

NOTA TÉCNICA n° 05/2021-PGJ
Lei de Proteção de Dados Criminais

Realização:
Grupo de Trabalho - PGJ
Secretaria Especial de Políticas Criminais
Centro de Apoio às Promotorias Criminais - CAOCrim
Procuradoria-Geral de Justiça - 19/2/2021

NOTA TÉCNICA Nº 05/2021-PGJ

EMENTA. PROTEÇÃO DE DADOS NAS ATIVIDADES DE SEGURANÇA PÚBLICA E PERSECUÇÃO PENAL. OBJETIVO DA LEI. EQUILÍBRIO ENTRE A PROTEÇÃO DE DIREITOS FUNDAMENTAIS E A EFICIÊNCIA DO ESTADO NA PROTEÇÃO DOS CIDADÃOS: ALTO NÍVEL DE PROTEÇÃO E COMPARTILHAMENTO DE DADOS. AUTORIDADE DE CONTROLE: CONTORNOS CONSTITUCIONAIS. RESPEITO À SEPARAÇÃO DOS PODERES E À INDEPENDÊNCIA DO MINISTÉRIO PÚBLICO E JUDICIÁRIO.

Sumário. 1. RELATÓRIO. 2. OBJETIVO DA LEGISLAÇÃO. 3. ALTO NÍVEL DE PROTEÇÃO E COMPARTILHAMENTO DE DADOS: DADOS SIGILOSOS E DADOS SENSÍVEIS. 3.1. Limites constitucionais: privacidade e a proteção de dados. 3.2. Flexibilização do direito fundamental por lei *proporcional*. 3.3. Aumento da proteção via legislativa: cláusula *legal* de reserva jurisdicional. 3.4. Transmissão de dados sigilosos *sem* prévia autorização judicial. 3.5 Formalização e controle sobre a finalidade do tratamento. 3.6. Sistema *interoperável* para o tratamento de dados pessoais. 4. AUTORIDADE DE CONTROLE: CONTORNOS CONSTITUCIONAIS. 4.1. Função NÃO jurisdicional. Separação dos poderes. Independência do Judiciário e Ministério Público em suas funções típicas. 4.2. Escolha do Conselho Nacional de Justiça como Autoridade de Controle. Função administrativa: poder normativo, fiscalizatório e sancionatório. 4.2.1. Autonomia administrativa do Ministério Público. 4.2.2. Impossibilidade de o Conselho Nacional de Justiça ingerir na autonomia administrativa de outros poderes. 5. CONCLUSÕES.

1. RELATÓRIO.

A novel Lei Geral de Proteção de Dados brasileira - Lei nº 13.709, de 14 de agosto de 2018 –, em seu artigo 4º, inciso III, *a* e *d*, incumbiu ao legislador infraconstitucional incumbiu de edificar um diploma legal sobre o tratamento de dados pessoais para fins de “segurança pública” e “atividades de investigação e repressão de infrações penais”.

O Presidente da Câmara dos Deputados instituiu *Comissão de Juristas* para a elaboração do anteprojeto com esse desiderato. Em 05 de novembro de 2020, a Comissão entregou ao Presidente da Câmara dos Deputados o “Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal”¹.

Em sua *exposição de motivos*, a *Comissão* frisou a busca por *equilíbrio* entre a proteção dos direitos fundamentais e a eficiência das intervenções estatais no âmbito da segurança pública e persecução penal e ressaltou a inspiração em regimes jurídicos com modernos e avançados níveis de amadurecimento sobre o tema, como, no ponto aqui em destaque, a Diretiva nº 680/2016 da União Europeia.

A opção pela Diretiva (UE) 2016/680 como principal *fonte de inspiração* para a elaboração do anteprojeto foi *adequada*, eis que a Europa vem desenvolvendo a proteção de dados desde pelo menos a década de 80. Outrossim, a convergência com o *padrão europeu* sobre a proteção *adequada* de dados abrirá espaço para o intercâmbio e cooperação com as autoridades europeias.

A adoção das balizas europeias para a proteção de dados, entretanto, exige um esforço para que ocorra um processo de **tradução** do referido regime jurídico ao ordenamento jurídico brasileiro, ou seja, um processo de adaptação às características do sistema jurídico pátrio. O legislador infraconstitucional, nesse ponto, está vinculado à formatação conferida pelo poder constituinte e deverá respeitar os parâmetros e limites constitucionais impostos pela Carta Republicana.

O anteprojeto apresentado à Câmara dos Deputados apresenta **lacunas estruturais** em relação ao sistema adotado na Europa, no que respeita ao

¹ Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica>.

equilíbrio entre a proteção de dados e a eficiência da persecução penal, o respeito à separação de poderes, a instituição de salvaguardas para a garantia da independência do Ministério Público e da Magistratura, a independência da Autoridade de Controle, segurança jurídica, dentre outras.

Ademais, é oportuno ressaltar que a Diretiva europeia é um *ponto de convergência* – não vinculante - no âmbito da União Europeia para a busca de uma *identidade supranacional* no tratamento de dados. Os países membros da União Europeia já ostentam legislações nacionais disciplinando amplamente a temática.

O Brasil, a despeito de possuir legislação atinente a inúmeras possibilidades de intervenções estatais sobre a temática (interceptações telefônicas e telemáticas, etc.), ainda carece de *lei* dispondo sobre diversas espécies de intervenções sobre dados pessoais, mormente uma *sistematização normativa* apta a conferir *segurança jurídica* em face da forma fragmentária com que a matéria é disposta no ordenamento jurídico.

O empenho da Diretiva europeia em busca de uniformização é *limitado*, eis que **não exaure o tema**, já que existem **ressalvas para o Estado-membro dispor em seu âmbito interno sobre aspectos materiais** atinentes ao sistema de justiça criminal e a **intervenção do Estado no âmbito de direitos fundamentais dos seus cidadãos**.

Logo, é necessário que a construção do referido projeto legal brasileiro encampe essas duas questões:

- i) preenchimento das *lacunas estruturais* omitidas do modelo europeu, sobretudo as salvaguardas para a separação de poderes e independência dos órgãos do sistema de justiça;
- ii) avanço sobre a regulamentação da intervenção estatal sobre os dados pessoais, observando-se: a) o sistema constitucional brasileiro, as suas peculiaridades, necessidades e o seu correspondente arcabouço legal e jurisprudencial já consolidado em aspectos importantes da intervenção estatal no âmbito dos direitos fundamentais; b) a necessidade de preencher as *lacunas legislativas preexistentes*.

A presente análise traz apenas uma reflexão preliminar e abrangerá *principalmente* a comparação do *anteprojeto* apresentado com: i) o texto constitucional brasileiro; ii) a jurisprudência do Supremo Tribunal Federal; iii) a Diretiva (UE) 2016/680; e iv) a legislação portuguesa.

A futura lei não poderá esvaziar as funções constitucionais exercidas pelo Ministério Público e Judiciário, tampouco criar um ambiente de **ingerência externa** nas atividades investigativas e processuais penais, mormente pelos exercentes dos poderes majoritários do Estado.

A futura lei não poderá criar um espaço de **imunidade** para o desempenho de práticas ilícitas e tornar-se um mecanismo eficiente para a perpetuação dos abusos dos poderes políticos e econômicos, maiores detratores da concretização do projeto constitucional brasileiro.

A presente *Nota Técnica* possui esses desideratos: apontar *reflexões preliminares* sobre lacunas em relação a *aspectos estruturais* do sistema adotado pela União Europeia pela Diretiva 2016/680, bem como demonstrar as possibilidades constitucionais brasileiras neste processo legislativo de construção da regulamentação sobre as intervenções estatais no âmbito da proteção de dados, com o intuito de pluralizar o debate e os pontos de vista sobre o tema e abrir espaço para o diálogo construtivo da legislação.

2. OBJETIVO DA LEGISLAÇÃO

O sistema europeu busca *equilibrar* a proteção de dados e a *eficiência* da persecução penal.

A definição adequada do *objetivo* da legislação é importante, eis que serve de viés valorativo para a construção coerente do referido regime jurídico.

O *objetivo* da lei deve abranger a conjunção de dois fatores: i) garantir uma proteção *adequada* aos dados pessoais; ii) instituir parâmetros para o tratamento de dados pessoais pelo Estado, aptos a exercer com *eficiência* e *segurança jurídica* as suas competências e atribuições constitucionais e legais, na melhor medida possível para o atendimento ao interesse público.

O legislador deve ter como *meta* o *equilíbrio* necessário para que o tratamento de dados pessoais obtenha o maior proveito à sociedade e ao titular do dado, maximizando os direitos individuais, com uma proteção adequada dos dados pessoais durante todo o seu *iter*, porém, sem tornar ineficiente à atuação estatal com a restrição indevida sobre o tratamento de dados.

Nesse sentido, oportuna menção à **Diretiva 2016/680** da União Europeia:

DIRETIVA (UE) 2016/680 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativa à **proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais** pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à **livre circulação desses dados**, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho

Considerando o seguinte: [...]

(4) A **livre circulação** de dados pessoais entre as autoridades competentes 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 a nível da União, e a sua transferência para países terceiros e organizações internacionais **deverão ser facilitadas, assegurando simultaneamente um elevado nível de proteção dos dados pessoais**. Este contexto obriga ao estabelecimento de um **regime de proteção de dados pessoais sólido** e mais coerente na União, apoiado por uma aplicação rigorosa das regras.

(93) Atendendo a que os **objetivos da presente diretiva**, a saber, **proteger os direitos e liberdades fundamentais das pessoas singulares**, nomeadamente o seu direito à proteção de dados pessoais, e **assegurar o livre intercâmbio desses dados pelas autoridades competentes na União**, [...]

CAPÍTULO I Disposições gerais Artigo 1.º Objeto e objetivos

[...]

2. Nos termos da presente diretiva, os Estados-Membros asseguram:

a) A **proteção dos direitos e das liberdades fundamentais das pessoas singulares** e, em especial, o seu direito à **proteção dos dados pessoais**; e

b) Que o **intercâmbio de dados pessoais** entre autoridades competentes na União, caso seja previsto pelo direito da União ou do Estado-Membro, **não seja limitado nem proibido por razões relacionadas com a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais**.

Em Portugal, a **Lei n.º 59/2019 de 8 de agosto**, que transpõe ao direito interno a **Diretiva (UE) 2016/680**, adotou a mesma sistemática.

Artigo 2.º

Âmbito de aplicação [...]

4 — O intercâmbio de dados pessoais entre autoridades competentes na União Europeia, quando legalmente exigido, não é limitado nem proibido por razões relacionadas com a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais.

Artigo 69.º

Sistema integrado de informação criminal

O disposto na presente lei **não implica qualquer restrição ou limitação na partilha e intercâmbio de dados entre os órgãos de polícia criminal e destes com as autoridades judiciais**, no âmbito do dever de cooperação estabelecido na lei de organização da investigação criminal, designadamente do **sistema integrado de informação criminal** instituído nos termos da Lei n.º 73/2009, de 12 de agosto, alterada pela Lei n.º 38/2015, de 11 de maio.

O anteprojeto brasileiro, todavia, ao contrário do sistema europeu, estabelece como **objetivo único** a proteção de dados pessoais.

CAPÍTULO I DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais realizado por autoridades competentes para atividades de segurança pública e de persecução penal, com o **objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural**.

A visão *restritiva* adotada no *anteprojeto* é verificada em seus **fundamentos**.

Art. 2º A disciplina da proteção de dados pessoais em atividades de segurança pública e de persecução penal tem como **fundamentos**:

I - a dignidade, os direitos humanos, o livre desenvolvimento da personalidade, e o exercício da cidadania pelas pessoas naturais;

II - a autodeterminação informativa;

III - o respeito à vida privada e à intimidade;

IV - a liberdade de manifestação do pensamento, de expressão, de informação, de

comunicação e de opinião;

V - a presunção de inocência;

VI - confidencialidade e integridade dos sistemas informáticos pessoais; e

VII - garantia do devido processo legal, da ampla defesa, do contraditório, da motivação e da reserva legal.

A ótica *restritiva* em relação aos *fundamentos* do anteprojeto é observada em análise comparativa inclusive com a **Lei nº 13.709/2018 - Lei Geral de Proteção de Dados brasileira**, que buscou instituir *equilíbrio* entre a proteção de dados pessoais e o **desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa e a livre concorrência**, *in verbis*:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o **desenvolvimento econômico e tecnológico e a inovação**;

VI - a **livre iniciativa, a livre concorrência** e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A instituição do **objetivo único** é prejudicial, eis que **as atividades de segurança pública e persecução penal possuem como objetivos a tutela e garantia de direitos e garantias fundamentais do cidadão**. A *preferência irrestrita e abstrata* da proteção de dados em prejuízo dos demais direitos e interesses em conflito é *desproporcional e inconstitucional*, eis que cria uma preferência *genérica e prima facie* de um direito fundamental sobre os demais e, por consequência, um espaço de ineficiência ao dever de proteção estatal.

As **intervenções estatais** no âmbito dos direitos fundamentais do cidadão deverão ser **proporcionais**, leia-se, **suficientes para atender a direito em conflito com idêntico status constitucional**, vedando-se o **excesso** e a **proteção insuficiente**.

Não atende ao equilíbrio:

1º. por violação à proteção de dados: um espaço irrestrito de obtenção e compartilhamento de bancos de dados, mormente transmissão daqueles sigilosos, sem controle sobre a *finalidade* do seu tratamento e procedimentos para controlar os riscos dos manejos das informações;

2º. por violação à eficiência: limitações e proibições ao tratamento de dados, isolando os órgãos de segurança, inteligência e persecução penal em verdadeiras “ilhas”, prejudicando a intercomunicabilidade e a atuação conjunta em seus âmbitos de atribuições.

O objeto da lei, portanto, deverá ser *regulamentar* e estabelecer *parâmetros* para a *intervenção estatal* no âmbito dos direitos informacionais do cidadão, com a conciliação sobre a proteção dos dados e a sua circulação eficiente. Os princípios de tratamento servem para destinar as informações *suficientes* para a sua *finalidade legítima*.

3. ALTO NÍVEL DE PROTEÇÃO E COMPARTILHAMENTO DE DADOS: DADOS SIGILOSOS E DADOS SENSÍVEIS.

3.1. Limites constitucionais: privacidade, autonomia informacional e a proteção de dados

A análise do âmbito de proteção de um direito fundamental deve partir do **texto constitucional**.

A Constituição Federal, ao estipular em seu artigo 5º, inciso X, bem como no inciso XII, primeira parte, o **direito à privacidade** e a tutela dos demais **meios de comunicação**, ou seja, **correspondência, telegrafia e dados**, não estipulou *cláusula de reserva jurisdicional*.

Em igual sentido a **autodeterminação informacional**, extraída da concepção de direito *geral* da personalidade, em interpretação conjunta entre o direito à privacidade (inciso X), a inviolabilidade da comunicação de dados (inciso XII) e o *habeas data* (inciso LXXII, *alíneas a e b*).

Em uma **primeira conclusão** extraída do texto constitucional, com ressalva às *comunicações telefônicas* e ao *domicílio*, a Constituição Republicana não fixou *cláusula de reserva jurisdicional* para a redução do seu âmbito de aplicação.

3.2. Flexibilização do direito fundamental por lei *proporcional*

“No entanto, as restrições aos direitos fundamentais não decorrem *apenas* das possibilidades advindas das previsões *expressamente* existentes no texto constitucional, ou as competências ostensivamente atribuídas aos poderes constituídos no âmbito da própria definição do direito. Isso porque, a referida técnica não resolveria as inúmeras colisões entre direitos fundamentais que, por sua vez, não ostentam caráter absoluto”. Com fundamento no direito geral de liberdade (artigo 5º, inciso II, CRFB/1988), “o *poder legislativo* poderá e, antes até mesmo deverá conformar os direitos e interesses constitucionais contrapostos em sua atividade legiferante, mesmo sem uma expressa previsão constitucional quanto a possibilidade de sua intervenção naquela espécie de direito ou garantia”².

Essa assertiva é, em regra, aceita em inúmeros instrumentos internacionais de *proteção de direitos humanos*, desde que prevista em *lei* e observado o *princípio da proporcionalidade*, e que seja *necessária* à efetividade do interesse público ou a proteção dos direitos e liberdades de terceiros.

Nesse sentido:

a) artigo 52º, 1., Carta dos Direitos Fundamentais da União Europeia – (2000/C 364/01):

1. Qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela presente Carta deve ser prevista por **lei** e respeitar o **conteúdo essencial desses direitos e liberdades**. Na observância do princípio da **proporcionalidade**, essas restrições só podem ser introduzidas se forem **necessárias** e corresponderem efectivamente a objectivos de **interesse geral** reconhecidos pela União, ou à necessidade de **protecção dos direitos e liberdades de terceiros**.

b) artigo 29, 1 e 2, da Declaração Universal dos Direitos Humanos da ONU;

1.O indivíduo tem **deveres** para com a comunidade, fora da qual não é possível o livre e pleno desenvolvimento da sua personalidade.

² GABRIEL DE SOUZA, João Paulo. Os parâmetros entre a tutela da privacidade e o dever de comunicação de ilícitos aos órgãos de persecução penal. Escola Superior do Ministério Público do Estado de São Paulo, São Paulo, 2020.

2.No exercício deste direito e no gozo destas liberdades ninguém está sujeito senão às limitações estabelecidas pela **lei** com vista exclusivamente a promover o reconhecimento e o respeito dos **direitos e liberdades dos outros** e a fim de satisfazer as **justas exigências** da moral, da **ordem pública** e do **bem-estar** numa sociedade democrática.

c) artigo 32, da Convenção Americana de Direitos Humanos, etc.

As restrições permitidas, de acordo com esta Convenção, ao gozo e exercício dos direitos e liberdades nela reconhecidos, não podem ser aplicadas senão de acordo com **leis** que forem promulgadas por motivo de **interesse geral** e com o propósito para o qual houverem sido estabelecidas.

O **Supremo Tribunal Federal** já adotou esse posicionamento em inúmeros julgados atinente as restrições sobre o âmbito de proteção da privacidade e personalidade em relação ao tratamento de dados pessoais, reconhecendo a possibilidade de restrição via legislativa, observada a proporcionalidade.

O Supremo Tribunal Federal também enfrentou a temática em julgados mais recentes, no ano de 2020, como no julgamento conjunto da **Medida Cautelar nas Ações Diretas de Constitucionalidade nº 6387, 6388, 6389, 6390 e 6393** (IBGE), **proferida pela Ministra Rosa Weber** (data do julgamento 24/04/2020), posteriormente **referendada pelo Pleno**, e no julgamento da **Medida Cautelar da Arguição de Descumprimento de Preceito Fundamental nº 695** (SERPRO e ABIN) **pelo Ministro Gilmar Mendes** (data do julgamento 24/06/2020).

[...] “Desde a concepção do direito à privacidade como manifestação do direito à autodeterminação informacional pela Corte Constitucional alemã, já se reconhece que o princípio da proporcionalidade desempenha relevante papel de aferição da constitucionalidade das interferências à proteção jurídica da autodeterminação informacional. O teste da proporcionalidade, a propósito, foi central na construção realizada pelo BVerfG a partir do julgamento da Lei do Censo de 1983”. (ADPF 695, Medida Cautelar, Voto Gilmar Mendes.)

As intervenções estatais no âmbito da autonomia informacional deverão ser proporcionais, excepcionais e atender a interesse com *status constitucional*.

3.3. Aumento da proteção legislativa: cláusula *legal* de reserva jurisdicional

Por outro lado, o legislador infraconstitucional brasileiro poderá conferir um alto nível de proteção aos dados pessoais agregando a determinadas circunstâncias a *cláusula de reserva de jurisdição*, ainda que não exigida pela Constituição. Esses

casos, no entanto, deverão circundar aquelas circunstâncias em que: i) houver um alto grau de expectativa do titular dos dados sobre o sigilo; ii) e/ou um alto potencial lesivo sobre a sua circulação.

Nesse sentido, oportuna menção à Diretiva **2016/680** da União Europeia:

3. A presente diretiva não obsta a que os Estados-Membros prevejam **garantias mais elevadas** do que as nela estabelecidas para a proteção dos direitos e liberdades do titular dos dados no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes.

O legislador infraconstitucional já adotou essa cautela em diversas circunstâncias, como pode ser exemplificado nas seguintes hipóteses:

- a) fluxo de comunicações em sistemas de informática e telemática (artigo 1º, parágrafo único, da Lei nº 9.296, de 24 de julho de 1996);
- b) inviolabilidade e sigilo do fluxo de comunicações pela internet, e das comunicações privadas armazenadas (artigo 7º, incisos II e III, da Lei nº 12.965, de 23 de abril de 2014).

3.4. Transmissão de dados sigilosos sem prévia autorização judicial

No entanto, a *cláusula de reserva de jurisdição* instituída por lei **não** deverá abranger irrestritamente todos os casos inerentes a dados sigilosos ou sensíveis, sob pena de conferir *prima facie* a preferência de um direito fundamental sobre o outro e nulificar a eficiência da segurança pública e da persecução penal.

Atividades com alto risco de desenvolvimento de práticas ilícitas *fomentam* uma maior fiscalização – vigilância, *surveillance* - pelo Poder Público, em especial em âmbito preventivo, como por exemplo, aquelas reconhecidas em âmbito internacional como condutas típicas de lavagem de capitais (Grupo de Ação Financeira Internacional – GAFI (*Financial Action Task Force* (FATF³)).

Nesse espeque, as atividades inerentes à segurança pública e persecução penal, a despeito de não se sobreporem, possuem *pontos inafastáveis* de convergência. Existindo *norma autorizativa* da intervenção estatal, como no caso da coleta de dados pelo COAF (primeira intervenção) e o compartilhamento posterior com o Ministério Público (segunda intervenção), o controle judicial deverá ser a

³ <http://www.fatf-gafi.org/about>

posteriori, eis que há uma justificativa *prima facie* apta a excepcionar a autonomia informacional.

O Supremo Tribunal Federal já reconheceu a legitimidade – inclusive em sede de controle concentrado de constitucionalidade – do compartilhamento de dados sigilosos sem autorização judicial prévia entre os órgãos públicos. A Corte constitucional reconheceu que não há propriamente a quebra de sigilo, mas “**uma transferência de dados sigilosos de um determinado portador, que tem o dever de sigilo, para outro, que mantém a obrigação de sigilo, permanecendo resguardadas a intimidade e a vida privada**” (STF, 2016⁴). Isso porque, o dever de sigilo é transmitido em conjunto com as informações sigilosas.

A título exemplificativo, o Supremo Tribunal Federal já ratificou a constitucionalidade das seguintes hipóteses:

a) no julgamento conjunto das **Ações Diretas de Constitucionalidade nº 2.390, 2.386, 2.397 e 2.859**, reconheceu a constitucionalidade dos *artigos 5º e 6º da Lei Complementar nº 105/2001*⁵ e seus decretos regulamentadores, que disciplinam o intercâmbio de informações financeiras sigilosas dos cidadãos pelas instituições financeiras com a Administração tributária e sua Procuradoria, *à revelia de autorização judicial*.

b) no julgamento do **Recurso Extraordinário nº 1.055.941**, o **Supremo Tribunal Federal** foi convocado a decidir e novamente reconheceu a constitucionalidade do compartilhamento de dados pessoais *bancários e fiscais*, tutelados pelo sigilo constitucional, agora, com os órgãos da persecução penal, sem prévia autorização judicial. A hipótese abrangia o compartilhamento de informações oriundas do COAF⁶, bem como aquelas comunicadas pela Administração tributária⁷, ambas, em circunstâncias de averiguação preliminar de ocorrência de

⁴ Dispôs ainda, *in verbis*: “O art. 1º da Lei Complementar 104/2001, no ponto em que insere o § 1º, inciso II, e o § 2º ao art. 198 do CTN, não determina quebra de sigilo, mas transferência de informações sigilosas no âmbito da Administração Pública. Outrossim, a previsão vai ao encontro de outros comandos legais já amplamente consolidados em nosso ordenamento jurídico que permitem o acesso da Administração Pública à relação de bens, renda e patrimônio de determinados indivíduos”.

⁵ A Lei Complementar nº 105, de 10 de janeiro de 2001 dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.

⁶ A Lei nº 9.613, de 03 de março de 1998, determinou em seu artigo 15 que: *O COAF comunicará às autoridades competentes para a instauração de procedimentos cabíveis, quando concluir pela existência de crimes previstos nesta Lei, de fundados indícios de sua prática, ou de qualquer outro ilícito.*

⁷ Nesse sentido dispõe a Lei Complementar nº 105, de 10 de janeiro de 2001 em seu artigo 1º, §3º, inciso IV, artigo 9º *In verbis*: Art. 1º, § 3º Não constitui violação do dever de sigilo: IV – a comunicação, às autoridades competentes, da prática de ilícitos penais ou administrativos, abrangendo o fornecimento de informações sobre operações que envolvam recursos provenientes de qualquer prática criminosa. E ainda: Art. 9º Quando, no exercício de suas atribuições, o Banco Central do Brasil e a Comissão de Valores Mobiliários verificarem a ocorrência de crime definido em lei como de ação pública, ou indícios da prática de tais crimes, informarão ao Ministério Público, juntando à comunicação os documentos necessários à apuração ou comprovação dos fatos

infrações penais (*Repercussão geral de questão constitucional no Recurso Extraordinário nº 1.055.941*).

A posição do Supremo Tribunal Federal, inclusive, originou a **Tese de Repercussão Geral nº 990**, que será abordada em oportuno.

Tese de Repercussão Geral nº 990:

1. É constitucional o 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, **devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional.**

[...]

Exemplifica-se, ainda, neste ponto, a **Lei nº 13.344, de 2016**, que alterou o **Código de Processo Penal** e permitiu ao Ministério Público e Polícia Judiciária, excepcionalmente, no caso de tráfico de pessoas, requisitarem diretamente às “empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso, com imediata comunicação ao juiz”, quando o juiz não julgar o pedido no prazo de 12 (doze) horas (artigo 13, §3^a).

3.5 Formalização e controle sobre a finalidade do tratamento

A proteção da *personalidade* e da *autodeterminação informacional* exigem que o dado pessoal seja protegido durante todo o *percurso* do seu tratamento.

Com isso, assume importância significativa não apenas as formas de obtenção do dado, mas também o estabelecimento de um *procedimento* para a garantia da *adequação* do tratamento dos dados às *finalidades* para as quais eles foram coletados ou compartilhados.

O Supremo Tribunal Federal, na **Tese de Repercussão Geral nº 990**, instituiu essas balizas procedimentais para a transferência de dados entre COAF, Receita Federal e os órgãos de persecução penal, *in verbis*:

Tese de Repercussão Geral nº 990:

[...]

2. O compartilhamento pela UIF e pela RFB, referente ao item anterior, deve ser feito unicamente por meio de **comunicações formais, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios**, vencido o Ministro Marco Aurélio, que não referendava a tese. Presidência do Ministro Dias Toffoli. Plenário, 04.12.2019.

3.6. Sistema *interoperável* para o tratamento de dados pessoais

Sem descurar dos limites da transmissão de dados, a instituição – na **medida do possível** - de um *sistema eletrônico interoperável das plataformas de dados digitais* poderá contribuir para, a um só tempo, garantir a eficiência na gestão do dado, especialmente o sigiloso e o sensível, e proporcionar um alto nível de proteção, especialmente do dado sigiloso, com registros de acessos pessoais, controle sobre a finalidade e, inclusive, a possibilidade de controle *a posteriori*.

Permite o atendimento aos princípios da *finalidade*⁸, *segurança*⁹, *prevenção*¹⁰ e a *responsabilização e prestação de contas*¹¹, imprescindíveis para o tratamento de dados pessoais.

Sobre o sistema interoperável, cita-se, na experiência brasileira:

- a) no âmbito da **segurança pública**, a **Lei nº 13.675, de 11 de junho de 2018**¹² que estabeleceu como diretriz do *Sistema Único de Segurança Pública* a “**sistematização e compartilhamento das informações de**

⁸ Art. 6º [...] I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

⁹ Art. 6º [...] VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

¹⁰ Art. 6º [...] VII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

¹¹ Art. 6º [...] X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

¹² Disciplina a organização e o funcionamento dos órgãos responsáveis pela segurança pública, nos termos do § 7º do art. 144 da Constituição Federal; cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS); institui o Sistema Único de Segurança Pública (Susp)”

segurança pública, prisionais e sobre drogas, em âmbito nacional¹³ entre os seus órgãos, inclusive com o “**Sistema Brasileiro de Inteligência (Sisbin)¹⁴**”, com possibilidade de “**acesso recíproco aos bancos de dados¹⁵**”.

- b) a **Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados** previu expressamente em seu *Capítulo IV – Do tratamento de dados pessoais pelo Poder Público* – que “**os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado¹⁶**” e que este compartilhamento deverá atender “**a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas**”, inclusive permitiu, excepcionalmente, o compartilhamento com “entidades privadas”;
- c) **Resolução nº 335, de 29 de setembro de 2020, do Conselho Nacional de Justiça**, que institui política pública para a governança e a gestão de processo judicial eletrônico. Integra os tribunais do país com a criação da Plataforma Digital do Poder Judiciário Brasileiro – PDPJ-Br.

Portugal

A **Lei nº 34, de 2009 de Portugal**, que *estabelece o regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial*, ainda vigente, prevê não apenas a possibilidade de intercâmbio de dados entre os sistemas públicos, como apresenta um rol *exemplificativo* sobre as entidades que poderão dialogar com o sistema judicial (Judiciário e Ministério Público).

CAPÍTULO V

Intercâmbio de dados com outros sistemas

Artigo 37.º

Comunicação de dados com outros sistemas

1 — Para os efeitos previstos na lei, pode haver comunicação de dados, por meios electrónicos, com os seguintes sistemas:

- a) Dos órgãos de polícia criminal; b) Do Serviço de Estrangeiros e Fronteiras; c) Da Autoridade de Segurança Alimentar e Económica; d) Da Autoridade Nacional de Segurança Rodoviária; e) Dos órgãos e serviços da administração local; f) Dos serviços da administração fiscal; g) Das instituições da segurança social; h) Da identificação civil; i) Do

¹³ Artigo 5º, inciso VIII;

¹⁴ Art. 10, inciso IV;

¹⁵ Art. 10, §4º;

¹⁶ Art. 25 Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

registo automóvel; j) Do registo comercial; l) Do registo criminal e de contumazes; m) Do registo nacional de pessoas colectivas; n) Do registo predial; o) Dos serviços prisionais; p) Da reinserção social; q) Da Ordem dos Advogados; r) Da Câmara dos Solicitadores; e s) Das demais entidades que colaborem com o sistema de justiça no âmbito dos processos judiciais, designadamente os fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações e as entidades com competência para a realização de perícias, redacção de pareceres técnico-científicos, elaboração do relatório social e verificação do cumprimento de injunções, penas substitutivas e sanções acessórias.

O rol, como dito, é **exemplificativo**, pois expressamente previsto que ele “não prejudica a comunicação de dados com outros sistemas” (artigo 38º e 39º¹⁷).

A sistemática é interessante, eis que traz um grau de *segurança jurídica mínima* e ao mesmo tempo *não engessa* ou *exaure* as possibilidades de intercâmbio de dados pessoais.

Por outro turno, o sistema legal português ainda privilegia, na medida do possível, que a comunicação de dados ocorra por meios eletrônicos.

CAPÍTULO V

Intercâmbio de dados com outros sistemas

Artigo 37.º

Comunicação de dados com outros sistemas

[...]

4 — Sempre que as condições técnicas o permitam, a comunicação de dados aos magistrados e funcionários de justiça que os coadjuvam pelos órgãos de polícia criminal e pelas demais entidades que colaborem com o sistema de justiça no âmbito da investigação e dos processos judiciais efectua -se por meios electrónicos.

¹⁷ Artigo 38.º

Acesso a dados constantes de outros sistemas

Os magistrados e os funcionários de justiça que os coadjuvam podem aceder aos dados constantes dos sistemas previstos no n.º 1 do artigo anterior para fins de identificação, localização ou contacto actualizados, em condições de segurança, celeridade e eficácia:

a) De quaisquer intervenientes em processos jurisdicionais e da competência do Ministério Público;
b) Da situação processual dos arguidos em processo penal;
c) De bens.

Artigo 39.º

Outros sistemas

O disposto nos artigos 37.º e 38.º não prejudica a comunicação de dados com outros sistemas, nem o acesso aos dados de outros sistemas, nos termos da Lei da Protecção de Dados Pessoais, aprovada pela Lei n.º 67/98, de 26 de Outubro.

5 — A comunicação de dados nos termos do número anterior dispensa o seu envio em suporte físico, sem prejuízo da possibilidade de os magistrados competentes para o processo a que respeitam o determinarem, quando o mesmo seja necessário para assegurar a finalidade para que os dados foram comunicados.

Em **Portugal**, há o denominado *sistema integrado de informação criminal*, regido pela **Lei nº 73, de 12 de agosto de 2009** que busca a “implementação de uma plataforma para o intercâmbio de informação criminal que assegure uma efectiva interoperabilidade entre sistemas de informação dos órgãos de polícia criminal”.

4. AUTORIDADE DE CONTROLE: CONTORNOS CONSTITUCIONAIS

O *anteprojeto* não observou inúmeras balizas instituídas pelo *regime europeu*, especialmente a garantia da independência do Judiciário e do Ministério Público.

4.1. Função NÃO jurisdicional. Separação dos poderes. Independência do Judiciário e Ministério Público em suas funções típicas.

A Autoridade de Controle **não** possui atribuição sobre as atividades *jurisdicionais* do Ministério Público e do Judiciário, ou seja, não possui atribuição sobre atos praticados em investigações e processos criminais por autoridades independentes.

Os referidos atos são controlados conforme as regras do *processo penal*, mediante o respeito ao devido processo legal e ao juiz e promotor naturais.

Em outras palavras, a *Autoridade de Controle* não analisará o tratamento de dados em investigações criminais e processos penais, notadamente, elementos de informação e provas. Essa função incumbe ao *juiz natural*, órgão imparcial, independente e com competência constitucional e legal para a análise sobre a sua licitude.

Entendimento em contrário consagraria violação à separação dos poderes, à independência do Judiciário e do Ministério Público, além de permitir o poder revisional no processo penal brasileiro por uma autoridade administrativa.

Essa *salvaguarda* foi consagrada no direito europeu.

Nesse sentido, oportuna menção à Diretiva **2016/680** da União Europeia:

DIRETIVA (UE) 2016/680 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à **livre circulação desses dados**, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho

Considerando o seguinte: [...]

20) A presente diretiva não obsta a que os Estados-Membros especifiquem as operações e os procedimentos de tratamento na **legislação processual penal nacional** no que se refere ao **tratamento de dados pessoais pelos tribunais e as outras autoridades judiciais**, em particular no que respeita aos dados pessoais que constem de uma decisão judicial ou de um registo relacionado com uma ação penal.

80) Embora a presente diretiva se aplique também às atividades dos tribunais nacionais e outras autoridades judiciais, **a competência das autoridades de controlo não deverá abranger o tratamento de dados pessoais efetuado pelos tribunais no exercício da sua função jurisdicional, a fim de assegurar a independência dos juízes no desempenho das suas funções jurisdicionais**. Esta exceção deverá ser estritamente limitada às atividades judiciais relativas a processos judiciais, não se aplicando a outras atividades a que os juízes possam estar associados por força do direito do Estado-Membro. Os Estados-Membros podem também prever a possibilidade de a **competência das autoridades de controlo não abranger o tratamento de dados pessoais efetuado por outras autoridades judiciais independentes no exercício da sua função jurisdicional, nomeadamente o Ministério Público**. Em todo o caso, o cumprimento das regras da presente diretiva pelos tribunais e outras autoridades judiciais independentes **deverá ficar sempre sujeito a uma fiscalização independente nos termos do artigo 8.o, n.o 3, da Carta**.

Secção 2 - Competência, atribuições e poderes

Artigo 45.º - Competência

1.Os Estados-Membros preveem que a respetiva autoridade de controlo seja competente para, no respetivo território, exercer as atribuições e os poderes que lhe são conferidos pela presente diretiva.

2.Os Estados-Membros preveem que a respetiva autoridade de controlo **não seja responsável pela supervisão de operações de tratamento efetuadas pelos tribunais no exercício da sua função jurisdicional**. Os Estados-Membros podem estabelecer que a respetiva autoridade de controlo **não tenha competência para supervisionar operações de tratamento efetuadas por outras autoridades judiciais independentes no exercício da sua função jurisdicional**.

Em Portugal, a **Lei n.º 59/2019 de 8 de agosto**, que transpor ao direito interno a **Diretiva (UE) 2016/680** adotou a mesma sistemática.

CAPÍTULO VI - **Autoridade de controlo**

Artigo 43.º - **Autoridade de controlo**

1 — Incumbe à CNPD a garantia e fiscalização do cumprimento da presente lei.

2 — O disposto do número anterior **não se aplica ao tratamento de dados pessoais efetuado pelos tribunais e pelo Ministério Público no exercício das suas competências processuais**.

3 — Para efeitos do n.º 1, a CNPD integra um magistrado judicial, designado pelo Conselho Superior da Magistratura, e um magistrado do Ministério Público, designado pelo Conselho Superior do Ministério Público.

4 — Cabe exclusivamente aos magistrados a que se refere o número anterior, sem prejuízo das competências do presidente da CNPD, o exercício das atribuições da CNPD que impliquem o acesso a dados objeto de tratamento ou aos registos cronológicos das operações de tratamento.

Aliás, a **Lei n.º 59/2019 de 8 de agosto**, a despeito de transpor ao direito interno a **Diretiva (UE) 2016/680**, ressaltou que o tratamento de dados em âmbito jurisdicional ainda continua a ser regulado pela **Lei nº 34, de 2009 de Portugal**, que *estabelece o regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial, verbis*:

Artigo 68.º

Dados referentes ao sistema judiciário

1 — O tratamento de dados constante de processo penal, de decisão judicial ou do registo criminal é regulado nos termos da lei processual penal.

2 — Ao tratamento de dados referentes ao sistema judicial é aplicável o regime jurídico próprio, constante da Lei n.º 34/2009, de 14 de julho.

A Constituição brasileira também **não admite** à intervenção de autoridades *administrativas* – como o Conselho Nacional de Justiça e o Conselho Nacional do Ministério Público - sobre a *função típica*, precípua (atividade fim) desenvolvida pelas autoridades *independentes* do Ministério Público e do Judiciário.

A assertiva foi referendada pelo **Supremo Tribunal Federal** em sede de controle concentrado de Constitucionalidade, em específico, no julgamento:

i) Ação Direta de Inconstitucionalidade nº 3.367:

2. INCONSTITUCIONALIDADE. Ação direta. Emenda Constitucional nº 45/2004. Poder Judiciário. **Conselho Nacional de Justiça**. Instituição e disciplina. **Natureza meramente administrativa. Órgão interno de controle administrativo, financeiro e disciplinar da magistratura.** Constitucionalidade reconhecida. **Separação e independência dos Poderes.** História, significado e alcance concreto do princípio. Ofensa a cláusula constitucional imutável (cláusula pétreia). Inexistência. **Subsistência do núcleo político do princípio, mediante preservação da função jurisdicional, típica do Judiciário, e das condições materiais do seu exercício imparcial e independente.** Precedentes e súmula 649. Inaplicabilidade ao caso. Interpretação dos arts. 2º e 60, § 4º, III, da CF. Ação julgada improcedente. Votos vencidos. São constitucionais as normas que, introduzidas pela Emenda Constitucional nº 45, de 8 de dezembro de 2004, **instituem e disciplinam o Conselho Nacional de Justiça, como órgão administrativo do Poder Judiciário nacional.**

[...]

4. PODER JUDICIÁRIO. Conselho Nacional de Justiça. **Órgão de natureza exclusivamente administrativa.** Atribuições de controle da atividade administrativa, financeira e disciplinar da magistratura. [...]

ii) Ação Direta de Inconstitucionalidade nº 4.638:

(...) esta Suprema Corte em distintas ocasiões já afirmou que o CNJ não é dotado de competência jurisdicional, sendo mero órgão administrativo. Assim sendo, a Resolução 135, ao classificar o CNJ e o CJF de "tribunal", (...) simplesmente disse – até porque mais não poderia dizer – que as normas que nela se contêm aplicam-se também aos referidos órgãos. [ADI 4.638 MC-REF, rel. min. Marco Aurélio, voto do min. Ricardo Lewandowski, j. 8-2-2012, P, DJE de 30-10-2014.]

Em outras palavras, a *Autoridade de Controle* não analisará o tratamento de dados em investigações criminais e processos penais, notadamente, com caráter probatório. Essa função incumbe ao *juiz natural*.

A *Autoridade de Controle* também não poderá – sob a pretensão de analisar tratamento de dados pessoais – analisar elementos de informação e provas inseridas em investigações criminais e processos penais, em especial, procedimentos e processos em sigilo.

Em Portugal, a **Lei n.º 59/2019 de 8 de agosto**, que transpôs ao direito interno a **Diretiva (UE) 2016/680**, adotou a mesma sistemática.

Artigo 19º

Direitos do titular dos dados em casos especiais

Os direitos de informação, de acesso, de retificação, de apagamento e de limitação do tratamento de dados pessoais constantes de um processo penal, de uma decisão judicial ou do registo criminal são exercidos nos termos da lei processual penal e da demais legislação aplicável.

4.2. Escolha do Conselho Nacional de Justiça como Autoridade de Controle. Função administrativa: poder normativo, fiscalizatório e sancionatório.

4.2.1. Autonomia administrativa do Ministério Público

Superada a questão pretérita, a Autoridade de Controle possuirá atribuições administrativas. No entanto, é necessário a filtragem constitucional.

O Ministério Público e o Poder Judiciário possuem *autonomia administrativa* (art. 99, *caput*, e art. 127, §2º, CRFB/1988).

A Constituição da República atribui o *controle da legalidade dos atos administrativos* do Poder Judiciário ao *Conselho Nacional de Justiça* e aos *Tribunais* e, no âmbito do Ministério Público, ao *Conselho Nacional do Ministério Público* e aos *Ministérios Públicos da União e dos Estados*.

A *Autoridade de Controle*, ao normatizar, fiscalizar e sancionar o tratamento de dados pessoais, **absorverá significativa atividade de controle de legalidade sobre os atos administrativos do Ministério Público.**

Logo, essa atividade não poderá ser transferida por via legislativa ao Conselho Nacional de Justiça, sob pena de *submissão completa* do Ministério Público ao Poder Judiciário.

Essa função deve estar em conformidade com a *garantia institucional* da *autonomia administrativa* do Ministério Público.

O **Supremo Tribunal Federal** já referendou a autonomia administrativa do Ministério Público frente aos poderes do Estado:

A alta relevância jurídico-constitucional do Ministério Público – qualificada pela outorga, em seu favor, da **prerrogativa da autonomia administrativa**, financeira e orçamentária – **mostra-se tão expressiva**, que essa instituição, embora sujeita à fiscalização externa do Poder Legislativo, com o auxílio do respectivo tribunal de contas, **dispõe de uma esfera própria de atuação administrativa, livre da ingerência de órgãos do Poder Executivo**, aos quais falece, por isso mesmo, competência para sustar ato do procurador-geral de justiça praticado com apoio na autonomia conferida ao *Parquet*. **A outorga constitucional de autonomia, ao Ministério Público, traduz um natural fator de limitação dos poderes dos demais órgãos do Estado, notadamente daqueles que se situam no âmbito institucional do Poder Executivo.** A dimensão financeira dessa autonomia constitucional – considerada a instrumentalidade de que se reveste – responde à necessidade de assegurar-se ao Ministério Público a plena realização dos fins eminentes para os quais foi ele concebido, instituído e organizado. (...) Sem que disponha de capacidade para livremente gerir e aplicar os recursos orçamentários vinculados ao custeio e à execução de suas atividades, o Ministério Público nada poderá realizar, frustrando-se, desse modo, de maneira indevida, os elevados objetivos que refletem a destinação constitucional dessa importantíssima instituição da República, incumbida de defender a ordem jurídica, de proteger o regime democrático e de velar pelos interesses sociais e individuais indisponíveis. **O Ministério Público – consideradas as prerrogativas constitucionais que lhe acentuam as múltiplas dimensões em que se projeta a sua autonomia – dispõe de competência para praticar atos próprios de gestão, cabendo-lhe, por isso mesmo, sem prejuízo da fiscalização externa, a cargo do Poder Legislativo, com o auxílio do tribunal de contas, e, também, do controle jurisdicional, adotar as medidas que reputar necessárias ao pleno**

e fiel desempenho da alta missão que lhe foi outorgada pela Lei Fundamental da República, sem que se permita ao Poder Executivo, a pretexto de exercer o controle interno, interferir, de modo indevido, na própria intimidade dessa instituição, seja pela arbitrária oposição de entraves burocráticos, seja pela formulação de exigências descabidas, seja, ainda, pelo abusivo retardamento de providências administrativas indispensáveis, frustrando-lhe, assim, injustamente, a realização de compromissos essenciais e necessários à preservação dos valores cuja defesa lhe foi confiada. [ADI 2.513 MC, rel. min. Celso de Mello, j. 3-4-2002, P, DJE de 15-3-2011.]

4.2.2. Impossibilidade de o Conselho Nacional de Justiça se ingerir na autonomia administrativa de outros poderes

Não se deve confundir as atividades *jurisdicionais* desempenhadas pelos órgãos do Poder Judiciário, com as atividades *administrativas* desempenhadas pelo Conselho Nacional de Justiça, que possui atribuição limitada no controle da legalidade de atos administrativos no âmbito do Poder Judiciário.

O CNJ não dispõe, constitucionalmente, de competência para deliberar sobre situações que alcancem ou que atinjam resoluções e manifestações volitivas emanadas de órgãos e autoridades vinculados a outros Poderes do Estado e, por isso mesmo, absolutamente estranhos ao âmbito de atribuições institucionais daquele órgão de controle meramente administrativo do Poder Judiciário, ainda que se trate de provimento de cargo de desembargador pela regra do quinto constitucional (CF, art. 94), pois, em tal hipótese, cuidando-se de procedimento subjetivamente complexo (RTJ 178/220 – RTJ 187/233-234 – RTJ 188/663, v.g.), o ato final de investidura pertence, exclusivamente, a agente público que chefia o Poder Executivo (CF, art. 94, parágrafo único). [MS 27.033 AgR, rel. min. Celso de Mello, j. 30-6-2015, 2ª T, DJE de 27-10-2015.]

5. CONCLUSÕES

A proposta de criação de uma nova legislação deverá:

5.1. Objetivo da Lei. Equilibrar a *alta proteção* de dados pessoais com a *eficiência* dos órgãos de persecução penal, evitando instituir limitações e proibições desproporcionais ao tratamento de dados e estabelecer balizas para a criação de um ambiente seguro para a circulação célere e adequada das informações, promovendo a integração entre os órgãos estatais, em benefício da sociedade e do titular dos dados;

5.2. Sobre os dados sigilosos e sensíveis.

5.2.1. Aplicar a *cláusula de reserva jurisdicional* apenas:

2.1.1 àquela prevista na Constituição, leia-se, às comunicações telefônicas;

2.1.2 ampliar as hipóteses de cláusula de reserva jurisdicional por via *legislativa* apenas àquelas circunstâncias em que há um *alto nível de expectativa de privacidade* por seu titular (ex. dados de conteúdo armazenados em *smartphones*) ou a *potencialidade de graves danos* ao titular dos dados com a sua circulação.

5.3. Para as demais hipóteses, mesmo em se tratando de *dado sigiloso* ou *sensível*, instituir os requisitos *gerais* e *proporcionais* via *legislativa* sobre as possibilidades de flexibilização do *sigilo* constitucional, conforme já autorizado pelo Supremo Tribunal Federal em relação a Lei nº 9.613/1998 e a Lei Complementar nº 105/2001.

5.3.1 A ideia é converter a Lei em um *estatuto geral* sobre as possibilidades de tratamento de dados com a finalidade em conferir maior segurança jurídica na aplicação da lei e eficiência na fiscalização dos ilícitos penais, cíveis e administrativos. Com isso, estabelecer parâmetros gerais para o intercâmbio de dados.

5.3.1.1. As intervenções estatais no âmbito de direitos fundamentais deverão ser proporcionais à *finalidade* do tratamento de dados. Logo, a futura lei não poderá ser prejudicial à disposição legal existente sobre as específicas e graduais formas de intervenção estatal nos direitos fundamentais, como ocorre, por exemplo, com a Lei de Interceptação Telefônica, bem como com a Lei nº 9.613/1998. A *preferência irrestrita e abstrata* da proteção de dados em prejuízo dos demais direitos e interesses em conflito é *desproporcional* e *inconstitucional*, eis que cria uma preferência *genérica e prima facie* de um direito fundamental sobre os demais e que cria um espaço de ineficiência ao dever de proteção estatal.

5.3.2 As comunicações sobre ilícitos penais, cíveis e administrativo de atribuição do Ministério Público que contenham dados sigilosos ou sensíveis deverão ser autorizadas pela presente Lei, eis que encerram em transmissão do sigilo e atendem ao sistema acusatório, com a ressalva daquelas informações com exigem *cláusula de reserva jurisdicional* para a sua obtenção e compartilhamento;

5.4. Estabelecer requisitos procedimentais mínimos sobre a circulação dos dados pessoais, inclusive os sigilosos e sensíveis, como a necessidade de *formalização*,

para a garantia de *adequação* do tratamento dos dados às *finalidades* para quais eles foram coletados ou compartilhados;

5.5. Estimular a criação de um sistema eletrônico *interoperável* para o tratamento e circulação de dados pessoais entre as instituições, facilitando a segurança da informação e criando um ambiente propício para o registro e controle de acesso, a auditoria e o controle posterior jurisdicional ou pela Autoridade de Controle;

5.6. Sobre a Autoridade de Controle:

5.6.1 proteção de dados inerentes à **função jurisdicional**:

5.6.1.1 o respeito à separação dos poderes e a autonomia e independência do Ministério Público e Judiciário. Essa garantia é concretizada pela delimitação de sua função meramente administrativa, ou seja, a Autoridade de Controle não exerce função jurisdicional. Logo, não incumbe a análise de **elementos de informação e provas** inseridas em investigações e processos criminais e, em consequência, também não possui atribuição para afastar o **sigilo** conferido a esses procedimentos e processos;

5.6.1.2 a normatização da proteção sobre o tratamento de dados constituídos **em elementos de informação ou provas** serão regulados pelo legislador infraconstitucional da União, na forma do artigo 22, inciso I, (penal, processual) da Constituição da República;

5.6.1.3 a análise sobre a licitude do tratamento de dados caberá ao juiz natural, autoridade com competência e independência para a análise em cada caso concreto;

5.6.2 proteção de dados inerentes à **função administrativa**:

5.6.2.1 o controle de legalidade de atos administrativos do Ministério Público e do Poder Judiciário, mormente a normatização, fiscalização e sancionamento sobre o tratamento de dados pessoais, deverá respeitar a *autonomia administrativa* constitucionalmente conferidas à essas instituições, ou seja:

5.6.2.1.1 ao Ministério Público, o respeito às atribuições constitucionais conferidas ao *Conselho Nacional do Ministério Público* e aos *Ministérios Públicos da União e dos Estados*;

5.6.2.1.2 ao Judiciário o respeito às atribuições constitucionais conferidas ao *Conselho Nacional de Justiça* e aos *Tribunais*.

Por fim, o CAOCRIM quer agradecer o empenho de todos os Promotores de Justiça Criminais que integraram o GRUPO DE TRABALHO e escreveram a presente Nota Técnica. Foram várias as reuniões e discussões realizadas, que permitiram a conclusão deste texto.

Integrantes do Grupo de Trabalho: Ricardo Silves, Amauri Silveira Filho, Gregório Edoardo Raphael Selingardi Guardia, João Paulo Gabriel de Souza, Leonardo Leonel Romanelli, Olavo Evangelista Pezotti, Paulo Guilherme Carolis Lima, Richard Gantus Encinas e Rogério Sanches Cunha.

São Paulo, 19 de fevereiro de 2021.

SECRETARIA ESPECIAL DE POLÍTICAS CRIMINAIS
CAOCRIM – CENTRO DE APOIO ÀS PROMOTORIAS CRIMINAIS