ENCCLA 2021

Ação 04/2021

Nota Técnica contendo a avaliação, propostas de alterações, contrastando o texto do anteprojeto com Convenções, recomendações e melhores práticas internacionais, em relação ao Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal – LGPD-Penal

1. Introdução

Em 18 de setembro de 2020, entrou em vigor a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais, a LGPD), que disciplinou o uso, a proteção e a transferência de dados de pessoais no Brasil.

Conforme disposto em seu artigo 4º, inciso III, a LGPD não se se aplica ao tratamentode dados pessoais realizado para fins exclusivos de: a) segurança pública; b) defesa nacional;
c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais. O parágrafo 1º do mesmo dispositivo prevê que nesses casos o tratamento de dados pessoais será regido por legislação específica.

A partir disso, foi instituída Comissão de Juristas, por Ato do Presidente da Câmara dos Deputados, em 26 de novembro de 2019, com a finalidade de elaborar anteprojeto que disciplinasse o tratamento de dados pessoais no âmbito da segurança pública e de atividades de investigação e repressão de infrações penais.

O anteprojeto da chamada "LGPD Penal" foi apresentado pela mencionada Comissão de Juristas em 5 de novembro de 2020. Em sua exposição de motivos, declara-se que a proposta legislativa pretende oferecer balizas e parâmetros que garantam um equilíbrio entrea proteção do titular contra a violação de seus direitos individuais e o tratamento de dados pessoais no âmbito de atividades de segurança pública e de persecução criminal.

Conforme apontado pela Comissão de Juristas, o texto do anteprojeto foi fortemente inspirado pela Diretiva 2016/680, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, que regula o tratamento de dados pessoais para fins de segurança pública e persecução penal no âmbito da União Europeia.

No entanto, em que pesem as contribuições que podem ser extraídas do normativo europeu, o comando legislativo que decorre do anteprojeto em estudo está em absoluto descompasso com a imprescindível integração entre os órgãos envolvidos, direta ou indiretamente, na investigação criminal, repressão penal e/ou segurança pública.

Em verdade, o anteprojeto poderá causar graves entraves ao exercício das funções institucionais dos órgãos e instituições competentes para as atividades de persecução penal e de segurança pública, impedindo sua atuação a fim de garantir a ordem pública.

Assim, a partir da análise dos capítulos dispostos pelo anteprojeto de lei, pretende-se demonstrar que seu texto apresenta não só grandes inconsistências, mas também carece de inúmeros reparos para que não venha a funcionar como uma barreira às atividades desegurança pública e persecução penal.

2. Capítulo I – Disposições Preliminares

Em seu Capítulo I, o anteprojeto de Lei Geral de Proteção de Dados Penal define seu objeto e seu âmbito de aplicação. Ao tratar deste primeiro aspecto, a proposta fixa o objetoem "tratamento de dados pessoais realizado por autoridades competentes para atividades de segurança pública e de persecução penal", vinculando-o, ato contínuo, à tutela dos "direitos fundamentais de liberdade e de privacidade e ao livre desenvolvimento da personalidade da pessoa natural", sendo, portanto, este o explícito direito tutelado pela Lei, de modo perfeitamente simétrico com o que dispõe o art. 1º da Lei nº 13.709, de 2018 (LGPD).

Impende recordar que referido anteprojeto pretende regular o tratamento de dados não regulado pela LGPD, que excetua, às alíneas 'a' e 'd' do inciso III, do art. 4º, o tratamento de dados realizado para tais finalidades.

Em que pese a referida simetria possa refletir coesão do sistema jurídico de tutela da privacidade, o regramento distinto expressamente dispensado pelo legislador a tais formas de tratamento de dados deve conformar limites claros ao exercício de referido direito. Nesse sentido, mostra-se consensual a necessidade de que, ao referir o objeto regulado e os direitos tutelados, evidencie-se a necessidade de resguardar o interesse público no compartilhamento de dados entre autoridades estatais legalmente incumbidas das atividades de segurança pública, investigação e repressão de infrações penais e pessoas jurídicas de direito privado, legalmente obrigadas a tal compartilhamento.

A partir disso, o recomendável seria que o artigo 1º apresente, de modo claro e sistemático, a relação entre referido anteprojeto, o microssistema jurídico de proteção de dados estabelecido pela LGPD e os dois objetos de tutela (não apenas a privacidade), conforme redação sugerida abaixo:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais realizado por autoridades competentes para atividades de segurança pública, de investigação e de repressão de infrações penais, previstas nas alíneas "a" e "d" do inciso III do artigo 4º da lei 13.709/2018, com o objetivo de:
> I - proteger os direitos fundamentais de segurança, liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural; e
> II-assegurar o compartilhamento de dados de modo a garantir a eficiência da atuação dos órgãos incumbidos das atividades mencionadas no caput deste artigo, seja por autoridades estatais legalmente incumbidas de tais atividades, seja por pessoas jurídicasde direito privado, legalmente obrigadas a tal compartilhamento, em procedimento sob tutela de pessoa jurídica de direito público.

A preocupação relacionada à existência de mecanismos que permitam a harmonizaçãoentre os direitos de privacidade e os meios de garantia da segurança pública e da persecução penal estende-se às sugestões de ajuste nos demais dispositivos do capítulo. Em seu art. 2º, o anteprojeto apresenta os fundamentos da proteção de dados pessoais no âmbito de sua aplicação adicionando explicitamente, ao que já dispõe o art. 2º da LGPD, os seguintes fundamentos: (i) a dignidade da pessoa humana; (ii) a presunção de inocência; (iii) a confidencialidade e integridade dos sistemas informáticos pessoais[1]; e (iv) a garantia do devido processo legal, da ampla defesa, do contraditório, da motivação e da reserva legal.

Relativamente ao direito de autodeterminação informativa, pilar do direito à proteção de dados pessoais, este é visto como fundamento necessário, porém cuja avaliação deve ser realizada em conjunto com outros fundamentos que desaconselhem a uma leitura absoluta de referido direito. Nesse sentido, propõe-se

[1] Considera-se que a redação deste dispositivo (art. 2º, V) não logrou obter a clareza necessária quanto ao seu objeto, assim, propõe-se o seguinte texto alternativo "V- disponibilidade, integridade, confidencialidade eautenticidade dos ativos informacionais".

a inclusão de fundamentos adicionais, dentre os já existentes na norma, que robusteçam os meios de ponderação entre os direitos tutelados:

> VIII - dever estatal de eficiência, por meio da previsão de mecanismos que otimizem a prevenção, investigação e repressão de infrações penais, sem incorrer em preconceitos de qualquer natureza;
>
> IX - a proteção de direitos individuais e difusos, por meio da aplicação de sanções civis ou penais proporcionais à gravidade das violações;
>
> X - a observância do princípio da proibição da proteção deficiente de bens jurídicos de extração constitucional;
>
> XI – respeito ao direito à segurança.

Quanto às definições trazidas pelo anteprojeto, convém destacar a necessidade de adequação dos conceitos trazidos no texto aos conceitos originais consignados no art. 5º da LGPD. A fim de evitar a contradição entre definições existentes em um e outro normativo, e

a fim de prestigiar a melhor técnica legislativa, propõe-se que seja feita a remissão aos conceitos existentes na LGPD, após o que se acresceriam as demais definições específicas que porventura sejam imprescindíveis à boa compreensão do anteprojeto.

No que se refere às novas definições introduzidas pelo anteprojeto, convém destacar oconceito de dado sigiloso (dado pessoal protegido por sigilo constitucional ou legal), como definição taxonomicamente adequada, porém com desdobramentos incertos quanto à eventualampliação ou impacto sobre o objeto regulado, abarcando dados revestidos pelo sigilo fiscal esigilo bancário, por exemplo, cujos procedimentos relacionados à violação do dever de sigilo e compartilhamento já contam com regulação específica, detalhada e robusta, de modo que serecomenda a sua exclusão do texto do anteprojeto.

Relativamente aos princípios insculpidos ao art. 6º, o anteprojeto agrega aos princípios referenciados na LGPD o princípio da licitude, definido como "embasamento do tratamento de dados pessoais em hipótese legal, nos termos do Capítulo II desta Lei;" i.e., aderência às bases legais para tratamento estabelecidos no art. 9° do anteprojeto. A inclusão do princípio que remete à simples observância da

própria lei, ademais de redundante, suscitou incertezas relativamente à eventual dúvida acerca de se tratar de licitude ou de tipicidade dos meios de tratamento de dados pessoais. Nesse sentido, sugere-se a supressão do inciso, sendo recomendado adotar como redação do caput do referido artigo a mesma fórmula remissiva sugerida ao art. 5º do anteprojeto, referindo os princípios já enumerados na LGPD.

Salienta-se que, em razão da já observada necessidade de que a Lei garanta os meios necessários à ponderação entre os direitos à privacidade e à segurança, a leitura de tais princípios também deverá ser realizada sob a lente do interesse público. Desse modo, em especial no que se refere aos incisos VI e VIII, respectivamente princípios de *livre acesso* e da *transparência*, há de se introduzirem meios a fim de que o exercício dos direitos a eles relacionados não inviabilizem as atividades de investigação e persecução penal. Referidos meios dizem respeito à possibilidade expressa de mitigação da abrangência de tais princípios de tal modo que a finalidade pública dessas atividades não se veja prejudicada pelo acesso prematuro do investigado ou terceiros aos tratamentos de dados realizados no curso da investigação.

Tal circunstância é semelhante àquela já enfrentada pela Administração na interpretação do art. 31 da Lei nº 12.527, de 2011 (Lei de Acesso à Informação) em casos de solicitação de dados pessoais utilizados em investigação preliminar (antes, portanto, de instaurado qualquer procedimento contraditório). Em referidos casos a interpretação preponderante considera tais informações de natureza "preparatória" permitindo-se desse modo a avaliação do interesse público sobre o acesso à informação demandada; o teste de interesse público, nesse contexto, tem como um de seus parâmetros precisamente aquele que aqui se busca prestigiar: o potencial prejuízo à legítima finalidade do processo[2].

No âmbito da UE, o Regulamento 2018/1725, relativo à proteção de dados de pessoas naturais pelos órgãos e entidades da União, admite de modo expresso referidos meios de mitigação, ao dispor, em seu art. 25 sobre a limitação de direitos

[2] BRASIL. Aplicação da Lei de Acesso à Informação no Poder Executivo federal. 4ª edição revista, atualizada eampliada. Brasília, 2019. p. 34

sobre o tratamento de dados pessoais quando “tal limitação respeite a essência dos direitos e das liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática para salvaguardar”, em especial no que tange à “prevenção, a investigação, a detecção e a repressão de infrações penais, ou a execução de sanções penais, incluindo a salvaguarda da segurança pública e a prevenção de ameaças à segurança pública”.

Considerando que o disposto no art. 20 do anteprojeto já veicula conjunto de exceçõesalinhadas ao exposto, avalia-se que a referência a mencionado dispositivo em parágrafo únicodo art. 6º ou mesmo no caput traria maior clareza e segurança sobre a forma como tais princípios deverão ser observados.

Quanto ao art. 8º, registra-se a necessidade de clarificação da redação do anteprojeto afim de evidenciar o agente responsável pela adoção de medidas ali definidas, bem como de ajuste na redação do parágrafo único, visto que a eliminação de dados ao longo de investigações criminais e ações de persecução penal em curso podem trazer prejuízo a tais ações.

3. Capítulo II - Do Tratamento De Dados Pessoais

O Capítulo II do anteprojeto destina-se a regular o tratamento de dados pessoais para as atividades de segurança pública e de persecução penal. Para isso, seus dispositivos não só restringem ao máximo as possibilidades de tratamento e acesso a dados por autoridades policiais e de segurança pública, como também preveem condicionantes para algumas situações, o que em muito obstruirá as atividades de persecução penal e segurança pública, assim como poderá frustrar a solução de crimes.

Isso significa que o anteprojeto retarda a ação policial e vai de encontro à eficiência e à celeridade das atividades de polícia judiciária, na medida em que burocratiza a atividade policial, criando figuras, procedimentos, controles e ritos que, no afã de proteger os direitos à intimidade e à privacidade, acabam por ter efeitos negativos e contrários a ações necessárias para prevenir e reprimir diversos crimes, notadamente aqueles que afetam outros direitos fundamentais igualmente basilares

ao Estado de Direito.

Igualmente, entende-se como a uma barreira ao sucesso de investigações a obrigação de que a requisição de dados descreva concretamente a sua adequação, necessidade e proporcionalidade ao caso concreto (art. 11), assim como a necessidade de especificação de quando deverá ser feita a notificação do acesso, pelo titular, aos dados que foram tratados (art. 11, §4º).

Observa-se que o ordenamento jurídico brasileiro já possui normas viabilizadoras de compartilhamento, acesso e requisição de dados pessoais e informações, como a Lei de Interceptação Telefônica (Lei n. 9.296/1996), que regula as escutas telefônicas e telemáticas; a Lei da Identificação Criminal (Lei n. 12.037/2009), que cuida do registro de dados pessoais,inclusive perfis genéticos, para uso em investigações criminais; os arts. 17-B e 17-E, da Leide Lavagem de Dinheiro (Lei n. 9.613/1998), sobre acesso a dados cadastrais; os arts. 15 a 17, da Lei do Crime Organizado (Lei n. 12.850/2013); e os arts. 13-A e 13-B do Código de Processo Penal (CPP), que disciplinam o acesso a dados cadastrais e metadados para uso em investigações criminais sobre tráfico de pessoas.

Nesse contexto, o ideal seria que o tratamento e o compartilhamento de dados, dentro das hipóteses legais já existentes, fossem mantidos incólumes a fim de garantir ao Estado o cumprimento de seu dever de zelar pela ordem pública.

Destaque-se, também, que a "análise de impacto regulatório" para dados pessoais sensíveis (art.13) não encontra semelhança ou guarida na própria LGPD brasileira, na Diretiva (UE) 2016/680 do Parlamento Europeu e no Conselho de 27 de abril de 2016 (fonte inspiradora do anteprojeto).

Além disso, a avaliação do descarte (art. 15) ou do término do tratamento de dados pessoais (art. 16) deve ser realizada à luz da possibilidade de seu aproveitamento para além
do contexto das investigações específicas, desde que restritas às finalidades de persecução penal e/ou segurança pública. A sugestão encontra-se abrigada nas dimensões de prevenção e detecção contempladas na Diretiva (UE) 2016/680, estando claramente inspirada no considerando 27, *in verbis*:

> (27) Para efeitos de prevenção, investigação ou repressão de infrações penais, **é necessário que as autoridades competentes tratem os dados pessoais, recolhidos no contexto da prevenção, investigação, deteção ou repressão de infrações penais específicas para além desse contexto**, a fimde obter uma melhor compreensão das atividades criminais e de estabelecer ligações entre as diferentes infrações penais detetadas.

Fica claro que essa disposição procura racionalizar a atividade estatal e evita a necessidade de nova coleta do mesmo dado pessoal para utilização em outras esferas sancionatórias, o que encontra paralelo no art. 4º da Diretiva (UE) 2016/680.

Além disso, não se pode ignorar que o tratamento de dados pessoais também envolve tanto a produção de documentos quanto seu arquivamento, e, portanto, sujeito à aplicação da legislação de arquivos.

Veja-se que é competência comum da União, dos Estados, do Distrito Federal e dos Municípios proteger os documentos, as obras e outros bens de valor histórico, artístico e cultural (art. 23, III, da Constituição Federal). Os documentos públicos são identificados como correntes, intermediários e permanentes, de acordo com o art. 8º, caput, da Lei nº 8.159, de 8 de janeiro de 1991.

Nesse contexto, pode ser que dados pessoais tratados para finalidades específicas de persecução penal e segurança pública tenham valor histórico e/ou probatório que impeça o término de seu tratamento ou seu descarte, razão pela qual se considera que a previsão expressa de hipóteses para que isso aconteça pode causar desdobramentos incertos quanto ao impacto sobre as políticas de segurança pública, as futuras investigações penais e acervo histórico do país.

Quanto ao art. 10 do anteprojeto, registra-se que o dispositivo nada mais é do que umareplicação do §2º do artigo 4º da Lei Geral de Proteção de Dados, que procura vedar o tratamento de dados pessoais para atividades de segurança pública e persecução penal por pessoas jurídicas de direito privado, exceto em procedimento sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico ao CNJ.

Como é cediço, umas das matérias-primas básicas de atividades relacionadas tanto à persecução penal quanto à segurança pública, é a busca, coleta e análise de

dados, condutas que dependem da colaboração de pessoas jurídicas de direito privado, legalmente obrigadas a tanto.

Assim, diante de tantas restrições e obrigações, é temerária a vedação ao tratamento de dados pessoais por pessoa jurídica de direito privado, sem a tutela de pessoa jurídica de direito público, para fins de segurança pública ou de investigação e repressão de infrações penais, uma vez que há várias pessoas jurídicas de direito privado que podem vir a subsidiar posterior repressão de infrações penais ou atividades de segurança pública, tendo em vista sua sujeição legal à coleta e compartilhamento de dados pessoais com autoridades de direito público, tanto de seus clientes como aquelas disponíveis publicamente, sempre com o fim de colaborar com a persecução criminal e a garantia da segurança pública. Ademais, pela própria definição de "tratamento" constante no art. 5º, XI, as entidades privadas detentoras de dados pessoais (cadastrais, bancários, telefônicos, telemáticos etc.), ao atenderem ordens judiciais, já realizam um tratamento dos dados para que possam ser disponibilizados.

Nenhuma genérica vedação pode obstar apurações internas e reportes realizados por pessoas jurídicas de direito privado para coleta e compartilhamento de dados de clientes ou pessoas a elas relacionadas envolvidas em atividades criminosas, inclusive vítimas dessas atividades. Referidas apurações e reportes são realizados, muitas vezes, em meio a atividades de gerenciamento de riscos de entidades privadas, previamente à instauração de inquéritos ou durante procedimentos de autoridades policiais e judiciárias competentes. São atos de colaboração essenciais para o sucesso desses procedimentos e para que o exercício regular de direitos por parte das vítimas ou instrução adequada com material probatório para a atos ilícitos e criminosos.

Além disso, tal disposição pode ter sua constitucionalidade questionada por ferir os princípios gerais da ordem econômica na Constituição Federal, como o da livre iniciativa e da livre concorrência, uma vez que é no campo privado em que é desenvolvida a maior gama de inovações tecnológicas, como softwares de tratamento de dados que são cada vez mais utilizados em atividades de persecução penal e segurança pública.

Sob tal perspectiva, entende-se que, ao invés de criar hipótese tão restritiva, o

melhor cenário seria a elaboração de critérios orientadores a serem observados por pessoas jurídicas de direito privado, para que estas possam fazer o tratamento de dados em atividades de persecução penal e segurança pública sob tutela de autoridades públicas.

4. Capítulo III - Dos Direitos Do Titular

Nesse capítulo, o anteprojeto pretende regular os princípios da autodeterminação informativa e da transparência, com o objetivo de garantir ao titular a prestação de informações e a concessão de acesso a dados pessoais em tratamento por autoridades de segurança pública e persecução penal.

Em seus artigos 27 e 28, procura assegurar aos titulares dos dados o exercício do direito de apresentar denúncias anônimas por violação ao tratamento de dados e a possibilidade de defesa de seus direitos de maneira individual ou coletiva, o que denota harmonia com o texto constitucional.

Ocorre que o art. 20 dispõe de forma precária acerca das hipóteses em que a prestaçãode informações poderá ser limitada ou recusada ao titular dos dados.

Ao dispor sobre a necessidade de "*indicar quando cessarão os motivos da recusa ou da limitação de acesso*", o §1º, do mesmo artigo, cria obrigação que apenas pode ser adimplida nas situações em que for viável fazer tal prognóstico.

Nesse contexto, seria necessário que o anteprojeto abrangesse outras hipóteses de adiamento, limitação ou recusa do acesso aos dados pessoais em tratamento, quando houver dúvidas sobre a identidade do solicitante e com a finalidade de proteger atividades de segurança pública.

Já em seu art. 24, o anteprojeto prevê a necessidade de prévia autorização de órgão externo como condição necessária para a adoção de tratamento automatizado de dados pessoais. Essa exigência incorre em flagrante desproporcionalidade e cria entraves ao tratamento de dados nas atividades de prevenção, detecção, investigação e repressão penal, eis que, hodiernamente, a atividade investigativa vem dependendo cada vez mais da utilização de ferramentas tecnológicas, para recepção, organização e análise da enorme gama de dados oriunda das mais variadas fontes de

prova.

No cenário atual, para que dados bancários, telefônicos, fiscais e telemáticos sejam recepcionados, tratados e analisados de forma satisfatória, os órgãos de persecução penal investem em recursos tecnológicos focados justamente no tratamento automatizado de dados, sendo que a previsão inserta no referido anteprojeto irá obstaculizar esse auxílio tecnológico para análise de grande massa de dados.

Com efeito, a maior parte das disposições previstas nessa parte do anteprojeto não encontra harmonia com o texto constitucional no que tange ao princípio da eficiência da segurança pública (144, §7º, CF), o qual dispõe sobre a obrigação estatal de prestação de serviços de segurança pública, com a finalidade de proteger a vida e incolumidade do cidadãoe de seu patrimônio.

Pode-se dizer, assim, que esse preceito constitucional apresenta, em certa medida, caráter programático, uma vez que confere ao legislador o poder de disciplinar os sistemas deatuação policial e organizacional a fim de aperfeiçoá-los para que seus respectivos órgãos apresentem desempenhos satisfatórios na preservação da ordem pública.

Desse modo, pela exigência de eficiência redobrada, tanto a política de segurança pública quanto os serviços de persecução e repressão penal devem apresentar alto nível de qualidade, e, para isso, seus órgãos precisam ser dotados de meios aptos a garantir o êxito de suas atividades funcionais.

5. Capítulo IV - Dos Agentes de Tratamento de Dados Pessoais

O caput do artigo 29 traz obrigação já constante na redação do artigo 13 em relação a elaboração de relatório de impacto à proteção de dados pessoais para tratamento de dados pessoais sensíveis, sendo inoportuna a sua repetição.

6. Capítulo V- Da Segurança e do Sigilo dos Dados

Acerca dessa parte do anteprojeto, merece destaque a necessidade de se

compatibilizaro prazo para comunicar incidente de segurança, previsto no art. 38, a, no mínimo, o prazo prescrito na LGPD, de forma a não conferir tratamento mais restritivo à ocorrência de incidente de segurança em relação às autoridades competentes para as atividades de segurança e de persecução penal.

A proposta também excede seu escopo ao dispor sobre o tratamento de registros criminais em seu artigo 39, adentrando questões próprias do Código Penal, do Código de Processo Penal e da Lei de Execução Penal, situação que, caso não corrigida, com a supressão do referido dispositivo legal, causará insegurança jurídica e embaraços de todo tipo às atividades de segurança pública, investigação e de persecução penal.

O tratamento dos registros criminais tem minuciosa regulamentação nos artigos 93 do Código Penal; nos artigos 6º, 20, parágrafo único, 28-A, §12, 694, 708, parágrafo único, 736, 748, 809 do Código de Processo Penal; e nos artigos 5º, 77, 106, 114, 163, 180 e 190 e 202da Lei de Execução Penal, sendo despiciendo que o anteprojeto venha dispor sobre tal matéria.

Além disso, cabe ressaltar que os registros criminais nada mais são do que dados tratados no âmbito de uma investigação criminal ou de um processo judicial em matériapenal, sendo sua regulamentação pertinente às regras aplicáveis aos processos judiciais. Não é por outra razão que a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016 assim dispõe:

> (49) Caso os dados pessoais sejam tratados no âmbito de uma investigação criminal ou de um processo judicial em matéria penal, os Estados-Membros deverão poder dispor que o exercício do direito à informação, ao acesso aos dados pessoais e à sua retificação ou apagamento, bem como à limitação do tratamento, seja feito nos termos das regras nacionais aplicáveis aos processos judiciais.

E mais, a Diretiva (UE) 2016/680, a LGPD Penal Portuguesa (art. 68), a LGPD Penal Italiana (art. 14), a LGPD alemã (art. 7º) excluem da supervisão da autoridade de controle as operações de tratamento de dados efetuados no exercício da função jurisdicional.

Deste modo, entende-se que o normativo brasileiro deve trilhar o mesmo caminho da LGPD Penal Portuguesa (art.68) que dispõe, expressamente, que o

tratamento de dados pessoais constante de processo penal, de decisão judicial ou do registro criminal é regulado nos termos da lei processual penal.

7. Capítulo VI- Acesso à Informação e Transparência

Em seus artigos 40 e 41, o anteprojeto pretendeu disciplinar o acesso à informação e a transparência, matérias exaustivamente disciplinadas pela Lei nº 12.527/2011 (Lei de Acesso à Informação), vigente há mais de uma década e já consolidada no âmbito da Administração Pública.

Admitir uma regulamentação distinta daquela já prevista na Lei de Acesso à Informação importará em inevitável insegurança jurídica, sem qualquer ganho para a proteção da intimidade do titular do dado.

Além disso, a disciplina proposta no anteprojeto causaria embaraços insuperáveis às atividades de segurança pública, investigação e persecução penal, tendo em vista a necessidade de manutenção de sigilo do tratamento de dados pessoais no curso das apurações,em regra sigilosas, com a finalidade de viabilizar elucidação do fato investigado, conforme disposição expressa no artigo 20 do Código de Processo Penal, sendo assegurado, enquanto direito do defensor e no interesse do representado, ter acesso amplo aos elementos de prova que, já documentados em procedimento investigatório realizado por órgão com competência de polícia judiciária, digam respeito ao exercício do direito de defesa, nos termos da Súmula Vinculante nº 14 do Supremo Tribunal Federal.

Assim, entende-se que o anteprojeto não deve tratar sobre o acesso à informação e a transparência, sendo suficiente para a proteção dos dados pessoais e para a promoção do direito à segurança pública e à persecução penal eficiente à legislação processual penal e à Lei de Acesso à Informação vigentes.

8. Capítulo VII - Tecnologias de Monitoramento e Tratamento de Dados de Elevado Risco

Nos artigos 42 a 44, o anteprojeto busca disciplinar a utilização de tecnologias de monitoramento ou o tratamento de dados pessoais que representem elevado risco para direitos, liberdades e garantias dos titulares dos dados.

Percebe-se, de plano, a ausência de uma definição do que seja tecnologia de monitoramento ou o tratamento de dados pessoais que representem elevado risco, o que, por si, gera grave insegurança jurídica. Além disso, o condicionamento da utilização de novas tecnologias de monitoramento e tratamento de dados à edição de lei específica, importa em inviabilizar o avanço tecnológico para a execução das atividades de segurança pública,investigação e persecução penal, tornando deficiente a proteção ao direito fundamental à segurança pública e a uma atuação eficiente dos órgãos e instituições públicos encarregados de tal mister.

Destaque-se, ainda, a inconstitucionalidade da tentativa de disciplinar o processolegislativo acerca da autorização para a utilização de tecnologias de vigilância e o tratamento de dados pessoais por autoridades competentes que implique elevado risco, exigindo a elaboração da denominada análise de impacto regulatório, instrumento não previsto na LGPD brasileira voltada para o tratamento de dados por agentes privados, tampouco previsto na Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Para além do fato de lei ordinária não ser o instrumento normativo adequado para disciplinar o processo legislativo, conforme disposto no art. 59, parágrafo único, da Constituição Federal, novamente, o texto do anteprojeto impõe ao desempenho das atividades de segurança pública e persecução penal restrições desproporcionais em relação aos direitos fundamentais tutelados pelos órgãos e instituições competentes.

Em sequência, o artigo 43 veda, de forma peremptória, o uso de tecnologias de vigilância associadas a técnicas de identificação de pessoas para os fins de segurança pública,restringindo de forma desproporcional a atividade de segurança pública, em suas facetas de detecção e prevenção de crimes.

A proibição do uso de tecnologias de vigilância associadas a técnicas de identificação de pessoas, nos moldes propostos no anteprojeto efetivamente se afigura como medidaexcessivamente restritiva e desproporcional, na medida em que somente poderia ser utilizada quando, concomitantemente: (a) haja lei autorizando;

(b) em casos de persecução penal individualizada e (c) mediante decisão judicial. A vinculação da utilização da referida tecnologia à edição de lei posterior e a limitação de seu uso à atividade de persecução penal, excluindo a possibilidade de sua utilização como meio de prevenção de crimes, mas unicamente para a persecução, por si só afrontam de forma chapada o direito à segurança previsto no artigo 6º, *caput*, da Constituição Federal.

É necessária a descrição de parâmetros adequados para a elaboração e implementação desse relatório de impacto à proteção de dados pessoais no texto do novel diploma legislativo para garantir a implementação de tecnologias de vigilância associadas a técnicas de identificação de pessoas e compatibilizar o direito à segurança pública com o direito àintimidade e à consequente proteção dos dados pessoais sensíveis.

9. Capítulo VIII - Compartilhamento de Dados

A maneira desproporcional como a proposta procura refrear o compartilhamento de dados entre as instituições e os órgãos encarregados constitucionalmente das atividades de persecução penal e de segurança pública não é reproduzida na própria LGPD, na Diretiva (UE) 2016/680 (artigo 45, 2), na LGPD Portuguesa (Lei n.º 59/2019, art. 43) e na Lei Federalde Proteção de Dados Alemã, de 30 de junho de 2017 (arts. 7º, 9º, 60). Aliás, ao contrário do que pretende o anteprojeto de LGPD Penal brasileira, a Diretiva (UE) 2016/680, em seu Considerando 7, destaca a necessidade de facilitar o intercâmbio de dados pessoais entre as autoridades competentes, a fim de assegurar a eficácia da cooperação judiciária em matéria penal e da cooperação policial.

Os artigos 45 a 52 pretenderam disciplinar qualquer modalidade de compartilhamento de dados pessoais entre autoridades competentes e o fizeram de forma extremamente restritiva e desproporcional, deixando completamente desprotegidos o direito fundamental à segurança e a atuação eficiente das autoridades competentes para as atividades de segurança pública e persecução penal.

A vingar o texto proposto no anteprojeto, restará inviabilizada, por completo,

a cooperação entre agências de persecução penal e de segurança pública, tão necessária ao combate da criminalidade organizada, cibernética, violenta ou de colarinho branco, bem como fatalmente comprometidas as dimensões da prevenção e da detecção de infrações penais, ao revés, inclusive, do quanto edificado no sistema europeu - inspiração do anteprojeto - e uma necessidade da vida em sociedade.

Com efeito, o tratamento de dados realizado no âmbito de atividades de segurança pública não pode, de forma alguma, obstar que os dados pessoais sejam utilizados a execução de outras missões de interesse público, para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais.

Essa é a solução adotada pela Diretiva (UE) 2016/680, como se vê do artigo 4º, 2, a seguir transcrito:

> Artigo 4º Princípios relativos ao tratamento de dados pessoais [...]
>
> 2. É permitido o tratamento pelo mesmo ou por outro responsável pelo tratamento para as finalidades previstas no artigo 1º, nº 1, diferentes da finalidade para a qual os dados pessoais foram recolhidos, DESDE QUE:
>
> a) O responsável pelo tratamento esteja autorizado a tratar esses dados pessoais com essa finalidade, nos termos do direito da União ou dos Estados-Membros; e
>
> b) O tratamento seja necessário e proporcionado para essa outra finalidade, nos termos do direito da União ou dos Estados-Membros. [...]
>
> (29) Os dados pessoais deverão ser recolhidos para finalidades determinadas, explícitas e legítimas abrangidas pelo âmbito de aplicação da presente diretiva e não deverão ser tratados para fins incompatíveis com os da prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais — nomeadamente a salvaguarda e a prevenção de ameaças à segurança pública.
> Se os dados pessoais forem tratados, pelo mesmo ou por outro responsável pelo tratamento, para uma finalidade abrangida pelo âmbito de aplicação da presente diretiva que não aquela para a qual foram recolhidos, esse tratamento deverá ser permitido, na condição de que esse tratamento seja autorizado em conformidade com as disposições legais aplicáveis e necessário e proporcionado para a prossecução dessa outra finalidade.
>
> (35) Para ser lícito, o tratamento de dados pessoais nos termos da presente diretiva deverá ser necessário para a execução de uma missão de interesse público por uma autoridade competente com

> base no direito da União oudos Estados-Membros para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. Estas funções deverão abranger a proteção dos interesses vitais do titular dos dados. O exercício das funções de prevenção, investigação, deteção ou repressão de infrações penais conferidas institucionalmente por lei às autoridades competentes permite-lhes exigir que as pessoas singulares cumpram o que lhes é solicitado. [...]

Mais condizente com a realidade e com a necessidade de se assegurar o direito à segurança, previsto no art. 6º da Constituição Federal, a LGPD Penal Portuguesa, por exemplo, destaca de forma expressa que as suas disposições não implicam qualquer restrição ou limitação na partilha e intercâmbio de dados entre os órgãos de polícia criminal e destes com as autoridades judiciárias, no âmbito do dever de cooperação estabelecido na lei de organização da investigação criminal (cf. art. 69 da Lei nº 59/2019), dispositivo que merece ser internalizado no âmbito da presente proposta de diploma legislativo.

A aprovação do texto nos moldes previstos no anteprojeto importaria na impossibilidade do uso de tecnologias em prol da eficiência das atividades de segurança pública e de persecução penal, provocando consequências ruinosas à sua efetividade, a exemplo de criar obstáculos tecnológicos ao compartilhamento de dados de forma contínua e direta pelo Conselho de Controle de Atividades Financeiras (COAF).

A vedação de compartilhamento de dados financeiros pelo COAF por meio do envio de relatórios de inteligência financeira, de forma direta e contínua, inclusive, foi objeto de apreciação pelo Supremo Tribunal Federal no âmbito do Recurso Extraordinário nº 1055941, que fixou a tese sobre a constitucionalidade do compartilhamento dos relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil, que define o lançamento do tributo, com os órgãos de persecução penal, para fins criminais, sem a obrigatoriedade de prévia autorização judicial.

Destaque-se, ainda, que a aprovação de dispositivo desta natureza teria o potencial de afetar a República Federativa do Brasil inclusive no cenário internacional,

diante da oposição de obstáculos ao atendimento às Recomendações do Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (GAFI/FATF), em especial a Recomendação 29 e a Recomendação 31, abaixo transcritas:

> **Recomendação 29. Unidades de Inteligência Financeira:** Os países deveriam estabelecer uma unidade de inteligência financeira (UIF) que sirvacomo um centro nacional de recebimento e análise de: (a) comunicações de operações suspeitas; e (b) outras informações relevantes sobre lavagem de dinheiro, crimes antecedentes e financiamento do terrorismo, e de disseminação dos resultados de tal análise. A UIF deveria ser capaz de obter informações adicionais das entidades comunicantes e ter acesso rápido a informações financeiras, administrativas e de investigação que necessitepara desempenhar suas funções adequadamente.
>
> **Recomendação 31. Poderes das autoridades de investigação e de aplicação da lei**: Durante o curso de investigações de lavagem de dinheiro, de crimes antecedentes e de financiamento do terrorismo, as autoridades competentes deveriam ter acesso a todos os documentos e informaçõesnecessários para as investigações, bem como para as ações penais e outras ações a elas relacionadas. Esses poderes deveriam incluir o poder de adotar medidas compulsórias para a requisição de registros mantidos por instituições financeiras, APNFD e outras pessoas físicas ou jurídicas, bem como para a busca de pessoas e propriedades, para a tomada de declarações de testemunhas, e para a busca e obtenção de provas. Os países deveriam assegurar que as autoridades competentes ao conduzirem investigação tenham acesso a uma grande variedade de técnicas investigativas adequadas às investigações de lavagem de dinheiro, crimes antecedentes e financiamento do terrorismo. Tais técnicas incluem: operações encobertas, interceptação de comunicações, acesso a sistemas computacionais e entrega controlada. Além disso, os países deveriam possuir mecanismos efetivos para identificar rapidamente se pessoas físicas ou jurídicas são titulares ou controlam contas. Deveriam também possuir mecanismos para garantir que as autoridades competentes tenham algum procedimento para identificar ativos sem notificação prévia do proprietário. Durante as investigações de lavagem de dinheiro, crimes antecedentes e financiamento do terrorismo, as autoridades competentes deveriam poder solicitar quaisquer informações relevantes à UIF.

Já no artigo 48, a proposta busca tornar exceção o compartilhamento de dados por pessoas jurídicas de direito privado com autoridades competentes para as

atividades desegurança pública e persecução penal.

A proibição, como regra geral, ou a imposição de um caráter excepcional ao compartilhamento de dados entre pessoas jurídicas de direito privado e as autoridades competentes viola diretamente o princípio da proporcionalidade, porquanto deixa desprotegido o direito fundamental à segurança e a uma atuação eficiente dos órgãos e instituições responsáveis pelas atividades de segurança pública e persecução penal em uma ponderação absolutamente desequilibrada com o direito a intimidade relativa aos dadospessoais custodiados por pessoas jurídicas de direito privado.

A disponibilização às autoridades competentes de dados controlados por pessoasjurídicas de direito privado é medida de rigor e se submete ao regime da requisição estatal amparado legal e constitucionalmente. Veja-se que à exceção dos dados submetidos à reservade jurisdição, o acesso aos demais dados custodiados por pessoas jurídicas de direito privado depende de apenas de requisição expedida pelo Ministério Público em procedimento de sua competência, conforme previsão no artigo 129, VI, da Constituição Federal, no artigo 7º, IV eVIII, da Lei Complementar nº 75/93, no artigo 26, II, da Lei nº 8.625/93, no artigo 8º, §1º, da Lei nº 7.347/85, nos artigos 15, 16, 17 da Lei nº 12.850/2013, e artigos 13-A e 13-B do Código de Processo Penal.

Note-se, ainda, que o compartilhamento de dados entre pessoas jurídicas de direito privado e as autoridades competentes não é vedado pela LGPD (Lei nº 13.709/2018), não havendo razão para se impor a proibição como regra geral para um compartilhamento fundamental na colaboração para o sucesso das atividades de segurança pública e de persecução penal. Outrossim, o compartilhamento de dados entre os órgãos da administração pública tem como finalidade aumentar a qualidade e a eficiência dos serviços prestados, em atenção ao art. 37, caput, da Constituição Federal e art. 1º do Decreto nº 10.046/2019.

Assim, em razão de causar graves embaraços ao exercício das funções institucionais dos órgãos e instituições competentes para as atividades de persecução penal e de segurança pública, o dispositivo deve ser suprimido.

10. Capítulo IX - Transferência Internacional de Dados e Cooperação Internacional

Em seu artigo 53, o anteprojeto de LGPD Penal cuida da transferência de dados pessoais para outro país ou para uma organização internacional; entretanto não ressalva a possibilidade de transferência sem o consentimento prévio na hipótese de se prevenir uma ameaça imediata e grave à vida, limitando-se à prevenção de ameaça à segurança do Brasil oude um país estrangeiro.

Diante da estatura do bem jurídico vida, faz-se necessário o ajuste no texto do anteprojeto para deixar evidente a possibilidade de transferência de dados pessoais para outro país ou para uma organização internacional, em situações em que se mostre necessário fazer frente a uma ameaça imediata e grave à vida.

De outro lado, é imprescindível o ajuste na redação proposta no artigo 53 de forma a esclarecer que as hipóteses de transferência internacional de dados pessoais são alternativas e não cumulativas, sob pena de obstar a tão necessária cooperação internacional em um mundo globalizado.

11. Capítulo X - Unidade Especial de Proteção de Dados em Matéria Penal

O ponto central a ser tratado diz respeito à atribuição ao Conselho Nacional de Justiça(CNJ), do papel de unidade especial de proteção de dados em matéria penal.

Ocorre, entretanto, que a ampliação das atribuições constitucionais do Conselho Nacional de Justiça por meio de lei ordinária não se coaduna com o nosso regime jurídico- constitucional.

Desde logo, cumpre ter claro que o CNJ, nos termos do disposto no art. 92, I-A da Constituição Federal, é órgão interno do Poder Judiciário, e tem atribuições expressamente determinadas na Constituição, que em seu artigo 103-B, § 4º dispõe que compete ao "*Conselho o controle da atuação administrativa e financeira do Poder Judiciário e documprimento dos deveres funcionais dos juízes*". Todo o plexo de atribuições conferidas peloconstituinte derivado ao CNJ enquadra-se nos limites da atuação geral de efetivar essecontrole administrativo e orçamentário dos órgãos

do Poder Judiciário e disciplinar dosmagistrados (excetuando-se o STF). Com efeito, ainda que o rol das competências constantes dos incisos I a VII do § 4º do art. 103-B seja meramente exemplificativo, não se pode desbordar dos limites constitucionais para conferir função anômala ao CNJ, distante do quadro desenhado pelo legislador constituinte.

Assim, propor que o CNJ possa constituir uma Unidade Especial de Proteção de Dados em Matéria Penal (UPDP) para assumir a função de autoridade nacional de proteçãode dados em matéria penal, resulta em uma ampliação inadequada das finalidades constitucionais do CNJ.

De fato, é preciso que se tenha claro que, como definido pelo STF quando do julgamento da ADI 3367, mais do que órgão de controle, o CNJ foi criado com a missão de exercer a função política de aprimorar o autogoverno do Judiciário nacional, cujas estruturas dispersas e fragmentadas a partir da repartição constitucional de competências, dificultam o esboço de uma estratégia político-institucional de âmbito nacional. Trata-se de um órgão interno ao judiciário e que detém as atribuições de centralizar as tarefas de formulação de diagnósticos, elaborar políticas judiciárias, tecer críticas construtivas e elaborar programas que, no limite de suas responsabilidades constitucionais, possibilitem respostas eficazes aos múltiplos problemas comuns à atividade de prestação jurisdicional.

Nesse contexto, tem-se que qualquer tentativa de alteração da matriz constitucional daatuação do CNJ esbarra nos limites que a Constituição desenhou para o funcionamento do órgão, estipulando claramente sua função dentro do equilíbrio institucional desenhado pelo constituinte.

Nesse ponto, cabe notar que a Constituição até autoriza que sejam ampliadas as competências do CNJ, desde que essa alteração seja levada a efeito pelo Estatuto da Magistratura, que nos termos do disposto no art. 93 da CF/88, será veiculado por LeiComplementar. Assim, uma vez que cláusula de abertura traçada pela Constituição restringe aampliação das competências do CNJ ao Estatuto da Magistratura, fica evidente que talampliação somente pode ocorrer quando relacionada a matérias que guardem estreita pertinência temática com a magistratura.

Não é o que se verifica no anteprojeto (art. 62), que além de não respeitar a

adequaçãoformal quanto à espécie normativa, visto que se trata de lei ordinária, não de lei complementar de iniciativa privativa do Supremo Tribunal Federal, como exige o art. 93 parao Estatuto da Magistratura, tampouco se refere a matéria relativa ao controle administrativoou disciplinar da magistratura.

Trata-se de atribuições que afetarão diretamente toda a rede de atuação dos envolvidosna persecução penal, atividade que, por sua própria natureza, implica o tratamento de dados pessoais.

Assim, seja em razão da irregularidade formal (lei ordinária ampliando competência que a Constituição somente admite seja ampliada por lei complementar de iniciativa privativa), seja em razão da inconstitucionalidade material (atribuição de funções estranhas à regra matriz constitucional para o funcionamento do CNJ), é descabido falar-se em constituição de uma Unidade Especial de Proteção de Dados em Matéria Penal (UPDP) para assumir a função de autoridade nacional de proteção de dados em matéria penal.

A essas questões de índole constitucional adiciona-se, ainda, uma relacionada a política criminal. É que o CNJ, tendo competência constitucional para efetuar o controle interno da magistratura, exerce efetivamente um elevado papel na atuação dos magistrados. Ainda que sua atuação seja meramente administrativa, não se pode descurar que por vezes a regulamentação de determinadas matérias situa-se em uma zona cinzenta entre o administrativo e o jurisdicional.

Daí porque a atividade jurisdicional ser comumente excluída do âmbito de incidência das normas relativas à proteção de dados em matéria penal, já que, no limite, seria possível cogitar-se de uma autoridade administrativa exercendo controle de atos de cunho nitidamente jurisdicional. Com efeito, basta pensar na possibilidade nada remota de que uma decisão judicial determine a coleta e o tratamento de dados relativos, por exemplo, às pesquisas feitas por buscadores na internet em um determinado período de tempo, em uma dada localidade e que tal decisão seja considerada inadequada pela autoridade administrativa competente para exercer o papel de responsável pela proteção de dados. Em tal hipótese, seria possível que a autoridade administrativa determinasse ao Judiciário a "*eliminação dos dados pessoais utilizados*", tal como previsto no art. 63, inciso IV do anteprojeto, ou mesmo

que determinasse a "*suspensão do exercício da atividade de tratamento dos dados pessoais*" por parte do Judiciário?

Em se tratando de autoridade meramente administrativa, evidentemente a resposta teria que ser negativa, por notória violação aos princípios da indeclinabilidade da jurisdição e da independência judicial, pedras angulares da atuação de um Judiciário que efetivamente possa atuar como terceiro imparcial na aplicação da lei e da Constituição. Havendo um conflito entre a autoridade judicial e a administrativa encarregada da proteção de dados, apesar dos ruídos institucionais, dificilmente haveria prejuízo sério à atividade jurisdicional,já que não haveria o necessário *enforcement* assegurando a aplicação da medida administrativa. Entretanto, se a autoridade administrativa fosse uma autoridade interna do Poder Judiciário, como o CNJ, especialmente quando somado ao controle administrativo também estivesse o controle disciplinar, certamente haveria um risco nada desprezível à violação da autonomia judicial. Como bem afirmou o relator da ADI 3367:

> "Ninguém tem dúvida de que não se pode a independência do Poder Judiciário, seja a externa, assim considerada a da instituição perante os demais Poderes e órgãos de pressão, seja a interna, a dos magistrados entre si, estar sob nenhum risco próximo nem remoto, porque, em resguardo da ordem jurídica e, ao cabo, da liberdade do povo, tal predicado constitui a fonte, o substrato e o suporte de todas as condições indispensáveis a que a atividade judicante seja exercida com a imparcialidade do tertius, sem a qual já não se concebe a jurisdição em nenhum Estado civilizado e, muito menos, no Estado democrático de direito"

A independência do Judiciário guarda especial relevo no quadro da separação de Poderes por ser necessária para garantia da imparcialidade jurisdicional, por isso que não se pode admitir a edição de normas que tendam a romper o equilíbrio constitucional em que se apoia esse atributo elementar da função típica do Poder Judiciário.

Assim, não é adequado que a função de autoridade nacional de proteção de dados em matéria penal seja assumida pelo CNJ, sendo necessário propor um arranjo institucional que reflita a complexidade do tema, a necessitar de uma abordagem multissetorial, com participação de representantes do Judiciário (a serem indicados

pelo CNJ), do Ministério Público (a serem indicados pelo CNMP), além de representantes do Ministério da Justiça e das secretarias de segurança pública dos estados, dentre outros, criando-se, por exemplo, um colegiado temático, de estrutura similar à ANPD – uma ANPD Penal, garantida a cooperação de pessoas jurídicas de direito privado fortemente envolvidas na colaboração com autoridadespúblicas para a persecução criminal e segurança pública.

12. Capítulo XI - Sanções

Por fim, quanto às sanções, previstas nesse capítulo, desde logo é de deixar claro que elas não poderão ser aplicadas ao tratamento de dados feito pelo Judiciário no exercício de sua atividade típica, isto é, no exercício da jurisdição. Por mais que a indeclinabilidade da jurisdição torne pouco provável que o órgão administrativo efetivamente possa aplicar sanções visando a coarctar a independência judicial e, portanto, a imparcialidade dos magistrados, não convém deixar aberta a porta para que se iniciem discussões acerca dessa matéria, especialmente quando se nota a sensibilidade da atuação em matéria penal.

Da mesma forma, tendo em conta que se cuida de regulamentar a atuação de agentes públicos, relacionada à utilização de dados coletados e armazenados em repositórios públicos, tampouco é possível pensar na possibilidade de aplicação das sanções previstas nos incisos V (suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador, quando cabível) e VI (suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de6 (seis) meses, prorrogável por igual período, quando cabível.) do anteprojeto, em razão de sua incompatibilidade com a natureza do tratamento de dados por autoridades competentes para atividades de segurança pública e de persecução penal.

13. Capítulo XII – Disposições Finais e Transitórias

A previsão do caput do artigo 67, no sentido de que "*a adequação do*

tratamento de dados às normas previstas nesta lei deverá ser implementada pelos agentes de tratamento até a sua entrada em vigor, sob pena de ilicitude do tratamento", permite uma interpretação errônea acerca das consequências da inadequação do tratamento de dados.

Sabido é que os atos processuais estão sujeitos à forma prescrita em lei, sob pena de invalidação. Contudo, o tema das nulidades no processo penal está umbilicalmente ligado à questão do prejuízo, seja em razão de violação às garantias constitucionais individuais inerentes ao processo penal, seja em razão de se colocar em risco a própria função judicante. Inclusive, a impossibilidade de anulação de ato processual sem comprovação de prejuízo já é entendimento consolidado em nosso Supremo Tribunal Federal (HC 151231, HC 137889, HC119293, HC 104.767, HC 84.098, RE 263.012-AgR, HC 79.446). Abaixo, esclarecedor
trecho da Ementa do HC 111472, Relator Min. Luiz Fux,

> (...) O processo penal rege-se pelo princípio da instrumentalidade das formas, do qual se extrai que as formas, ritos e procedimentos não encerram fins em si mesmos, mas meios de se garantir um processo justo e equânime, que confira efetividade aos postulados constitucionais da ampla defesa, do contraditório e do devido processo legal. (...)

Diante do exposto, e mesmo considerando-se a sugestão de elastecimento do prazo de *vacatio legis*, sugere-se a supressão da referência à ilicitude do tratamento em caso de atraso na implementação das disposições da LGPD Penal, para constar "a adequação do tratamento de dados às normas previstas nesta lei deverá ser implementada pelos agentes de tratamento até a sua entrada em vigor".

É necessário, também, elastecer o prazo previsto para a vigência da norma, tendo em vista o grande impacto que trará a todos os órgãos e instituições que desenvolvem atividades de segurança pública e de persecução penal, em defesa do interesse público.

Ressalte-se que serão necessários investimentos de recursos públicos para fazer frente às novas exigências legais e sua mensuração somente será possível a

partir da sanção e publicação do novel diploma legislativo. Deste modo, deverá ser assegurado prazo suficiente para que os órgãos e instituições que desenvolvem atividades de segurança pública e de persecução penal contemplem em seus orçamentos os valores correspondentes às adaptações às quais estarão obrigadas a atender, o que exige, no mínimo, que o lapso temporal alcance tempo superior a um ciclo orçamentário.

Assim, entende-se ser necessário a alteração do prazo previsto no art. 68 do anteprojeto da LGPD Penal para se prever o período de *vacatio legis* de 24 meses, após a datade sua publicação.

14. Conclusão

É cediço que cada vez mais a internet e aplicações tecnológicas passam constantemente por avanços, e isso implica em pontos positivos e negativos para a sociedade. Entre os pontos negativos encontra-se uma gama de dados pessoais, públicos, sigilosos e sensíveis, que devem ser tratados de maneira segura por entidades e órgãos públicos eprivados, a fim de evitar a violação de direitos individuais da sociedade.

Contudo, não se pode perder de vista que, para que órgãos e entidades de segurança pública e persecução penal possam cumprir suas funções institucionais, o tratamento e compartilhamento de dados pessoais para essa finalidade não pode seguir a mesma lógica da Lei Geral de Proteção de Dados ou adotar regramento mais gravoso, sob pena de inviabilizara eficiência de suas atividades. Sem prejuízo, pode adotar seus conceitos e princípios para fins de coesão sistêmica, contanto que esses não afrontem ou violem a eficiente persecução penal e a garantia da segurança pública, fundamentais para a ordem pública brasileira.

Os direitos fundamentais não são absolutos e não podem impedir o uso inteligente de dados nas atividades de prevenção, detecção, investigação e repressão de infrações penais, funcionando escudo para a atuação de organizações criminosas.

A partir disso, o anteprojeto apresenta, na verdade, um grande descompasso na busca de equilíbrio e proporcionalidade entre a proteção a direitos individuais e o dever social de persecução penal e de segurança pública, criando embaraços aos

mecanismos e instrumentos básicos de investigação, repressão, prevenção e segurança pública

Portanto, essa Ação da ENCCLA entende que o texto do anteprojeto necessita de profundas reformulações, de modo a compatibilizar o direto fundamental à segurança pública e o dever de eficiência do sistema penal com os direitos individuais afetos à personalidade, proteção de dados e autodeterminação informativa.