Alemanha, o chamado direito policial é estudado também em outros países. Em Portugal, p.ex., há inclusive considerável literatura manualística: *Valente* (nr. 53); *de Sousa*, Manual de Direito Policial, 2016; *Raposo*, Direito Policial, 2006.

1. Bem protegido: a segurança pública

Por segurança pública se entende, principalmente, um determinado estado de coisas: a ausência de violação da ordem jurídica.[60] Embora se fale em bem protegido, segurança pública não designa um conteúdo material próprio, mas só existe em referência às demais normas que compõem a ordem jurídica. Papel de maior relevância cabe às normas que estabelecem delitos e contravenções penais, pois designam condutas violadoras do direito. Em relação a normas de direito privado, a intervenção de órgãos de segurança pública deve ser subsidiária à proteção jurisdicional, sendo lícita apenas nos casos em que, sem a atuação daqueles órgãos, a realização de um direito se torna impossível ou muito improvável.[61]

A doutrina estrangeira menciona também outras duas concretizações do conceito de segurança pública: a inviolabilidade de bens individuais e a existência e funcionamento de instituições estatais. Essas duas concretizações são, no entanto, residuais, aplicando-se, sobretudo, em caso de eventos naturais que geram danos e perigos a direitos individuais e instituições. Não se podendo falar em violação da ordem jurídica, que pressupõe uma ação humana, complementa-se, com isso, o conceito de segurança pública.[62] Boa parte da doutrina discute sob a inviolabilidade de bens individuais também medidas para evitar perigos que o próprio titular do direito gera para si mesmo, em especial, para evitar o suicídio.[63]

Nesse contexto, discute-se também a *ordem pública* como um bem protegido, entendendo-se por ordem pública o conjunto de normas sociais e morais amplamente aceitas e necessárias para uma convivência pacífica.[64] No Brasil, o conceito de ordem e segurança pública são muitas vezes utilizados de forma indiscriminada. Se por ordem pública entende-se, no entanto, o referido há pouco, ou seja, uma determinada ordem social e moral, isso não deve, em nossa opinião, ser tido por um bem protegido, pois implica um conceito de difícil determinação e vulnerável a abusos.[65]

---

[60] Cf., p.ex., *Kingreen/Poscher*, Polizei- und Ordnungsrecht, 11. ed. 2020, pp. 99 ss., nm. 2 ss.; *Gusy*, Polizei- und Ordnungsrecht, 10. ed. 2017, p. 39; *Götz/Geis*, Allgemeines Polizei- und Ordnungsrecht, 16. ed. 2017, p. 22 ss.; *Denninger*, Polizeiaufgabe, in: Lisken/Denninger (org.), Handbuch des Polizeirechts, 5. ed. 2012; nm. 17.

[61] Essa subsidiariedade em relação à proteção jurisdicional de direitos privados está prevista, na Alemanha, nos próprios códigos policiais, ver, por exemplo, Art. 2 Abs. 2 do Código Policial da Baviera ou § 1 Abs. 4 do Código Policial de Berlim.

[62] Cf. *Kingreen/Poscher* (nr. 60), p. 105, nm. 21.

[63] Cf. *Götz/Geis* (nr. 60), p. 27 s., nm. 28, 30, 32 ss.

[64] Assim, p.ex., a definição legal de ordem pública no § 3 II do Código Policial de Sachsen-Anhalt: "O conjunto de regras não escritas para o comportamento de indivíduos em espaços públicos que se situem dentro dos limites constitucionais e cuja observação é tida, na concepção da maioria, como uma condição indispensável para a convivência pacífica dos cidadãos."

[65] Assim, *Kahl*, Verwaltungsarchiv 2008 451, 455 ss. Um panorama da discussão em torno do conceito de ordem pública na Alemanha, também com críticas à figura, é oferecido por *Bäcker*, Kriminalpräventionsrecht, 2015, pp. 312 ss.

2. Objeto material da ação estatal: o perigo

Perigo é talvez o conceito mais importante para um direito de segurança pública. Por um lado, ele distingue a atividade de segurança pública da atividade de persecução criminal (que não se vincula a perigos, mas a suspeitas); de outro, ele a separa também das atividades de inteligência, que se desenvolvem previamente à segurança pública e prescindem da vinculação estrita à ocorrência de um perigo mas não estão autorizados a realizar uma série de medidas a que a polícia está autorizada (busca e apreensão, detenção, identificação criminal etc.)[66]. Ou seja, a inteligência não pode agir.[67]

Perigo deve ser compreendido como a *probabilidade suficiente* de que uma situação ou um comportamento produzirá um dano a um bem jurídico, caso não haja uma intervenção no curso esperado dos acontecimentos.[68] "Suficiente" designa o grau de probabilidade, que, obviamente, não pode ser determinado com perfeita exatidão, mas oferece algum parâmetro de controle. Ao mesmo tempo em que não é necessário ter certeza sobre a ocorrência do dano, tampouco é suficiente a mera possibilidade de produção desse dano, na forma de suposições sem fundamentos fáticos.

No direito de segurança pública, costuma-se distinguir perigos concretos de abstratos, conferindo-lhes um outro sentido distinto do emprego tradicional em direito penal. Perigos concretos dizem respeito a casos individuais em que há probabilidade suficiente de dano a bens jurídicos, como, por exemplo, uma agressiva discussão entre dois jovens extremamente alcoolizados em um bar. Nesse caso, a ocorrência do dano pode ser previsivelmente concretizada em todos os aspectos relevantes: material (integridade corporal), pessoal (dois jovens), espacial (no bar) e temporal (momento da discussão). Perigos abstratos se referem a situações ou a comportamentos que, notoriamente ou em razão de conhecimentos científicos, tipicamente geram perigos para bens jurídicos. O porte de armas ou o consumo de bebidas alcoólicas em estádios de futebol, por exemplo, podem ser tidos como uma tal situação que tipicamente conduz a perigos.

Por fim, assume relevância nesse contexto também a intensidade do dano provável. Quanto maior a intensidade desse dano, menores são as exigências de probabilidade

---

[66] Nesse sentido, *Götz* (nr. 55) § 85, p. 693 s. nm. 39.

[67] *Greco* (nr. 16), p. 53; cf. também *Bull* FS-Götz, p. 347. Cf., p.ex., § 8 III BVerfSchG (Lei de Ofício Federal de Proteção à Constituição alemã): "Ao Ofício Federal de Proteção à Constituição não assistem faculdades policiais; ele tampouco pode requerer à polícia, por meio de cooperação institucional, a realização de uma medida cuja imposição não lhe é facultada.

[68] Sobre esta definição e demais especificações do conceito de perigo apresentadas a seguir, cf. *Kingreen/Poscher* (nr. 60), pp. 114 ss.; *Götz/Geis* (nr. 60), p. 42 ss.; *Denninger* (nr. 60), nm. 39 ss.

para a verificação de um perigo relevante. Por outro lado, se o dano é irrelevante, assumindo a forma de meros incômodos, tampouco há que se falar em perigo no sentido acima referido.

Não há como negar a vagueza do conceito de perigo, mas os elementos acima referidos oferecem parâmetros não só para excluir casos extremos aos quais o conceito evidentemente não se aplica. Esses parâmetros servem também de critérios para a adequação da medida e do nível de intervenção tolerável em direitos fundamentais. Em geral, perigos concretos e danos mais intensos autorizam intervenções mais invasivas do que perigos abstratos e danos de menor intensidade.

3. Objeto pessoal da ação estatal: os destinatários

Em regra, as medidas de garantia da segurança pública devem ter por destinatário os denominados "perturbadores", ou seja, aqueles a quem se pode atribuir a causa do perigo. Essa classe dos perturbadores se subdivide em perturbadores por comportamento (*Verhaltensstörer*), quando o perigo é substanciado em uma ação ou omissão, e perturbadores por estado (*Zustandsstörer*), nos casos em que o perigo advém de uma coisa pela qual o destinatário é responsável.[69]

É possível, entretanto, que normas especiais fixem os destinatários da ação estatal para além da figura tradicional do perturbador. Em especial, essa ampliação é particularmente comum em regras que autorizem o tratamento de dados para fins de prevenção de crimes. Consequência disso é que a licitude da medida deve estar estritamente submetida à *proibição de excesso*. Assim, a verificação de identidade não deve ser autorizada em relação a toda pessoa, em toda e qualquer circunstância, mas apenas em relação a pessoas, por exemplo, que se situam em locais de amplo acesso público, como praças, regiões de intenso comércio ou estações rodoviárias. No Brasil, embora a Lei 12.037/09 disponha sobre identificação criminal, não há regulação sobre em que situações a polícia está autorizada a verificar a identidade dos cidadãos. A possibilidade de levantamento indiscriminado de dados de identificação não é compatível com as exigências de proporcionalidade.

É esse, portanto, o quadro geral em que se devem inserir as normas de autorização para tratamento de dados pessoais no âmbito da segurança pública. Além de requisitos formais de licitude dos respectivos atos, a elaboração de normas para o tratamento de dados tem de levar sempre em conta os bens protegidos, o perigo em questão e o grupo

[69] Cf. *Kingreen/Poscher* (nr. 60), pp. 138 ss.; *Gusy* (nr. 60) pp. 203 ss.; *Götz/Geis* (nr. 60), pp. 87 ss.

dos destinatários. Esses três elementos compõem também a base para o juízo de proporcionalidade da medida.

II. Um exemplo de norma de autorização: a identificação eletrônica de veículos automotivos

Órgãos de segurança pública contam hoje, em vários países, com um sistema automatizado de identificação de automóveis. Por meio de câmeras de vídeo, faz-se o reconhecimento óptico da sequência que identifica os veículos, que é registrada e empregada para fins diversos. No Brasil, correm notícias na mídia sobre a utilização dessa tecnologia não apenas por órgãos de trânsito, mas também por órgãos de segurança pública e investigação criminal, inclusive com a possibilidade de cruzamento dos dados levantados com outros, pertinentes a bancos de dados estatais.[70] Há, entretanto, pouca discussão sobre a forma e as condições em que o reconhecimento automatizado de placas pode ser empregado. Embora essa tecnologia inquestionavelmente contribua para a maior eficiência das atividades de prevenção e investigação, ela permite um levantamento massivo e indiscriminado de dados pessoais, que, combinado com outras formas de tratamento, resulta numa grave ameaça a um regime de proteção da personalidade e da autodeterminação informacional.

Tornar a utilização dessa tecnologia compatível com um regime de proteção à autodeterminação informacional é uma tarefa das normas de autorização. Nisso a experiência alemã, que conta já com alguns anos de utilização dessa técnica e com uma regulação clara da matéria, inclusive com algumas decisões do BVerfG[71], também pode servir de ponto de partida para se pensar uma regulação própria para o Brasil. A seguir serão expostos os aspectos centrais da regulação dessa medida na Alemanha e uma versão traduzida de um dispositivo contendo uma norma autorizativa.

A tecnologia de reconhecimento automatizado de placas é, em geral, empregada na localização de pessoas ou objetos (*Fahndung*) e dá-se de acordo com o seguinte procedimento:[72] com base na imagem gerada por câmeras fixas ou móveis, um software faz o reconhecimento óptico da sequência de caracteres e números, que é armazenada e comparada com os dados referentes ao objeto da busca. No caso de uma

[70] Ver, p.ex., matéria do Intercept Brasil sobre o sistema Córtex, supostamente utilizado pelo Ministério da Justiça. Acessível em: https://theintercept.com/2020/09/21/governo-vigilancia-cortex/. Há também notícias que reportam a utilização dessa tecnologia pelas polícias estaduais. Ver, p.ex.: https://paranaportal.uol.com.br/geral/geral-geral/452-pre-testa-viaturas-placas/.
[71] BVerfGE 120, 378; BVerfGE 150, 244.
[72] Para uma descrição do procedimento, com mais referências, ver *Roßnagel* NJW 2008, 2547; *Guckelberger* NVwZ 2009, 352.

coincidência, o sistema notifica os agentes públicos, que então realizam as medidas necessárias (apreensão do veículo, prisão do foragido etc.). Os contornos para um uso proporcional dessa medida foram estabelecidos, em boa parte, pela própria jurisprudência constitucional, que conta com algumas decisões especificamente sobre normas que autorizam a identificação eletrônica de veículos.

Num primeiro momento, em uma decisão de 2008, o BVerfG analisou a constitucionalidade de dois dispositivos dos códigos de polícia dos Estados de Hesse e Eslésvico-Holsácia que autorizavam o levantamento da identificação dos veículos para fins de localização de pessoas e coisas.[73] O tribunal considerou que o levantamento não implicava uma intervenção no âmbito de proteção do direito à autodeterminação informacional nos casos em que o sistema aponta um resultado negativo do cruzamento de dados, desde que os dados levantados fossem imediata e automaticamente eliminados, não permitindo uma identificação dos afetados.[74] Já nessa decisão estabeleceu-se, no entanto, que uma autorização para o fim genérico de comparar os dados levantados com aqueles que se busca não seria suficiente. Seriam necessárias maiores especificações desse fim. Além disso, o princípio da proporcionalidade exigiria que a medida não fosse empregada de forma ampla e indiscriminada, desvinculada, portanto, de um *ensejo concreto*.[75]

Em uma decisão recente, o tribunal revisou a afirmação de que o levantamento massivo, seguido da imediata eliminação dos dados, não interviria no direito à autodeterminação informacional.[76] Tratava-se, no caso, de uma norma do Código Policial da Bavária, que autorizava a criação de postos de controle. Considerou-se que, nesse caso, os afetados não tinham seus dados levantados de forma acidental ou como consequência necessária da tecnologia empregada, senão que eram objeto direto de controle dos órgãos policiais. O simples fato de saber que seus dados estão sendo controlados teria consequências para o exercício da liberdade, pois implicaria uma situação em que os cidadãos são indiscriminadamente registrados, gerando um sentimento de estarem sendo constantemente vigiados. Isso implicaria uma intervenção no direito à autodeterminação informal e estaria sujeito a requisitos mais estritos.[77] Além da necessidade de um ensejo concreto para a criação de tais postos de controle, a proporcionalidade da intervenção exigiria também que a técnica fosse empregada apenas para a proteção de *bens jurídicos relevantes* ou *interesses públicos de peso correspondente*.[78]

[73] BVerfGE 120, 378.
[74] BVerfGE 120, 378 (399).
[75] BVerfGE 120, 378 (430).
[76] BVerfGE 150, 244.
[77] BVerfGE 150, 244 (266 ss.).
[78] BVerfGE 150, 244 (287 ss.).

Pode-se assim, com base nos critérios acima mencionados, resumir os requisitos que uma norma de autorização tem de conter. Quanto ao bem protegido, não é suficiente a mera referência à segurança pública. É necessária uma restrição a determinados bens jurídicos ou interesses públicos especialmente relevantes. O perigo em questão pode ser tanto concreto quanto abstrato. No último caso, no entanto, é necessário um ensejo concreto, um motivo fundado, para a medida. Pode-se vincular a isso um requisito formal para a licitude da medida, a saber, a fundamentação da medida com base nos elementos fáticos que a justificam. Quanto aos destinatários, não há restrições, já que a medida afeta, em princípio, todas aquelas pessoas que tomam parte no tráfico de veículos.

O art. 39 do Código Policial da Bavária, destinado exclusivamente à identificação eletrônica de veículos, oferece-nos um exemplo do que seria uma tal norma de autorização conforme os requisitos mencionados:

> **Art. 39 Sistemas automatizados de reconhecimento de placas**
> (1) [1]A polícia poderá, por meio do uso oculto de sistemas automatizados de reconhecimento de placas, levantar a identificação de veículos automotivos, bem como lugar, data, horário e direção, se a situação é correspondente à dos casos previstos no Art. 13 Abs. 1 Nr. 1 até 5. [2]No caso do art. 13 Abs. 1 Nr. 1a, a autorização vale apenas em relação a um perigo para um bem jurídico relevante e, no caso do art. 13 Abs. 1 Nr. 5, apenas para rodovias europeias ou federais. [3]O cruzamento da identificação com os dados policiais de busca será permitido
>
> 1. para veículos ou placas
> a) extraviados por meio de crimes ou de outra forma ou
> b) em relação aos quais há indícios de que serão utilizados para cometer crimes,
>
> 2. para pessoas registradas
> a) para observação policial, controle dirigido ou registro oculto,
> b) em razão de persecução ou execução penal, extradição ou transferência,
> c) para a realização de medidas de direito estrangeiro,
> d) para que contra ela se realizem medidas determinadas para a proteção contra perigos.
> [4]Um cruzamento com arquivos policiais criados para a proteção contra perigos em casos concretos ou em relação a acontecimentos que impliquem perigos de modo geral será permitido apenas quando necessário para a proteção contra aqueles perigos. [5]O levantamento da placa não será empregado de forma ampla e indiscriminada.
> (2) [1]As medidas constantes de Abs 1. serão apenas ordenadas pelas pessoas previstas em Art. 36 Abs. 4 Satz 2 und 3. [2]A ordem escrita deverá conter o destinatário e forma, amplitude e duração da medida concreta, bem como a seleção dos dados ou arquivos de busca e os motivos essenciais para sua determinação, inclusive a descrição das circunstâncias fáticas.
> (3) [1]Os dados referentes às placas levantadas com base em Abs. 1 serão imediatamente eliminados após o cruzamento de dados, sempre que a placa não corresponder aos dados ou arquivos da busca. [2]Exceto nos casos previstos em Abs. 1 Satz 3 Nr. 2, os reconhecimentos individuais não serão vinculados a uma imagem em movimento. [3]Cruzamentos segundo Abs. 1 não serão protocolados.

O art. 13 Abs. 1, a que se refere o dispositivo traduzido acima, regula as hipóteses em que a polícia está autorizada a realizar o controle de identidade. Em especial, ele é cabível em face da existência de perigos concretos (art. 13 Abs. 1 Nr. 1) e a determinadas localidades tidas por perigosas (art. 13 Abs. 1 Nr. 2). O legislador bávaro optou, então, por aplicar essas hipóteses também ao uso de sistemas de levantamento de placas.

E. Intervenções informacionais para o fim de persecução criminal

Embora a situação da proteção de dados no processo penal brasileiro não seja tão crítica quanto a quase absoluta ausência de correlata proteção no âmbito da segurança pública, pode-se dizer que também está longe da adequada conformidade. Ao mesmo tempo, é o processo penal a atividade com consequências sancionatórias mais graves para o indivíduo afetado, que pode ser mantido preso e, inclusive, punido. Aqui, portanto, devem ser concentrados muitos esforços para uma correta regulação da proteção de dados. Porque se, por um lado, afigura-se mais simples corrigir problemas e lacunas legais do que criar, praticamente do zero, um âmbito de regulação jurídica como o da segurança pública, por outro, é mais importante domesticar o uso das sanções mais graves. A isso se soma também o fato de que, em princípio, as intervenções na segurança pública que não estejam legalmente autorizadas não podem ser praticadas. É de se esperar que os tribunais, especialmente o STJ e o STF, estejam atentos para essa ilegalidade/ilegitimidade de intervenções sem fundamento legal e passem a exigir ação legislativa (criação de lei). No processo penal, normas autorizativas existentes podem, portanto, causar mais danos, porque estão (muitas vezes, desproporcionalmente) autorizadas na forma de suas redações.

À deficiente regulação de muitas normas autorizativas específicas para medidas investigativas,[79] soma-se ainda a inexistência de autorização para outras importantes na atual realidade tecnológica. Isso, por si só, resultaria, quando muito, em uma simples incapacidade funcional dos órgãos de persecução penal – sem comprometimento da autonomia informacional –, não fosse uma corriqueira posição de parte da literatura processual penal brasileira segundo a qual leis apenas *regulamentam* intervenções.[80] Se um direito fundamental permitir, em regra, uma intervenção, abre-se mão das garantias inerentes à reserva de lei e à reserva

[79] A título de exemplo, cf. o art. 3º II Lei 12.850, que apenas menciona a permissibilidade da medida interventiva talvez mais gravosa na sistemática processual brasileira sem qualquer regulação. Essa autorização é, por várias razões, inconstitucional.

[80] A terminologia empregada por *Cabette*. Interceptação telefônica, 2015, p.86, é reveladora: "seria *desejável* que houvesse *tratamento* legal, impondo os limites da proporcionalidade taxativa e expressamente, para quaisquer comunicações (telegráficas, correspondência epistolar ou de dados), *evitando* assim que a aplicação e determinação das situações de excepcional quebra de garantia *fiquem ao simples alvedrio* do juiz, gerando insegurança jurídica e desigualdade de tratamento em casos concretos por causa da lacuna legal." É imperioso esclarecer que, tendo os fundamentos que tem, a reserva de lei não trata, senão autoriza, e não com o fim de evitar que acabe o juiz tendo que fazer por ele mesmo, porque o que não está autorizado está ilícito. Cf. também Clever *Vasconcelos*. Interceptação telefônica, 2011, p. 60, que enxerga na norma do art. 5º XII CF já uma determinação para os procedimentos da escuta telefônica, quando, na verdade a referida norma simplesmente estabelece um direito fundamental que, em termos de dogmática constitucional, contém *reserva qualificada*. *Bitencourt/Busato*. Comentários à Lei de organização criminosa, 2014, p. 101; *Rorato Maciel*. Crime Organizado. Persecução Penal e política criminal, 2015, p. 173, 282; *Gomes Rodrigues da Silva*. Organizações criminosas e técnicas especiais de investigação, 2015, p. 413; *Araújo da Silva*. Organizações criminosas. Aspectos penais e processuais da Lei 12.850/2013, 2ª ed. 2015, p. 117 *Greco Filho*, Vicente. Comentários à Lei de organização criminosa, Lei 12.850/13, 2014, p. 35; *Greco Filho*, Vicente. Interceptação telefônica, 2015, p. 25 – embora já tenha defendido ser o sigilo a regra e a interceptação, a exceção, cf. *idem*. Interceptação telefônica, 1996, pp. 13 s.

parlamentar. Não é apenas a execução da medida interventiva o que deve ser regulamentado, é necessário saber também o que está autorizado enquanto medida.

É possível dizer, sem exagero, que um processo penal é um completo processamento de dados. Ele, por si só, é um conjunto organizado de informações necessárias para a descoberta da verdade sobre um fato pretérito. O trabalho dos órgãos de persecução penal é, majoritariamente, um tratamento de dados pessoais das mais variadas naturezas: levantamento de informações, armazenamento de documentos, gravação de audiências, publicação de decisões, acesso aos autos, expedição de ofícios, compartilhamento de provas, divulgação, eliminação, inutilização de dados pessoais, requisição de registros criminais etc. Ao longo do processo, dados pessoais não são apenas colhidos, mas também produzidos. O termo de indiciamento, a peça acusatória (denúncia ou queixa-crime), a sentença, os acórdãos etc. contêm, todos, alguns dados pessoais que o Estado, embora não levante, produz. Eles também estão protegidos pelo direito da personalidade, pelo menos, pela autodeterminação informacional. A forma na qual são utilizados, armazenados e compartilhados também é uma intervenção sempre carente de fundamento formal e material.

Isso justifica a impossibilidade de, nesta ocasião, dar tratamento completo a todas as formas de intervenção informacional no processo penal, que são muitas. Por isso, é necessário adotar uma outra estratégia metodológica, que consiste na apresentação de fundamentos e critérios gerais para as normas de levantamento, armazenamento, utilização e alteração de dados pessoais e, especialmente, dos sensíveis, dos sigilosos e dos *intocáveis* (ou melhor: daqueles absolutamente protegidos).

Antes, porém, é necessário apresentar, outra vez, algumas considerações gerais.

I. Considerações gerais

1. O princípio da publicidade do processo e a proteção da personalidade

Um aspecto inegligenciável da proteção de dados no processo penal está relacionado a um caro princípio do Estado de Democrático de Direito[81]: a publicidade dos *atos da audiência* (*Verhandlugunen des Gerichts*[82]). "Ela [a publicidade] se deixa reconduzir, historicamente, às demandas iluministas e liberais e deve ser entendida como reação aos juízos secretos e de gabinete"[83]. Também se encontra taxativamente estabelecida no art. 93 IX CF: "*todos os julgamentos dos órgãos do Poder Judiciário serão públicos* (...)".

[81] *Velten*, SK-StPO 5. ed. 2016, Vor § 169 GVG, nm. 1, nm. 8 ss.
[82] No direito alemão: § 169 GVG [Publicidade]: "O julgamento do juízo de conhecimento, incluindo a proclamação do veredito e das decisões, é pública. Não é a permitida a gravação sonora e de rádio-televisão, assim como a gravação de som e vídeo com finalidade de transmissão pública ou publicação de conteúdo.
[83] *Velten*, SK-StPO (nr. 81), Vor § 169 GVG, nm. 1.

Podendo ser restringida apenas "quando a defesa da intimidade ou o interesse social o exigirem" (art. 5º LX CF). Ou seja, ela não pode ser simplesmente eliminada sem fundamento ou sem compensação, pode, no entanto, também sofrer restrições. Bastaria para tanto – usando as palavras de *Velten* – que, em seu lugar, haja "um *equivalente funcional* que garanta, da mesma forma, um controle público".[84]

É impensável, contudo, que essa garantia institucional e individual seja compreendida na forma de uma publicidade ampla de todos os atos processuais, que afete a intimidade, a honra, o livre desenvolvimento da personalidade e, pelo menos por meio da execração pública, também a dignidade. Portanto, parece correto diferenciar entre processo e julgamento.[85]

"O julgamento não deve ser entendido como o conjunto de todos os atos orientados a uma decisão, mas apenas daqueles orientados à decisão de mérito (Sachentscheidung)"[86] e praticados em audiência: ocasião da produção de provas, do debate das partes e, de regra, do anúncio do veredito (arts. 400 ss., especialmente 403 *caput* e § 3º CPP; art. 81 Lei 9099/95). Por isso, a publicidade não deve valer para os atos processuais preparatórios ou mesmo autônomos, caso tenham apenas significado procedimental em relação ao processo principal:[87]

> *Essa clara limitação da lei harmoniza-se com a compreensão (pré-positiva) da máxima da publicidade, uma vez que, para sua principal função crítica, basta possibilitar a apreciação pública sobre se o fundamento do veredito sustenta a decisão judicial de mérito e se esse fundamento é completo*.

Baseado nesses argumentos, a publicidade, no processo penal, deveria abranger apenas a audiência de instrução e julgamento de todas as instâncias. Isso significa que, *em princípio*, nem o inquérito policial, nem as fases anteriores ou posteriores aos atos de audiência e prolação da sentença e nem os registros documentais do processo deveriam ser públicos. Tudo isso afeta sobremaneira a autodeterminação informacional. E o sigilo que, hoje, a legislação brasileira prevê de forma quase excepcional[88] para os *autos do processo* deveria ser a regra. Nem mesmo o art. 792 CPP fundamenta o contrário. Ele assegura a publicidade dos atos processuais praticados em dia e hora certa e na sede do tribunal – ou seja, com a presença de espectadores – como leilões, citação/intimação, assinatura do termo de suspensão condicional do processo (art. 89 Lei 9099/95) etc. Uma regra que visa garantir a publicidade das audiências não pode ser interpretada, em desfavor dos direitos fundamentais, para assegurar também a publicidade dos autos processuais.[89] Todo tratamento informacional pelo poder público representa uma intervenção "quando não há dados

[84] *Velten*, SK-StPO (nr. 81), Vor § 169 GVG, nm. 8.
[85] *Velten*, SK-StPO (nr. 81), Vor § 169 GVG, nm. 4.
[86] *Velten*, SK-StPO (nr. 81), Vor § 169 GVG, nm. 4.
[87] *Velten*, SK-StPO (nr. 81), Vor § 169 GVG, nm. 4.
[88] Cf. arts. 201 § 6º CPP, 189 CPC.
[89] Em sentido diverso, TRF3 MS-SP 2004.03.00.008540-9, j. em 17.8.2005.

irrelevantes", inclusive a permissão de acesso a informações a outras autoridades públicas ou mesmo a pessoas privadas (cf. E). O princípio visa garantir somente a *audiência*,[90] ou seja, a presença de espectadores (cf. art. 795 CPP). E que estes, consequentemente, possam servir de *multiplicadores*, o que garante também a anotação de conteúdos da audiência para serem usados como base informativa.[91] Com base no princípio da publicidade (ou da garantia de livre acesso à sala)[92] da audiência, não há fundamento para a publicidade dos autos do processo.

Trata-se, assim, de permitir *controle* público do julgamento. A transformação da audiência em *espetáculo* público não estaria, assim, garantida pelo princípio da publicidade da audiência que poderia onerar desnecessariamente o acusado, ainda inocente (cf. art. 792 § 1º CPP). Há clara diferença entre assistir e reproduzir digitalmente um ato processual. É necessário um fundamento para a eternização de acontecimentos em audiência na forma de dados (ou de franqueamento de acesso a peças escritas dos autos). Estes acontecimentos devem ser controlados pelo *testemunho*[93] dos presentes, mas, de regra,[94] não deveriam ser gravados ou reproduzidos sem fundamento legítimo. Isso evita efeitos estigmatizantes e satisfação do sentimento sensacionalista, mas também protege contra afetações à descoberta da verdade[95]. O processo penal é um ato de coação que implica a responsabilidade do Estado. Mesmo a liberdade de informação e de radiofusão, em princípio, não são afetadas pela compreensão de que a publicidade se restringe ao acesso público à sala de audiência, não garantindo a gravação visual e sonora:[96] porque deles não se extrai nenhum direito a revelação de alguma fonte informacional.[97]

A conformação de toda a sistemática dessa relação entre a proteção dos interesses públicos e individuais é, aqui, especialmente complexa e merecedora de profundas reflexões, para as quais esta via, definitivamente, não permite uma contribuição adequadamente fundamentada. Estão, em jogo, variados princípios, conceitos, regras de equilíbrio, regras de exceção, remédios jurídicos etc. E o caráter científico de um Parecer desautoriza a tomada de posição irrefletida. A sede própria para a resolução desse problema é, certamente, a da monografia. Ocorre, no entanto, que, sem essa compreensão, o restante das ideias a seguir pareceria – e justificadamente – incoerente. Isso fica claro com exemplos: qual é o sentido das regras para o compartilhamento de informações processuais com órgãos da segurança pública, quando, em princípio, os autos processuais são acessíveis a qualquer um; e, sendo assim, como ou para que proteger documentos do processo em sistemas informáticos dos tribunais?

---

[90] De maneira semelhante, *Velten*, SK-StPO (nr. 81), Vor § 169 GVG, nm. 12.
[91] *Velten*, SK-StPO (nr. 81), Vor § 169 GVG, nm. 9.
[92] Fala-se, em alemão, no princípio do acesso público à sala de audiência (Saalöffentlichkeit).
[93] *Velten*, SK-StPO (nr. 81), Vor § 169 GVG, nm. 7.
[94] Exceções podem ser pensadas, por exemplo, diante de um interesse público mais significativo, como a gravação para a reprodução mais fiel dos acontecimentos visuais e sonoros (cf., p.ex., § 169 II GVG).
[95] Cf. BVerfGE 119, 309, 324 s.; 103, 44, 64; 119, 309, 322; BVerfG NJW 20140, 3013, 3015; NJW 2009, 352.
[96] BVerGE 103, 44, que declarou a constitucionalidade do § 169 GVG (cf. nr. 82); sobre a discussão, cf. *Roxin* Strafprozessrecht und Medien, in: FS zum 30jährigen Bestehen der Münchner Juristischen Gesellschaft 1996, p. 97; *Huff* NJW 2001, 1622; *Zuck* NJW 2001, 1623; *Ernst* NJW 2001, 1624.
[97] *Velten*, SK-StPO (nr. 81), Vor § 169 GVG, nm. 37.

Com isso quer-se apenas esclarecer que o desenvolvimento restante das diretrizes para a conformação da proteção de dados no processo penal pressupõe a inexistência desse acesso público irrestrito a todos os atos (e autos) processuais, uma vez que é, em grande medida, incompatível com o direito de proteção de dados aqui desenvolvido.

2. A presunção de inocência e os níveis de suspeita do fato

Até o trânsito em julgado da condenação, todo acusado é considerado inocente. Por isso, o processo penal não pode estar associado à garantia de que apenas culpados sejam processados. Portanto, o que fundamenta que um indivíduo possa ser penalmente investigado/processado é o *grau de suspeita* que lhe recai.

Não por outra razão, é natural que também o nível das intervenções que o indivíduo deva suportar esteja em direta relação com esse grau de suspeita. O legislador brasileiro não está vinculado a uma categorização dogmática específica, mas aquela desenvolvida na dogmática processual penal alemã nos parece servir como boa direção. As normas do StPO diferenciam três tipos de suspeitas, para distintas fases e medidas processuais: a suspeita inicial, a suspeita forte e a suspeita suficiente.[98] "Enquanto a *suspeita forte* é afirmada nos casos em que, segundo o estado atual da investigação, haja grande probabilidade de que o imputado tenha praticado o crime, a *suspeita suficiente* é afirmada quando o imputado tem mais chance de, em vista das provas colhidas, ser condenado do que absolvido. (...) A suspeita suficiente é verificada sempre ao término dos procedimentos investigatórios, enquanto a suspeita forte se baseia no estado atual da investigação, que pode vir a ser alterado".[99]

É verdade que o legislador brasileiro também faz uso de distintas classes de *indícios* (art. 239 CPP): veementes (ex.: relacionado à origem do bem para a decretação de sequestro, art. 126 CPP), suficientes (ex.: relacionado à autoria e ao perigo para a decretação de prisão preventiva, art. 312 CPP; e para a pronúncia, art. 413 CPP) e simples (ex.: relacionado à autoria ou participação para o retorno dos autos ao Ministério Público, a fim de nova deliberação sobre a colaboração de terceiros para o fato, art. 417 CPP). No entanto, seria problemático apoiar-se em tal distinção que, em muitos aspectos, é assistemática. Por isso, manteremos a terminologia que nos parece mais apropriada. Isso viabilizará, nas passagens seguintes, indicar, à luz dos graus de suspeitas, os níveis de proteção que parecem adequados a cada intervenção informacional.

3. Formas de tratamento de dados no processo penal

[98] Cf. Hilgendorf/Valerius, Direito Penal: Parte Geral, São Paulo, 2018, p. 153, nota de tradutor (*Gleizer*).
[99] *Greco/Gleizer*, A infiltração online no processo penal – Notícia sobre a experiência alemã. RBDPP 5/3, 1483, p. 1499).

Pelas razões apresentadas acima, é importante distinguir as várias formas de tratamento de dados no processo penal, a fim de compatibilizá-las, segundo suas naturezas, com o regime de proteção do livre desenvolvimento da personalidade. Organizando-as em grandes blocos, seria possível ordená-las em três grupos que nos parecem carentes de maior atenção: medidas de investigação, acesso aos dados pessoais constantes dos autos processuais e aos externos a ele.

Não é possível, nessa oportunidade, apresentar diretrizes para todas essas formas de tratamento de dados no processo penal. Por isso, concentraremos nossa atenção nas medidas de investigação (II), tomando como exemplo o monitoramento das telecomunicações[100]. E, posteriormente, apresentaremos, de forma bem resumida, breves considerações a respeitos das demais (III).

II. Medidas de investigação na persecução penal

É possível enxergar as medidas de investigação do processo penal de uma perspectiva inerente ao processo, enquanto formas obtenção de prova (medidas cautelares).[101] No entanto, elas têm uma face, muitas vezes, negligenciada. Os direitos fundamentais, como está claro, têm aplicação imediata. Eles impõem barreiras verdadeiramente protetivas à esfera do indivíduo afetado por uma ação estatal. E isso não por meio de considerações meramente abstratas e principiológicas (melhor: programáticas), mas por instrumentário denso: um conjunto de critérios dogmáticos verificáveis em cada ato interventivo pelo Tribunal Constitucional em relação à lei e pelo juízo em relação à autorização da medida interventiva no processo penal do caso concreto. Portanto, de uma perspectiva externa ao processo, a busca e o levantamento de informações – ou seja, as medidas de investigação – representam sempre uma intervenção em direitos fundamentais. Esses direitos demarcam espaços em que o Estado, a princípio, não está autorizado a adentrar. Querendo fazê-lo, com a finalidade de exercer suas competências – por exemplo, a de construir uma sociedade justa (art. 3º I CF) –, ele precisará sempre de uma *justificação especial*.[102]

[100] Para a discussão a respeito de outras dessas medidas, cf. também *Gleizer,* Busca estatal por informações digitais e intervenções em direitos fundamentais no processo penal (parte I e II), Penal em Foco, Jota, 31.7.2019 (parte I) e 12.8.2019 (parte II), acessível em: https://www.jota.info/opiniao-e-analise/colunas/penal-em-foco/busca-estatal-por-informacoes-digitais-e-intervencoes-em-direitos-fundamentais-no-processo-penal-31072019.
[101] Mais detalhes em *Gleizer,* Busca estatal por informações digitais... (parte I), (nr. 100).
[102] Mais detalhes e referências em *Greco/Gleizer* RBDPP 5/3, 1483, pp. 1485 s.

Essa justificação se dá, grosso modo, por *três pressupostos* de relevância geral: norma autorizativa (cf. B III 1), não afetação do conteúdo essencial/de dignidade do direito e proporcionalidade.

No caso das intervenções informacionais, que afetam a garantia ao livre desenvolvimento da personalidade, o conteúdo essencial/de dignidade concretiza-se em um *núcleo da esfera privada*. No direito alemão, essa garantia é conformada por alguns direitos fundamentais específicos: como a autodeterminação informacional (de caráter residual/subsidiário), a inviolabilidade do domicílio, o sigilo das telecomunicações e a garantia de integridade e confiabilidade dos dispositivos informáticos. Todos eles visam garantir que o indivíduo possa confiar que, em circunstâncias normais, não esteja sendo vigiado e possa, assim, agir com a espontaneidade necessária para ser quem é ou quem deseja ser. O conteúdo essencial comum a todos eles é, portanto, o núcleo da esfera privada. Enquanto conteúdo essencial, ele é *intocável*, ou seja, nenhuma intervenção em seu âmbito pode ser justificada.[103]

O *núcleo da esfera privada* é um conceito que surge da *teoria das esferas* criada para o direito civil.[104] Essa ideia propõe a separação da esfera privada em três círculos concêntricos. O externo seria o da *esfera social* ou publica, que está sujeita a intervenções sem altos pressupostos de justificação, e seria afetado já por indagações sobre a vida social ou pública, como a profissão, ou pequenas pesquisas online sobre o que é público a respeito do investigado/acusado. O intermediário seria o da *esfera privada*, que exige maiores pressupostos de justificação e é afetado pela coleta de informações, por exemplo, sobre a rotina de uma pessoa, sobre suas compras e seu círculo de amigos. E, por fim, o círculo interno seria o núcleo da esfera privada, que, enquanto expressão da dignidade humana, não comportaria qualquer intervenção. O conteúdo desse núcleo é bastante controverso.[105] Em princípio, uma informação que tenha relação direta com crimes – por sua imanente relação social – não pertence a ele.[106] A proteção absoluta de diários também já foi negada, ao argumento de que quem faz uso da forma escrita renunciaria a um total controle sobre o conteúdo correspondente.[107] Já a gravação do solilóquio de um investigado foi reconhecida como violação desse núcleo.[108] Quanto à conversa com *advogados de defesa criminal*, fala-se em dupla proteção absoluta (tanto em razão do núcleo quanto por razões institucionais).[109] O BVerfG também reafirma, constantemente, a necessidade de garantia do núcleo em relação a medidas de observação;[110] e o legislador alemão também prevê legalmente essa garantia em muitas normas autorizativas de intervenção informacional no StPO. O legislador, em relação a medidas gravosas, como o monitoramento das telecomunicações, a escuta ambiental domiciliar e a infiltração online, proíbe a prática das medidas em circunstâncias nas quais essa proteção absoluta pode ser violada (§ 100d I StPO). Em algumas das medidas, que, a exemplo da infiltração online, se voltam a registros digitais – e, por

[103] BVerfGE 103, 21, 31 ss; 109, 279, 313 ss.; 112, 304, 318 ss.
[104] Mais a respeito em *Greco* (nr. 16), p. 34.
[105] Cf. *Kingreen/Poscher* (nr. 8), p. 446, com mais detalhes e referências.
[106] Havendo quem diga ser ela pertencente à história (*Greco* FS-Rogall, 2018, p. 504) ou tratar-se de "bem público" (*Sieber* CR 1995, 100, 111); cf. também BVerfGE 113, 348, 391; NJW 2007, 2753, 2754; BVerfG NJW 2009, 2431, 2436; BVerfG 26. Juni 2008, Az.: 2 BvR 219/08, nm. 19 ff.
[107] BVerfGE 80, 367.
[108] BGHSt 57, 71, 74 ss.
[109] *Wolter/Greco* SK-StPO 5. ed. 2016, § 100a nm. 56
[110] Cf. BVerfGE 6, 32, 41; 34, 238, 245; 80, 367, 373 s.; 109, 279, 313 ss.; 113, 348, 391; BVerfG NJW 2008, 822, 834 ss.

isso, permitem, controle mais direcionado da medida –, chega, além disso, também a exigir a utilização de meios técnicos para assegurar que essas informações não sejam levantadas (§ 100d III StPO).[111] Há, na lei, ainda, determinações expressas de eliminação imediata desses dados ou de submissão imediata à apreciação de um juiz (p.ex.: §§ 98b III, 100d III, 100e V 2, 100g IV, 100i II StPO). Informações do núcleo obtidas pelo emprego de certas medidas gravosas, além disso, não podem servir de prova (cf., p.ex., § 100d II StPO).

Quanto às exigências da proporcionalidade para o ato interventivo que analisamos nesta ocasião – a norma autorizativa de levantamento de dados – são feitas muitas concretizações, na forma de direitos, deveres, limites, prazos etc. As mais importantes aparecerão adiante.

Por último, é importante deixar claro que, diferentemente do processo penal alemão, tomado como exemplo neste parecer, o processo penal brasileiro é carente de autorização para muitas medidas de intervenção informacional importantes na atualidade. Pode-se citar algumas como exemplo: localização de pessoas ou objetos (*Fahndung*)[112], monitoramento de telecomunicação na fonte, captação de IMSI, análise de estrutura molecular de DNA, infiltração online etc. Enquanto não houver autorização específica para tais medidas, sua prática é, *de lege lata*, vedada – por violação da reserva de lei (cf. B III 1).[113] Por isso, para a resposta dessa parte de nossa Consulta, qual seja, da indicação de diretrizes para a proteção de dados no processo penal, é crucial demonstrar como são concretizados esses parâmetros/pressupostos e, posteriormente, como devem ser conformados no ato de confecção legislativa de tais normas, o que será demonstrado por meio de uma norma do StPO tomada como exemplo.

1. Critérios para regras especiais de autorização

a) Critérios formais

As regras especiais de autorização no processo penal devem estar submetidas a diferentes requisitos formais, a depender da natureza da medida.

Aqui também é importante considerar se a medida investigativa é realizada explicitamente, como no caso da coleta de depoimentos, da busca e apreensão ou da verificação de identidade. Nesse caso, pode-se vincular a licitude do ato à instrução sobre o direito de permanecer calado ou de não colaborar ativamente para a medida (a tolerância, contudo, é um dever imposto pela norma autorizativa) ou ao

[111] Cf. *Greco/Gleizer* RBDPP 5/3, 1483, pp. 1505 s.

[112] Não se trata aqui da busca física do art. 240 CPP, mas do uso de dados de diversas naturezas para a localização de alvos (pessoas ou objetos) procurados.

[113] Quanto aos efeitos para o valor probatório das informações obtidas por meio dessa violação, cf., por todos, *Greco* FS-Rogall, 2018, p. 485, pp. 502 ss., com mais referências.

esclarecimento sobre a razão da medida. Visto que a maioria das medidas de investigação não são explícitas, esses critérios têm, no entanto, pouca relevância.

Medidas ocultas reduzem as possibilidades de reação jurídica por parte do afetado, que, sem delas tomar conhecimento, a elas não se opõe.[114] Por isso, o controle judicial é sobremaneira importante para as medidas ocultas de investigação. A maior parte das medidas ocultas de investigação deve submeter-se à chamada *reserva de jurisdição* (cf., p.ex, §§ 98b, 100, 100e, 100f StPO).

b) Critérios materiais

Quanto aos critérios materiais das normas de autorização, também aparecem as figuras do bem protegido e do objeto pessoal da ação interventiva (o destinatário). A esses soma-se também a subsidiariedade e a gravidade no caso concreto. E aqui, como já dito, a *suspeita*, enquanto objeto material da ação interventiva, substitui o perigo (elemento das normas autorizativas da segurança pública).

O bem protegido pelas autorizações de medidas investigativas está sempre relacionado, nas normas do processo penal, ao crime investigado. Nesse âmbito, o Estado investiga com finalidade repressiva em busca de informações sobre um fato típico já ocorrido. Isso facilita a vinculação do valor do bem jurídico protegido, que autoriza a medida investigativa, por meio da referência direta a alguns crimes. Recorre-se, nesses casos, ao chamado *catálogo de crimes*, para cuja persecução seria possível fazer uso da medida. O legislador brasileiro também faz uso desse critério para a limitação de algumas medidas investigativas, mas, em muitos casos, traça, com eles, limites desproporcionais – a exemplo da interceptação telefônica (art. 2º III LIT), que está permitida para todos os crimes com pena de reclusão. Caso uma medida dessa gravidade, que afeta a confiabilidade do indivíduo no uso de meios de telecomunicação, seja permitida para a investigação de quase todos os crimes do ordenamento jurídico (inclusive o furto simples do art. 155 CP), é possível presumir que, em algum momento, todos terão, por alguma razão, interceptadas suas telecomunicações. Bastaria, para isso, telefonar para alguém que esteja sendo investigado. E, com esses critérios, é possível assumir que muitas pessoas, provavelmente do convívio de todos, podem ser, em algum momento, alvo dessas medidas. É esse o serviço que a proporcionalidade presta ao direito fundamental e, às normas autorizativas, a vinculação ao bem jurídico protegido: garantir que medidas investigativas sejam excepcionais e usadas apenas em relação a crimes para cujos interesses sociais de punição superam a garantia de privacidade de inocentes.

[114] Em língua portuguesa, cf. a monografia de *Ramalho*, Métodos ocultos de investigação criminal em ambiente digital, Coimbra, 2017, especialmente pp. 179 ss.

Os destinatários de medidas interventivas graves no processo penal são, em princípio, apenas os imputados/suspeitos. Os insuspeitos, com poucas exceções, não devem ter que tolerar medidas invasivas.[115]

Este conceito mais genérico, desenvolvido pela dogmática processual alemã, é importante para que algumas coisas façam sentido em relação às medidas investigativas. Ao imputado são conferidos alguns direitos que não se confere a qualquer pessoa que é chamada, por exemplo, pela polícia, a depor. O imputado tem o direito de se manter calado (§ 136 I 2 StPO) e não produzir provas contra si mesmo (art. 14 III g PIPDCP[116]), de consultar-se com seu defensor (§§ 137 I 1 StPO) e de ser informado sobre esses direitos (§ 136 I 2 StPO). Por isso, imputado é o status do sujeito passivo do processo penal em todas as fases, inclusive na investigação/no inquérito. Após o recebimento da denúncia, o imputado também é chamado de *réu/acusado* (§ 157 StPO). As medidas investigativas, no entanto, não fazem distinção entre fases processuais, e por isso se referem, na maior parte das vezes, sempre a imputados e não-imputados. Portanto, discute-se o momento em que uma pessoa deve passar a ser vista como imputada e, consequentemente, ser informada de seus direitos. Na ausência de definição legal, garante-se esse status à pessoa contra a qual se volta alguma medida dos órgãos de persecução penal que tenha por fim persegui-la em razão de um possível fato penal.[117]

Contudo, muitas medidas de intervenção informacional afetam, comumente, terceiros *não-imputados/insuspeitos*. Em relação aos terceiros a que se referem as normas autorizativas de intervenção informacional, a legislação usa algumas categorias: como a dos acompanhantes do imputado (§ 163e StPO), dos intermediários de mensagem (§ 100a III StPO) e dos disponibilizadores da conexão (§ 100a III StPO). Elas aparecem em algumas normas autorizativas e sempre com o sentido de excepcionar, em poucas hipóteses, a legitimidade de afetação da esfera jurídica dos insuspeitos. Isso significa que, quando a lei é silente, prevalece a absoluta ilegitimidade de uma intervenção informacional *dirigida* contra o insuspeito.

A subsidiariedade é a representação do que se conhece, na dogmática processual, por estado de necessidade probatório. A ideia não é, entre nós, desconhecida – cf., p.ex., art. 2º II e art. 8º-A I LIT. A forma como o legislador brasileiro conforma essas cláusulas – de maneira menos específica do que o alemão – não nos parece problemática. É perfeitamente possível que, por meio de redações simples como "a prova não puder ser feita por outros meios disponíveis e igualmente eficazes", a concretização dessa exigência seja deixada a cargo dos tribunais.

A gravidade no caso concreto, por sua vez, é idônea a permitir também ao juiz a ponderação, no caso em análise, entre a necessidade interventiva e a afetação da esfera individual. Dessa forma, não se encontra o juiz obrigado a deferir a medida apenas por estar a medida autorizada para a defesa de um específico bem jurídico.

Em relação ao nível de suspeita que deve recair sobre um imputado para a legitimidade de específicas medidas, a legislação alemã, também por exigências

[115] Sobre intervenções informacionais contra insuspeitos, cf. *Estellita/Gleizer,* A investigação penal de insuspeitos, Folha de São Paulo, 12.9.2020
[116] Pacto Internacional sobre Direitos Civis e Políticos – Decreto 592/1992.
[117] *Roxin/Schünemann* (nr. 25), § 25 nm. 11, com mais detalhes e outras referências.

jurisprudenciais, distingue entre suspeitas (p.ex.: § 81h StPO – pesquisa de sequência de DNA) e suspeitas fortes (p.ex.: § 100a StPO – monitoramento de telecomunicações).

A seguir, esses critérios formais e materiais serão demonstrados com base em uma medida investigativa autorizada no StPO. Ela não foi escolhida aleatoriamente. Antes, representa uma intervenção, por um lado, gravosa e, por outro, comum também ao processo penal brasileiro. Por fim, apresentaremos a tradução de sua correspondente norma autorizativa, a fim de que a abstração possa, finalmente, ganhar traços mais concretos.

2. Um exemplo de norma de autorização: o monitoramento de telecomunicações

O StPO autoriza e regula o monitoramento e a gravação de telecomunicações (§ 100a StPO). Sua nomenclatura não é acidental e, além de indiciar uma orientação a um objeto de intervenção mais amplo ("telecomunicações") do que a de sua correspondente brasileiro ("comunicações telefônicas", art. 2º LIT), a norma ainda autoriza, com mais precisão, o *monitoramento* e a *gravação* da telecomunicação. Não é autorizada aqui a ação, que entre nós causa tanta divergência, de *interceptação*. Com isso, evita-se a inconveniente e improfícua discussão a respeito de se a ação autorizada é apenas aquela que, ao capturar, retém mensagem destinada a terceiro, impedindo que este dela tome conhecimento. Tendo em vista o objetivo da medida, é evidente que o legislador brasileiro também não optou, conscientemente, por essa alternativa extremamente restritiva da intervenção, ainda que tenha sido infeliz na maneira de se expressar.

A medida está autorizada no ordenamento jurídico alemão desde 1968 e, desde então, os avanços tecnológicos e as exigências investigativas mudaram de forma tão severa, que a norma já foi objeto de, praticamente 40 alterações legislativas. Com isso, o § 100a é, de todo o StPO, o dispositivo que mais sofreu modificações.[118] Em sua grande maioria, essas modificações serviram apenas para alterar/incrementar seu catálogo de fatos. Mas, recentemente, a norma foi objeto de uma autêntica reforma.[119] A reforma consistiu, principalmente, em dar autorização para uma específica medida cuja legalidade era há muito tempo controversa: *o monitoramento de telecomunicação na fonte* (TKÜ-Überwachung). Isso foi necessário – e serve como um bom exemplo do rigor de uma garantia de reserva de lei consequente – porque alguns métodos de telecomunicação por softwares que garantem criptografia (como o Skype) por meio de sistema VoIP (*voice over IP*) exigiam uma medida adicional, a infiltração de sistemas informáticos. Por isso, o legislador alemão precisou criar uma autorização específica para essa medida (§ 100a I 3 StPO), já que a analogia é, em regra, vedada pelo imperativo de clareza e determinação, fundamentado nos princípios da reserva de lei e parlamentar.

[118] *Bär*, TK-Überwachung, 2010, p.. 43 nm. 19.
[119] Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17.08.2017 BGBl. I S. 3202.

Telecomunicação é definida, no direito alemão, como "processo técnico de envio, transferência e recebimento de sinais por meio de dispositivos de telecomunicação" (§ 3 nr. 22 TKG). Estão incluídos, nesse conceito abrangente, todo tipo de transferência de mensagens por dispositivos de telecomunicação, ou seja, inclusive *paging*, SMS, e-mails, chats e telefonia por internet.[120]

A telecomunicação pressupõe a participação de, pelo menos, duas pessoas naturais, uma vez que o vocábulo comunicar (do latim, *communicare*) denota tornar uma informação comum (a alguém).[121]

Duas espécies de dados surgem com o início do processo de telecomunicação: dados de conteúdo e dados de tráfego.

> "*Dados de conteúdo* são as próprias informações transmitidas durante o processo de telecomunicação. Já *dados de tráfego* (ou metadados) são as informações produzidas, processadas ou utilizadas em razão da prestação do serviço de telecomunicação. Dados de tráfego são, por exemplo, a data e o local do início e término da conexão, informações sobre o serviço de telefonia usado, o local de envio e de destino da informação, o horário, os interlocutores e a quantidade das mensagens, a duração e as eventuais tentativas de estabelecimento de uma chamada telefônica, a natureza do processo de telecomunicação empregado (se auditivo ou visual) etc.; especificamente quanto ao uso de telefonia móvel, são exemplos os registros da ERB (Estação Rádio Base) com a qual o aparelho se comunicou para a conexão (mesmo em modo de espera), que revelam sua localização ou posição geográfica por meio de técnicas de triangulação; e, na comunicação pela internet, destacam-se, por exemplo, o *endereço de IP dinâmico*, a data e horário da comunicação e o acesso a uma aplicação. Ou seja, metadados são as informações técnicas do processo comunicativo por meio do qual o conteúdo é trocado à distância entre os participantes e que revelam, portanto, informações específicas sobre a (tentativa de) comunicação entre duas pessoas. Esses são, portanto, os elementos básicos de toda telecomunicação. É preciso esclarecer que dados de tráfego pressupõem ao menos uma tentativa de telecomunicação por parte dos usuários – critério importante para resolução de conhecidos problemas, como da chamada SMS silenciosa [*stille SMS*], do IMSI-Catcher (§ 100i StPO), do rascunho de *e-mail* ou do *e-mail* enviado a si mesmo, de conteúdos solipsistas, de gravações de voz no dispositivo digital, de solilóquios, de captação de diálogos de fundo, dentre outros."[122]

Essa autorização, portanto, corporifica uma intervenção no específico direito fundamental ao sigilo das comunicações à distância (Art. 10 GG), que protege, em primeira linha, a confiança no uso de determinados meios de telecomunicação e, com isso, é uma garantia ao livre desenvolvimento da personalidade. A ideia aqui é a seguinte: o direito ao sigilo da telecomunicações visa a reduzir os maiores riscos provenientes da distância existente entre os comunicantes, porque o lançamento de informações de um ponto a outro, diferentemente de uma comunicação presencial, implica uma menor capacidade do indivíduo de controlar o acesso indesejado ao conteúdo de suas informações. A proteção que se pode exercer contra a tomada de conhecimento das informações trocadas em uma comunicação presencial reduz-se à

[120] *Roxin/Schünemann* (nr. 25), § 36 nr. 3.
[121] *Gleizer* REC 19/79, p. 211, p. 215, com outras referências; uma demonstração mais detalhada das razões em *Heinrich* ZIS 15-9, p. 421-430, 2020.
[122] *Gleizer* REC 19/79, p. 211, pp. 214 s.

medida em que são incluídos meios técnicos para a transmissão das informações. Sem o conhecimento dos interlocutores, estes meios técnicos podem sofrer monitoramento.

Dessa forma, qualquer tratamento que se dê aos dados levantados por meio dessa medida será sempre uma nova intervenção neste direito específico, e não naquele mais amplo da autonomia informacional.[123] O sentido da realização dessa proteção jurídica contra intervenções estatais por meio de um ou de outro direito está no fato de que cada um deles possui particulares exigências justificadoras (principalmente na categoria dogmática da proporcionalidade). E isso tem *importância fundamental para toda a dogmática das intervenções informacionais*. Pois as regras de armazenamento, utilização e alteração de dados precisam levar em conta o direito afetado no levantamento.

Mas, concentrando-se na medida de levantamento, fica mais fácil compreender essas exigências justificadoras (sobretudo, o catálogo de fatos, a gravidade no caso concreto, a subsidiariedade, os possíveis afetados, a proteção do núcleo da esfera privada) voltando-se ao dispositivo em si:

> **§ 100a Monitoramento de telecomunicação**
> (1) Sem o conhecimento do afetado [ocultamente], pode-se, monitorar e gravar a telecomunicação, caso
> 1. fatos determinados fundamentem a suspeita de que alguém consumou ou, caso a tentativa seja punível, tentou consumar como autor ou partícipe ou, por meio de um crime, preparou um **crime grave**, listado no rol da Abs.2,
> 2. o crime seja especialmente grave **também no caso concreto** e
> 3. a investigação dos fatos ou do local onde se encontra o imputado fosse, de outro modo, consideravelmente **mais difícil ou infrutífera**.
> O monitoramento e gravação da telecomunicação também pode ocorrer por meio de intervenção, com meios técnicos, em sistema informático utilizado pelo imputado, caso isso seja necessário, para possibilitar o monitoramento e gravação, especialmente, em forma descriptografada. Os conteúdos e as informações da comunicação armazenados no sistema informático do imputado só podem ser monitorados e gravados, caso eles, durante o processo de telecomunicação, também pudessem ter sido monitorados e gravados, em forma criptografada, em rede de telecomunicação pública.
> (2) **Crimes graves** no sentido da Abs. 1 nr. 1 são:
> 1. do Código Penal:
> a) crimes de alta traição e de perigo para o estado democrático de direito... b) corrupção ativa ou passiva de mandatório da federação ou dos estados... c) crimes contra a defesa nacional... d) crimes contra a ordem pública... e) falsificação de moedas... f) crimes contra a autonomia sexual... g) pornografia infantil... h) homicídio e homicídio qualificado... i) crimes contra a liberdade pessoal (tráfico de pessoas... prostituição compulsória... escravidão...) j) furto em bando... k) roubo e extorsão... l) crimes de receptação... m) lavagem de dinheiro... n) estelionato e estelionato informático... o) estelionato de subvenção... p) estelionato de apostas esportivas... q) apropriação indébita trabalhista ou previdenciária... r) crimes de falsificação documental... s) bancarrota... t) crimes contra a concorrência... u) crimes de perigo comum... v) corrupção ativa e passiva...
> 2. do Código Tributário: a) sonegação fiscal… b) contrabando… c) receptação tributária…
> 3. da lei antidoping... 4. da lei de asilo 5. da lei de migração... 6. da lei de economia externa... 7. da lei de drogas... 8. da lei de insumos de drogas... 9. da lei de controle de armas de guerra... 9a. da lei de novos psicotrópicos... 10. do Código de Direito Penal Internacional... 11. da lei de armas...

[123] *Puschke/Weßlau* SK-StPO § 479 StPO, nm. 21 ss.

(3) A medida só pode ser autorizada contra o **imputado** ou contra pessoas sobre as quais assumir, em razão de fatos concretos, que **intermediam mensagens** para o imputado ou que lhe **disponibilizam conexões ou sistemas informáticos**.
(4) Em razão da autorização, todos que operam o serviço de telecomunicação ou contribuem para sua operação estão obrigados a possibilitar, ao juízo, à promotoria ou seus agentes de investigação em serviço policial, a medida e a fornecer, imediatamente, as informações necessárias para ela. Devem ser atendidas as determinações da Lei de Telecomunicações e do Regulamento Geral de Monitoramento de Telecomunicações a respeito de se e em que medida devem ser adotadas precauções. Aplica-se, no que couber, o § 95 Abs. 2.
(5) Em relação às medidas das Abs. 1 e 2, deve-se assegurar tecnicamente que
1. possam ser monitoradas e gravadas, exclusivamente:
a) a telecomunicação em curso (Abs. 1 S. 2), ou
b) conteúdo e circunstâncias da comunicação que, do momento da autorização segundo o § 100e Abs. 1 em diante, também possam ser monitoradas e gravadas durante o processo de transferência em curso em rede de telecomunicação pública (Abs. 1 S. 3)
2. só sejam realizadas alterações nos sistemas informáticos que sejam indispensáveis para o levantamento dos dados e
3. as alterações realizadas, desde que tecnicamente possível, sejam desfeitas automaticamente assim que encerrada a medida.
O meio empregado deve ser protegido, segundo os padrões técnicos, contra usos desautorizados. Dados copiados devem ser protegidos, segundo os padrões técnicos, contra alterações, eliminações e tomada de conhecimento desautorizados.
(6) Em toda ocasião em que se empregue a medida, é imperativo o registro
1. da qualificação do meio técnico empregado e do momento de sua utilização,
2. de informações para a identificação do sistema informático e das alterações realizadas que não sejam simplesmente transitórias,
3. de informações que possibilitem a determinação dos dados levantados, e
4. do departamento que executa a medida.

§ 100d StPO:
(1) As medidas dos §§ 100a a 100c são inadmissíveis caso seja possível assumir, com base em elementos fáticos, que suas execuções venham a obter apenas informações relativas ao núcleo da esfera privada.
(2) Informações do **núcleo da esfera privada**, obtidas por meio das medidas dos §§ 100a a 100c, **não podem ser valoradas** no processo. Registros de tais informações devem ser **imediatamente eliminados**. O fato de terem sido obtidas e eliminadas deve ser documentado.
(3)... (4) …
§ 101 – Regras procedimentais relativas a medidas ocultas
... (8) Os dados pessoais, obtidos por meio das medidas, que não sejam mais necessários para a persecução penal ou para uma eventual verificação judicial devem ser **imediatamente eliminados**. Desde que os dados sejam mantidos apenas para uma eventual verificação judicial, eles podem ser utilizados sem o consentimento do afetado apenas para esse propósito;
eles devem ser bloqueados.

III. Demais formas de tratamento de dados pessoais no processo penal

Além das medidas de investigação, há outras formas de tratamento de dados pessoais no processo penal carentes de autorização, que podem ser divididas, grosso modo, em

dois blocos: franqueamento[124] de acesso a dados pessoais a) constantes dos autos do processo e b) externos aos autos do processo. O compartilhamento de informações dos autos entre órgãos de segurança pública e de persecução penal é questão que merecerá um tópico próprio (cf. F).

a) Dados constantes dos autos do processo

Tendo em conta o fato de que, em princípio, o acesso aos autos de qualquer processo penal deve ser excepcional (porque a regra é a proteção de qualquer informação pessoal), o processo penal brasileiro merece uma ampla reforma. Aqui é necessário ponderar a estrita necessidade de franquear acesso aos autos a pessoas interessadas no processo (sobretudo as partes) com a garantia de que o indivíduo ainda inocente seja preservado contra exposições desnecessárias. O interesse público em casos excepcionais (como, p.ex., de funcionários públicos, de casos socialmente relevantes ou de políticos) também deve ser ponderado pelo legislador.

b) Dados externos aos autos do processo

Por fim, também é necessário que haja autorizações legais expressas para acessos de terceiros a dados externos aos do processo, por exemplo, àqueles constantes dos sites dos tribunais que apresentam andamentos dos autos ou aos armazenados em bancos de dados após extrações de informações obtidas ao longo do processo (p.ex., os registros criminais). Ao que nos parece, informações pessoais não devem ser disponibilizadas a um amplo acesso público nestes bancos de dados. Se até mesmo o compartilhamento de informações sobre a existência de uma demanda cível já é uma intervenção na autodeterminação informacional; o que dizer de uma criminal. Essas questões podem parecer menos importantes, mas não são. Em primeiro lugar, a premissa assumida no direito de proteção de dados é a de que não há dados irrelevantes. Além disso, o tratamento posterior dos dados colhidos por meio de medidas de investigação deve ser calculado segundo o específico direito afetado no levantamento.

[124] Optou-se aqui pelo termo franqueamento de acesso, a fim de que se torne claro do que se trata. No entanto, o franqueamento de acesso é, de uma perspectiva jurídica, um ato de compartilhamento de informações, ainda que (do Estado) com particulares.

F. O compartilhamento de dados entre órgãos de segurança pública e persecução penal

I. Licitude formal: o modelo das duas portas

Todas as considerações feitas até aqui são desenvolvidas a partir de um único fio condutor: cada uma das formas de tratamento de dados pessoais por órgãos de segurança pública e persecução penal demanda autorização em lei e tem sua legitimidade avaliada separadamente em face da natureza de cada uma destas atividades estatais. Por conseguinte, deve haver normas de um direito de segurança pública que autorizem respectivamente levantamento, armazenamento, alteração e utilização, assim como devem fazê-lo também as normas atinentes ao processo penal. Com base nesses pressupostos, o compartilhamento de dados revela-se especialmente problemático, pois ele, por sua própria natureza, extravasa um âmbito de atuação específico. Dados pessoais são transferidos de um órgão para outro, que lhes atribuem uma finalidade distinta daquela pela qual os dados foram levantados e armazenados. Isso gera algumas peculiaridades, que têm de ser consideradas na hora de conceber normas de autorização para o compartilhamento.

Uma dessas peculiaridades consiste em um problema normativo-material (e, possivelmente, de competência legislativa[125]) das normas de compartilhamento. Normas que autorizam o compartilhamento são normas relativas à atividade do órgão que compartilha os dados (controlador primário) ou elas dizem respeito à atividade do órgão que os recebe (controlador secundário)? Por exemplo, se a polícia compartilha imagens produzidas por câmeras de vigilância com o Ministério Público, para que sirvam como prova em um processo criminal, as normas que regram o compartilhamento seriam normas de um direito de segurança pública ou do processo penal? Esse problema tem sido bastante discutido na doutrina estrangeira, com bons argumentos para ambas as respostas possíveis.[126]

A opinião majoritária na discussão alemã enxerga no denominado *modelo das duas portas* a melhor solução para o problema.[127] Segundo esse modelo, o compartilhamento

[125] Por exemplo, se se considera que os Estados, e não a União, têm competência exclusiva para legislar em matéria de segurança pública. Como exposto acima, não se pode afirmar com clareza a quem compete no Brasil legislar sobre essa matéria. Na prática, há tanto leis federais quanto estaduais dispondo sobre segurança pública. Assim, p.ex., a Lei 15.518/04 do Estado de São Paulo, que dispõe sobre a instalação de câmeras de vigilância, ao passo que medidas de identificação criminal são objeto da Lei Federal 12.037/09.

[126] Para um resumo da discussão, com mais referências, ver *Weßlau/Puschke*, SK-StPO 5. ed. 2020, Vor § 474 nm. 17.

[127] A respeito, cf. *Gleizer*. A proteção por duas portas nas intervenções informacionais. REC 19/79, p. 211-230, 2020, sobre decisão do BVerfG que estabelece o modelo das duas portas no compartilhamento de dados entre o Estado e empresas telefônicas.

de dados pessoais pressupõe um duplo fundamento legal. Seria necessário, em primeiro lugar, uma norma que autorize o controlador primário, aquele que primeiro levantou e armazenou, a dar acesso aos dados. Além disso, exige-se também do controlador secundário, ou seja, do órgão que receberá os dados, uma autorização para tanto. Somente se presentes ambos os fundamentos autorizados – metaforicamente, somente se abertas ambas as portas -, seria possível um compartilhamento de dados pessoais.

Do ponto de vista dos direitos fundamentais, parece ser essa de fato a solução mais consequente. Afinal, o compartilhamento de dados envolve duas intervenções distintas, que demandam, cada uma por si, um fundamento formal próprio. A primeira intervenção, realizada pelo órgão que dá acesso aos dados, consiste na mudança da finalidade que determinou o levantamento dos dados. Atribui-se-lhes uma nova finalidade, diferente da original, o que representa uma quebra do princípio da vinculação à finalidade. Embora tal quebra seja possível, ela exige fundamento legal próprio, pois consiste em nova intervenção. Essa autorização legal tem de especificar, pelo menos, a extensão dos dados compartilhados e as novas finalidades em relação às quais esse compartilhamento é aceitável. Com isso, compreende-se a razão para existência da primeira porta. A segunda porta diz respeito ao armazenamento e utilização dos dados pelo controlador secundário. É necessário um fundamento legal próprio que especifique as condições de tratamento dos dados e assegure standards de proteção, em especial, deveres de controle e eliminação.

Se ambos os controladores estão submetidos a regimes jurídicos de competência de um único ente (p. ex. se segurança pública e processo penal são de competência da União), é aceitável, para evitar repetições desnecessárias, que ambas as "portas" estejam previstas em único dispositivo. Este tem, contudo, de autorizar e regular com clareza ambos os atos que compõem o compartilhamento.[128]

II. Licitude material: a vinculação ao fim e o critério do levantamento hipotético

O modelo das duas portas, contudo, não garante por si só uma proteção adequada dos direitos informacionais. É necessário complementá-lo com requisitos materiais para a produção das normas de autorização em questão. Para seguir com a metáfora, tampouco se poderia falar em proteção adequada, caso as duas portas, embora existam, sejam compostas de papel. Há, portanto, alguns requisitos materiais que as normas autorizadoras do compartilhamento têm de satisfazer.

[128] Nesse sentido, também *Bäcker* (nr. 65), p. 482.

O princípio material por detrás das normas de compartilhamento de dados consiste na *diferenciação de acordo com a proximidade* entre finalidade do levantamento e a nova finalidade perseguida com o compartilhamento. Aqui o princípio da vinculação finalística revela, mais uma vez, sua importância fundamental. O tratamento autorizado dos dados está restrito à finalidade que determinou seu levantamento. Toda mudança de finalidade representa uma nova intervenção nos direitos informacionais, e essa intervenção é tanto mais gravosa, quanto díspares forem a finalidade original e a finalidade que determina o compartilhamento. E, por conseguinte, as exigências a que deve estar submetido o compartilhamento serão tanto mais rigorosas quanto maior for a disparidade desses fins.

Uma concretização desse princípio fundamental é discutida na doutrina estrangeira sob a denominação de alternativa hipotética de intervenção (*hypothetischer Ersatzeingriff*).[129] Esse critério material surge da necessidade de evitar que o compartilhamento sirva como subterfúgio para ter acesso a dados nos casos em que um órgão não está autorizado a realizar determinadas medidas de levantamento. Chega-se, portanto, à seguinte exigência: o compartilhamento é possível se o órgão que recebe os dados contar com autorização semelhante para levantá-los. Em outros termos, somente pode ser favorecido por um compartilhamento aquele que tivesse autorização legal para, ele mesmo, levantar os dados que estão sendo compartilhados.

O critério do levantamento hipotético permite submeter o compartilhamento não só à existência de uma autorização hipotética para levantar os dados, mas também que o controlador secundário estivesse autorizado a empregar *meios* tão gravosos quanto os que foram utilizados para levantar os dados pelo controlador primário. Portanto, o critério não implica apenas que o órgão recebedor pudesse, de alguma forma, levantar os dados, mas que ele pudesse levantar os dados com medidas com nível de intensidade semelhante ao daquelas efetivamente utilizadas pera levantar os dados. Assim, sobretudo em se tratando de medidas ocultas de levantamento de dados (observações duradouras, agentes infiltrados, interceptações telefônicas, infiltrações online etc.), o compartilhamento deve estar submetido à existência de autorização para se utilizar de meios com intensidade interventiva comparável aos utilizados para levantar os dados em questão.[130]

[129] Cf. BVerGE 100, 313 (389); BVerfGE 109, 279 (377); BVerfG NJW 2016, 1781 (1801); *Weßlau/Puschke*, SK-StPO 5. ed. 2020, Vor § 474 nm. 8; *Singelnstein*, MüKo-StPO 1. ed. 2019 nm. 27. Com críticas e oferecendo um modelo alternativo de regulação, *Bäcker* (nr. 65), p. 486 ss.
[130] Assim, ver, especialmente, BVerfG NJW 2016, 1781 (1802).

Síntese e Parecer

Assumidas as premissas delineadas ao longo deste documento, podem estes signatários sintetizar as seguintes ideias:

a) o reconhecimento da autodeterminação informacional (arts. 1º e 2º LGDP) enquanto direito fundamental impõe um *dever de abstenção geral do Estado em relação a todo e qualquer dado pessoal*;

b) a autodeterminação informacional soma-se aos outros direitos que protegem o livre desenvolvimento da personalidade. Por isso, tem por fim, obstando acesso estatal desarrazoado e desproporcional a dados pessoais, repelir sensação social de vigilância, de modo a proteger as condições sociais caras à espontaneidade humana, fundamental para que o indivíduo possa determinar, ele mesmo, quem e como quer ser;

c) o livre desenvolvimento da personalidade e seus corolários operam a proteção contra esse acesso estatal irrestrito a dados pessoais por meio das exigências das reservas de lei e parlamentar e da proporcionalidade. Enquanto direitos de *aplicação imediata* (art. 5 § 1º CF), está o Estado brasileiro categoricamente impedido de operar qualquer tratamento de dados pessoais senão em virtude de lei (art. 5º II CF).

Portanto, como nos **parece**:

a principal diretiva que devemos anunciar à *Data Privacy Brasil* a respeito da regulação da proteção de dados pessoais nas atividades brasileiras de segurança pública e persecução penal, de modo que seja possível garantir reais condições sociais para a autodeterminação informacional e o livre desenvolvimento da personalidade humana, é a defesa intransigente da reserva de lei e parlamentar, que demandará a tarefa de revisão completa das legislações aplicadas aos setores. Para o cumprimento dessa tarefa, esperamos ter contribuído com as demais diretivas regulatórias enunciadas anteriormente.

Honrados pela Consulta, desejamos à equipe Data Privacy Brasil sucesso em seus diligentes esforços pela garantia das condições necessárias e suficientes para o livre desenvolvimento humano no território brasileiro.

Berlim/Halle (Saale)/Salvador, 1° de novembro de 2020.



Eduardo Viana Lucas Montenegro Orlandino Gleizer

Subscritores:

Eduardo Viana (OAB/BA 18.281) é consultor, professor adjunto de Direito Penal da Universidade Federal da Bahia (UFBa) e da Universidade Estadual de Santa Cruz (UESC), doutor e mestre em Direito Penal pela Universidade do Estado do Rio de Janeiro (UERJ), tendo realizado todo o período de pesquisa doutoral na Universidade de Augsburg (Alemanha) e na Universidade Pompeu Fabra (Barcelona, Espanha);

Lucas Montenegro (OAB/CE 44.334) é consultor, assistente científico na cátedra do Prof. Dr. Joachim Renzikowski na Universidade Martinho Lutero, de Halle e Wittenberg, doutorando em Ciência do Direito pela Universidade Humboldt de Berlim e LL.M. pela Universidade Georg August de Göttingen (Alemanha);

Orlandino Gleizer (OAB/RJ 175.710) é consultor, assistente científico na cátedra do Prof. Dr. Dr. Eric Hilgendorf na Universidade Julius Maximiliam de Würzburg, doutorando em Ciência do Direito pela Universidade Humboldt de Berlim, LL.M pela Universidade de Augsburg (Alemanha) e mestre em Direito Penal pela Universidade do Estado do Rio de Janeiro (UERJ).