

O direito de acesso às comunicações entre COAF e autoridades
investigativas como reflexo do direito constitucional à proteção de dados
pessoais

*The right to access communications between FIU and investigative
authorities as a consequence of the constitutional right to personal data
protection*

Marcelo Neves Rezende¹



This work is licensed under a Creative Commons Attribution 4.0 International License.

Resumo: O presente artigo pretende explorar alguns reflexos do recém consagrado direito constitucional à proteção de dados pessoais sobre a etapa de disseminação de informações de inteligência financeira pelo COAF às autoridades de investigação penal. Aplicando-se esse direito fundamental nessa fase de compartilhamento, limites deverão ser observados, para evitar devassas injustificadas na esfera de privacidade dos indivíduos. Assim, tratando-se essa etapa procedimental de uma atividade que se aproxima de uma investigação penal, a incidência desse direito deverá ser mais acentuada, o que induz à necessidade de exercer controle de legalidade mais rigoroso sobre os atos de comunicação entre COAF e autoridades investigativas. Controle esse que, segundo defendemos, somente poderá ser exercido com o acesso a essas comunicações pelos indivíduos titulares dos dados compartilhados.

Palavras-chave: acesso – comunicações – compartilhamento – COAF – proteção de dados

Abstract: This article intends to analyze some of the consequences that the recent Brazilian Supreme Court's decision, declaring Personal Data Protection as a fundamental right, will have on the procedures of dissemination of Financial Intelligence Reports between the Brazilian

¹ Pós-graduado em Processo Penal e Garantias Fundamentais pela Academia Brasileira de Direito Constitucional – ABDConst-Rio. Bacharel em Direito pela Pontifícia Universidade Católica do Rio de Janeiro – PUC-RJ. Advogado criminal.

Financial Intelligence Unit – FIU and investigative authorities. The recent recognition of Personal Data Protection as a fundamental right enforces the authorities to observe some limits for dissemination of Financial Intelligence Reports, to avoid unjustified violations of people data privacy. Since this stage of dissemination of information is equivalent to a criminal investigation, the legal boundaries for the dissemination of Financial Intelligence Reports must be even more strict. In that order, we defend that all the communications must be accessed by the holders of the shared data.

Keywords: Access – Communications – Dissemination – UIF - Data Protection

1. Introdução

O Conselho de Controle de Atividade Financeira (COAF) – unidade de inteligência financeira (UIF) do Brasil – precisou de tempo para aperfeiçoar sua atividade até chegar à capacidade atual de processamento e disseminação de dados. Em meados de 2012, substanciais mudanças puderam ser notadas com a implementação de novas tecnologias, a informatização de sistemas cadastrais em geral e a edição da Lei nº 12.683/2012, que expandiu os mecanismos de combate à lavagem de dinheiro.

Desde então, mas em especial nos últimos anos (2020 – 2021), duas variáveis têm crescido exponencialmente: (i) a utilização do meio digital para a circulação de capital, com predomínio de transações financeiras informatizadas, até chegarmos ao pagamento instantâneo “Pix”; (ii) e o aprimoramento das técnicas de processamento das informações, com o uso de mineração de dados, análises preditivas, etc.

Essa predominância dos meios digitais nas transações financeiras, somada ao aperfeiçoamento da capacidade de processar dados pelo COAF tem resultado um aumento expressivo no número de relatórios de inteligência financeira compartilhados anualmente, segundo dados do SISCOAF registrados até 31/12/2021.¹

¹ Em números, foram: 2.104 relatórios em 2012; 2.450 em 2013; 3.178 em 2014; 4.304 em 2015; 5.661 em 2016; 6.608 em 2017; 7.345 em 2018; 6.272 em 2019; 11.693 em 2020 e 12.512 em 2021. Disponível em <https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/RACoaf2021publica20220311.pdf>. Acesso em 17 maio 2022.

Diante desse monitoramento cada vez maior do sistema financeiro nacional, é natural que a unidade de inteligência financeira brasileira adquira protagonismo no combate a crimes econômicos, especialmente os de lavagem de capitais, dada a capacidade do COAF de detecção de operações irregulares para afastar o proveito econômico da ilicitude, muitas vezes por meio da utilização de empresas de fachada, transações sem lastro, dentre tantos outros expedientes, o que demonstra a importância de aprofundar o estudo sobre os impactos desse poder de vigilância.

E é bom que haja essa expansão, porquanto as fraudes se mostram cada vez mais sofisticadas, sendo as atividades de inteligência, por meio de um tratamento de dados consideravelmente mais livre do que o previsto no devido processo legal, o meio mais eficaz de prevenir e combater crimes tais como a lavagem de capitais.²

Antes, porém, do desenvolvimento mundial das atividades de inteligência financeira, já era possível notar esse crescimento da capacidade de coleta, processamento e cruzamento de informações pessoais, com a formação de bancos de dados centralizados por órgãos da administração pública e por empresas privadas, o que influencia profundamente no direito à privacidade do indivíduo, pois, a partir do uso dessas novas tecnologias, possibilita-se a formação de um retrato completo sobre aspectos íntimos da pessoa, sem a sua participação ou conhecimento.³

Nesse contexto é que o direito à proteção dos dados pessoais dá seus primeiros passos no direito comparado, especialmente na Alemanha, sendo aos poucos reconhecido como um direito fundamental limitador do poder estadual, como proteção ao livre desenvolvimento da personalidade.

No Brasil, apenas recentemente, no ano de 2020, o Supremo Tribunal Federal reconheceu que os *dados pessoais (...) integram o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII). Sua manipulação e tratamento, desse modo, hão de observar, sob pena de lesão a esses direitos, os limites delineados pela proteção*

² Segundo as razões da Diretiva 2021/0250 (COD), cerca de 1% do produto interno bruto da União Europeia é “detectado como estando envolvido em suspeita de atividade financeira suspeita”. São muitas as disposições tendentes a ampliar a forma como os dados são processados por essas unidades, o que mostra ser o serviço de inteligência financeira, hoje, a principal forma de prevenção e combate à lavagem de dinheiro e ao terrorismo no mundo.

³ MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 31.

constitucional. Em 11/02/2022, com a publicação da emenda constitucional nº 115, o direito à proteção de dados passou a ser expressamente previsto na Constituição Federal como uma garantia fundamental e autônoma.

Do ponto de vista das atividades do COAF, a um primeiro olhar, pode parecer que há um conflito entre a necessidade de expansão tecnológica no processamento e cruzamento desses dados pessoais – como transações e informações cadastrais – e a observância do direito fundamental à proteção de dados pessoais.

Nesse sentido, Laura Schertel Mendes⁴ afirma que “*a melhor forma de se observar a questão não é por meio da dicotomia entre tecnologia e privacidade, mas, sim, a partir da concepção de que o desenvolvimento tecnológico deve ser harmonizado com a preservação da privacidade*”, aludindo ainda para a comparação feita por Simson Garfinkel⁵, de que a suposta dicotomia entre desenvolvimento econômico e preservação ambiental, presente na década de 1950 e 1960, foi superada pela compreensão de desenvolvimento econômico sustentável.

É justamente sob esse mote que o presente artigo pretende dar contribuições, no intuito de harmonizar a expansão do poder informacional do COAF com o recém consagrado direito constitucional à proteção de dados.

Certo é também que, em se tratando de atividades de inteligência financeira, essa filtragem constitucional pode ser explorada sob diversos ângulos, especialmente porque o tratamento de dados pelo COAF se divide em várias etapas, podendo-se citar o recebimento, as fases de processamento e a disseminação. Parece-nos que, em cada uma dessas etapas, deverá haver certa compatibilização com o direito à proteção de dados pessoais, estudo que merece – como se tem visto – um constante aprofundamento teórico.

Para os fins do presente artigo, estabelece-se como recorte a etapa de disseminação dos dados para as autoridades investigativas, por meio do envio de relatórios de inteligência financeira, de modo a explorar – sem a pretensão de exaurir o tema – alguns impactos do recém consagrado direito constitucional à proteção de dados, bem como identificar possíveis consequências.

⁴ MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 34.

⁵ GARFINKEL, SIMSON. *Database Nation: the death of privacy in the 21th Century*. California: O'Reilly Media, 2000, p. 5.

2. O direito à proteção de dados pessoais

Como visto, o direito à proteção de dados pessoais, para além da tutela da privacidade, se desenvolve a partir do implemento das novas tecnologias de processamento de dados e da formação de bancos de dados centralizados, a partir das décadas de 1970 e 1980. O cruzamento das informações pessoais, em níveis até então inimagináveis, passou a permitir a construção de um *retrato completo sobre a pessoa, sem a sua participação ou conhecimento*⁶, o que influencia no livre desenvolvimento da sua personalidade.

Nesse sentido, não há como deixar de citar, ainda que sumariamente, a decisão proferida pelo Tribunal Constitucional alemão, no julgamento sobre a “Lei do Recenseamento”, em 1983, considerada um marco no reconhecimento desse direito como fundamental⁷. Nesse emblemático julgamento, a Suprema Corte alemã desenvolveu conceitos que balizaram o que se entende por autodeterminação informativa, contribuindo para o reconhecimento do direito à proteção de dados como um direito fundamental.

Como explica Laura Schertel, *a privacidade, antes compreendida, prioritariamente, como o direito negativo de ser deixado em paz (right to be let alone), passa a significar também o controle dos dados pessoais pelo próprio indivíduo, que decide quando, como e onde os seus dados pessoais devem circular*.⁸

Reconheceu-se, então, naquele julgamento, que a circulação indiscriminada de dados pessoais, à revelia do seu titular, influencia diretamente a formação livre da personalidade, isto é, o direito de decidir livremente como e em que circunstâncias deseja apresentar sua personalidade ao público. Ao passo que as tecnologias de processamento de dados são capazes de formar um perfil completo sobre os indivíduos, consagrou-se o direito à autodeterminação informativa, que visa garantir o poder do titular de decidir sobre sua coleta, processamento e transmissão. É o que afirma Laura Schertel, ainda explicando o julgamento da “Lei do Recenseamento”, em 1983:

Assim, afirma o Tribunal que o processamento automatizado dos dados ameaçaria o poder do indivíduo de decidir por si mesmo se e como ele desejaria fornecer a terceiros os seus dados pessoais, considerando que o processamento de dados possibilitaria a elaboração de um “perfil completo da personalidade” por meio

⁶ MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 31.

⁷ ALEMANHA. Tribunal Constitucional Federal. *BVerfGE* 65, 1 (1983)

⁸ MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 36.

de “sistemas automatizados integrados sem que o interessado pudesse controlar de forma suficiente sua correção e utilização”. (A sentença referente ao recenseamento da população do Tribunal Constitucional (BVerfGE 65, 1)

Tal utilização ampliaria a influência do Estado sobre o comportamento do indivíduo, que não mais seria capaz de tomar decisões livres em virtude “da pressão psíquica de participação pública”. Uma sociedade, “na qual os cidadãos não mais são capazes de saber quem sabe o que sobre eles, quando e em que situação”, seria contrária ao direito à autodeterminação informativa, algo prejudicial tanto para a personalidade quanto para o bem comum de uma sociedade democrática. (BVerfGE 65,1 (42), Recenseamento).

Destarte, o Tribunal Constitucional constata que do art. 2º, §1º (livre desenvolvimento da personalidade), combinado com o art. 1º, §1º (dignidade humana), da LF, resultaria um direito fundamental à autodeterminação informativa que garantiria “o poder do indivíduo em determinar sobre a coleta e utilização de seus dados pessoais”. (BVerfGE 65,1 (43), Recenseamento). O Tribunal reforça que o direito fundamental não seria ilimitado, pois as informações pessoais denotariam um “retrato da realidade social” e, portanto, não poderiam ser atribuídas somente ao indivíduo.

Todavia esses limites somente seriam justificados em nome de um interesse geral preponderante. Ademais, eles teriam que ter uma base legal para cumprir tanto o imperativo da clareza das normas quanto o princípio da proporcionalidade. Por fim, teriam que ser tomadas providências de cunho organizacional para diminuir os riscos à personalidade do cidadão. (BVerfGE 65,1 (44), Recenseamento).

Decisivo para a concepção do direito à autodeterminação informativa é o princípio segundo o qual não mais existiriam dados insignificantes nas circunstâncias modernas do processamento automatizado de dados. O risco do processamento de dados residiria mais na finalidade do processamento e nas possibilidades de processamento do que no tipo dos dados tratados.

A fim de prestar proteção contra o risco decorrente do moderno processamento de dados, o Tribunal formula que todos os dados pessoais estariam abrangidos no âmbito de proteção do direito à autodeterminação informativa e que somente o próprio interessado poderia decidir sobre sua coleta, processamento e transmissão. (BVerfGE 65,1 (45), Recenseamento).

Isso significa que, na jurisprudência do Tribunal Constitucional, a mudança definitiva da concepção da esfera privada para o direito à autodeterminação informativa, na qual a atribuição de dados a uma esfera íntima não tem mais nenhum papel significativo. O Tribunal Constitucional alemão estendeu a proteção frente à coleta, armazenamento, utilização e transmissão aos dados pessoais em vez de limitá-la a uma esfera privada que protegeria somente informações íntimas (GRIMM, 1997, p. 15). Dessa forma, o Tribunal formula um princípio constitucional, já encontrado desde os anos de 1970 no direito à proteção de dados infraconstitucional, no qual o caráter pessoal de um dado era o fator decisivo de proteção, e não o fato de se tratar de dado íntimo ou privado.

Esse emblemático julgamento contribuiu profundamente para o desenvolvimento de normas pela União Europeia, por meio de diversas diretivas, podendo-se citar a principal

Diretiva 95/46/CE, “relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados”.

Portanto, uma das chaves para compreender a essência desse direito é observar que não apenas dados da esfera íntima são dignos de proteção constitucional, como também dados que poderiam ser tidos como insignificantes, mas que revelam traços, ainda que distantes, da personalidade. Afinal, “o risco do processamento de dados residiria mais na finalidade do processamento e nas possibilidades de processamento do que no tipo dos dados mesmos (ou no fato de quão sensíveis ou íntimos eles são)”.⁹

Em última análise, a consagração do direito à proteção de dados se presta a manter, mesmo que de forma limitada, o controle decisório sobre o tratamento dos dados pessoais com o seu titular, como forma de garantir a sua liberdade de construir sua personalidade.

No ponto, Ingo Sarlet traça linhas mais marcantes que afastam o direito à proteção de dados do direito à privacidade¹⁰, embora comumente se afirme ser aquele uma evolução deste. Vejamos:

Uma primeira diferença que pode ser apontada reside no fato de que – na esteira das lições de Stefano Rodotà – a privacidade indica uma visão negativa e estática, em larga medida pautada na concepção de impossibilitar a interferência de terceiros. Em contrapartida, a proteção de dados confere ao titular poderes positivos e dinâmicos postos à sua disposição com vistas ao controle sobre a coleta e o processamento dos dados que lhe digam respeito. Assim – de acordo com Rodotà –, o bem jurídico tutelado na privacidade gira em torno da informação e do sigilo, enquanto no direito à proteção de dados abarca a informação, a circulação e o respectivo controle.

Em decorrência dessa delimitação, o direito à proteção de dados – diferentemente do direito à privacidade, que estabeleceria um “não fazer” de terceiros para evitar uma invasão na esfera íntima – põe à disposição do titular, segundo Sarlet, *poderes positivos e dinâmicos* para o controle do tratamento de seus dados pessoais.

Daí porque conclui o autor que:

(...) o direito à autodeterminação informativa apresentar dupla dimensão individual e coletiva, no sentido de que garantida constitucionalmente não é apenas (embora possa ser, como direito subjetivo individual, o mais importante) a

⁹ MENDES, Laura Schertel. **Autodeterminação informativa**: a história de um conceito. Pensar: Revista de Ciências Jurídicas, Fortaleza, V 25, nº 4, out/dez 2020. P. 11.

¹⁰ SARLET, Info Wolfgang; Fundamentos Constitucionais: O Direito Fundamental à Proteção de Dados. In: **Tratado de proteção de dados pessoais**, coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021, p. 32/33.

possibilidade de cada um decidir sobre o acesso, uso e difusão de seus dados pessoais, mas também – e aqui a dimensão metaindividual (coletiva) – se trata de destacar que a autodeterminação informativa constitui condição para uma ordem comunicacional livre e democrática, distanciando-se, nessa medida, de uma concepção de privacidade individualista e mesmo isolacionista à feição de um direito a estar só (*right to be alone*). Dito de outro modo, a proteção de dados é, enquanto proteção de direitos fundamentais, espinha dorsal de uma democracia liberal.

Retoma-se, aqui, as considerações feitas no início deste artigo, de que, ao mesmo tempo em que só há crescimento econômico se for sustentável, aqui, no campo do avanço tecnológico em processar dados pessoais, só haverá progresso se observado esse direito coletivo de autodeterminação informativa.

Compreender essa transcendência do direito à proteção de dados sobre esse caráter negativo e estático do direito à privacidade é fundamental para explorar, pouco mais adiante, os seus impactos em atividades como as de compartilhamento de informações pelo COAF.

O direito brasileiro, por sua vez, bastante em linha com os conceitos desenvolvidos pelo direito alemão e com as diretivas europeias, recentemente consagrou a proteção de dados como um direito fundamental *decorrentes de cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII)*, segundo decidido em 2020, pelo Supremo Tribunal Federal, nas ADIs 6.387, 6.388, 6.389, 6.390 e 6.393, em casos que tratavam do compartilhamento de dados por empresas de telecomunicações prestadoras de serviço telefônico com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE).

Não demorou – ao menos desde o julgamento da ADI – e, em 11/02/2022, a proteção de dados pessoais foi positivada na Constituição Federal como direito autônomo, em especial no artigo 5º, LXXIX: “*é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais*”.

3. A aplicabilidade da proteção de dados pessoais às atividades de inteligência financeira

O Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal, é verdade, ainda se encontra em tramitação legislativa, de modo que, na data de divulgação deste artigo, ainda não há uma lei geral que proteja e limite o poder estatal no uso de dados pessoais em investigações penais e atividades de inteligência.

No entanto, há vários fatores que induzem à conclusão de que todo esse conceito de direito à proteção de dados pessoais é plenamente aplicável às atividades de inteligência financeira desempenhadas pelo COAF, especialmente no que diz respeito ao compartilhamento dessas informações com órgãos de persecução.

Em primeiro lugar, esse direito já se encontra expressamente previsto na Constituição Federal como um direito autônomo, de sorte que a plena eficácia de normas constitucionais permite – senão impõe – a sua aplicação sobre as atividades de todas as instituições que se submetem ao Estado de Direito brasileiro, como é o caso do COAF.

No direito comparado, não parece haver dúvida quanto à aplicabilidade do direito à proteção de dados pessoais sobre as atividades de inteligência financeira, desempenhadas pelas FIUs – *Financial Intelligence Units*, ficando o debate a cargo de quando, onde e como devem essas garantias incidir.

Não à toa, na Europa, o constante investimento nas unidades de inteligência financeira como forma de combate à lavagem de dinheiro e ao terrorismo tem sido acompanhado de uma preocupação pela garantia à proteção de dados, impedindo ou, ao menos, excepcionalizando fluxos de informação que atentem contra a finalidade para a qual determinados dados foram obtidos.

Exemplo recente disso é que, após a edição da Diretiva 2021/0250 (COD), pelo Parlamento Europeu, em 20/07/2021, *relativa aos mecanismos a serem criados pelos Estados-Membros para prevenir a utilização do sistema financeiro para efeitos de branqueamento de capitais ou d/e financiamento do terrorismo*, na qual se ampliou de forma significativa o acesso e o processamento de dados, bem como a comunicação entre as unidades de inteligência financeiras dos países e outras autoridades, o *European Data Protection Supervisor (EDPS)* emitiu a *Opinion 12/2021*, demonstrando preocupação com possíveis violações à privacidade, especialmente quanto à amplitude de acesso a dados e a sua forma de processamento.¹¹

¹¹ Segundo a Opinion: *The EDPS notes that the proposed AML package takes a risk-based approach to the screening of bank's clients in order to assess whether they may represent a money-laundering risk. While the EDPS appreciates the value of the risk-based approach underpinning the proposed legislative package, he considers that further clarifications are needed to minimize intrusion into individual's privacy and to ensure full compliance with data protection rules. (...) In relation to the proposal for the coordination mechanism of Financial intelligence Units (FIUs), the EDPS emphasizes in his opinion that access to information related to criminal offences in particular, and access to administrative information and financial information about individuals should be limited to what is necessary in light of specific purposes. In this regard, he invites the legislator to reassess the necessity and proportionality of the proposed access rights. (...) The EDPS notes the reference, under recital 51 of the Proposal for a Directive, to functionalities of the FIU.net allowing "FIUs to match their data with data of other FIUs in an anonymous way with the aim of detecting subjects of the FIU's*

No Brasil, como visto, o anteprojeto de lei de proteção de dados voltado para segurança pública e persecução penal ainda se encontra em tramitação legislativa. Em seu texto, há expressa indicação de que as proteções ali dispostas se aplicam às atividades de inteligência financeira.

Independentemente da conversão desse anteprojeto em lei, a recente consagração do direito à proteção de dados pelo Supremo Tribunal Federal já tem produzido impactos sob diversas instituições, tais como órgãos de inteligência e o compartilhamento de seus dados.

Na ADI 6.529/MC, o Plenário do Supremo Tribunal Federal, em 13/08/2020, conferiu interpretação conforme a dispositivos da Lei nº 9.883/1999¹², que preveem o compartilhamento de dados entre órgãos do sistema de inteligência brasileiro (SISBIN) – nos quais se incluem o COAF – com a ABIN.

Embora os dispositivos legais impugnados estejam vigentes há mais de 20 (vinte) anos, votos importantes como os do Ministro Edson Fachin¹³ e do Ministro Gilmar Mendes dirigiram o olhar para o cenário atual de fluxo facilitado de informações entre instituições públicas, aplicando princípios do direito à proteção de dados pessoais para limitar esse compartilhamento entre órgãos de inteligência e a ABIN.

interests in other Member States and identifying their proceeds and funds, whilst ensuring full protection of personal data.” In this regard, the EDPS reiterates, as already indicated in the Opinion 1/2017 and in the Opinion on the Action Plan, that he considers more in line with the principles of proportionality and purpose limitation a legal configuration of the powers of FIUs as “investigation-based” rather than ‘intelligence-based’. The latter approach would be more similar to data mining than to a targeted investigation, thus further impacting data protection. The specification under recital 51, not mirrored by the way by a corresponding provision in the operative part of the Proposal for a Directive, seems to refer indeed to a data mining technique for the identification of subjects of (merely) potential interest. Hence, the EDPS recommends deleting the aforementioned wording in recital 51 of the Proposal for a Directive. Disponível em https://edps.europa.eu/data-protection/our-work/publications/opinions/anti-money-laundering-and-counter-finance-financing_en. Acesso em 19 maio 2022.

¹² Lei n. 9.883/1999, Art. 4º (...) Parágrafo único. Os órgãos componentes do Sistema Brasileiro de Inteligência fornecerão à ABIN, nos termos e condições a serem aprovados mediante ato presidencial, para fins de integração, dados e conhecimentos específicos relacionados com a defesa das instituições e dos interesses nacionais.

¹³ Confira-se trecho do voto do Ministro Edson Fachin: *A plausibilidade do pedido realizado na inicial é exacerbada, precisamente, pela natureza das atividades de inteligência. Ainda que se possa, em momento posterior, discutir o caráter de política pública do serviço de inteligência, delimitando inclusive sua adequação à ordem de um Estado de Direito Democrático, é evidente que tal compartilhamento de dados ativa inúmeras sensibilidades democráticas, incluindo o risco de construção de mecanismos típicos de um Estado policiaresco. Neste sentido, o presente caso, por tratar de envio de dados pessoais a agência de inteligência, acarreta ainda maiores restrições às liberdades que aquele julgado nas ADIs 6.387, 6.388, 6.389, 6.390 e 6.393. Tem-se um cenário em que a ausência de protocolos claros de proteção e tratamento de dados, somada à possibilidade, narrada na inicial e amplamente divulgada na imprensa, de construção de dossiês investigativos contra servidores públicos e cidadão pertencentes à oposição política, deve gerar preocupações quanto à limitação constitucional do serviço de inteligência.*

Em especial, o voto do Ministro Gilmar Mendes afirma que esse compartilhamento de dados de inteligência deve ser interpretado sob o prisma do direito à autodeterminação informativa, consagrando-se um “*devido processo informacional*”, no qual o titular dos dados possa ter “*o direito de evitar exposições de seus dados sem possibilidades mínimas de controle*”:

I – Da autonomia do direito fundamental à proteção de dados pessoais na ordem constitucional brasileira

Em primeiro lugar, é importante situar epistemologicamente que o parâmetro de controle invocado nesta ADI está relacionado à afirmação do direito à proteção de dados pessoais enquanto categoria autônoma de direito fundamental na ordem constitucional brasileira, especialmente na forma de uma projeção alargada do direito à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, consagrado no art. 5º, inciso X, da CF.

(...)

Em uma dimensão subjetiva, a proteção do indivíduo contra os riscos que ameaçam a sua personalidade em face da coleta, processamento, utilização e circulação dos dados pessoais e, em uma perspectiva objetiva, a atribuição ao indivíduo da garantia de controlar o fluxo de seus dados. (MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 140., p. 176-177).

A partir da tradição norte-americana, também é possível identificar como corolário da dimensão subjetiva do direito à proteção de dados pessoais, a preservação de verdadeiro “*devido processo informacional*” (informational due process privacy right), voltado a conferir ao indivíduo o direito de evitar exposições de seus dados sem possibilidades mínimas de controle, sobretudo em relação a práticas de tratamento de dados capazes de sujeitar o indivíduo a julgamentos preditivos e peremptórios.

(...)

Essa abrangência da proteção atribuída ao direito de autodeterminação constitui importante chave interpretativa do âmbito de proteção do direito fundamental à proteção de dados pessoais, o qual não recai propriamente sobre a dimensão privada ou não do dado, mas sim sobre os riscos atribuídos ao seu processamento por terceiros.

É justamente a partir deste prisma que deve ser examinada a constitucionalidade dos dispositivos impugnados da Lei 9.883, de 1999, que dispõe, no que interessa, sobre o fornecimento à ABIN de dados e conhecimentos específicos relacionados com a defesa das instituições e dos interesses nacionais.

(...)

Verifica-se que o art. 4º, parágrafo único, da lei, ao contemplar a análise de dados como etapa essencial das atividades de inteligência, esclareceu a possibilidade – e não necessariamente a obrigatoriedade – de compartilhamento de dados entre os órgãos componentes do Sistema.

Essa simples previsão legal, porém, apesar de ser necessária, não é em si suficiente para legitimar todo e qualquer procedimento de compartilhamento e requisição de dados, uma vez inafastável a observância das garantias institucionais de

cunho constitucional, sobretudo naquilo que diz respeito ao direito ao sigilo ou a reserva de jurisdição.

Nesse aspecto, ao menos em um juízo de cognição sumária típico dessa fase processual, entendo que o exame da constitucionalidade deve ser examinado a partir do clássico teste da proporcionalidade, o qual, aliás, afigura-se central para a verificação de violações ao direito à autodeterminação informacional, como consagrado na jurisprudência do BVerfG a partir do julgamento da Lei do Censo de 1983.

(...)

Por todos esses motivos, entendo que, no caso concreto, há alguma verossimilhança nas alegações da autora, no sentido de que o ato normativo trazido a exame desta Suprema Corte – justamente por contemplar aplicações múltiplas e genéricas – tem o potencial de violar os direitos fundamentais da proteção da privacidade, da proteção de dados e da autodeterminação informativa dos cidadãos brasileiros (art. 5º, incisos X e XII, da CF/88), e tampouco mostra-se proporcional ante as suas finalidades.

Do voto do Ministro Gilmar Mendes, é possível inferir que esse intercâmbio de dados de inteligência, mesmo que entre órgãos integrantes do SISBIN, se submete ao regime constitucional da proteção de dados. Podemos ver aí a formação do que Ingo Sarlet chamou de “*ordem comunicacional livre e democrática*”, encarando a privacidade como um direito coletivo e uma obrigação institucional do Estado Democrático de Direito.

Com esses e outros fundamentos jurídicos, o Plenário do STF estabeleceu como balizas para esse compartilhamento de dados de inteligência os seguintes parâmetros: a) os órgãos componentes do Sistema Brasileiro de Inteligência somente podem fornecer dados e conhecimentos específicos à ABIN quando comprovado o interesse público da medida, afastada qualquer possibilidade de o fornecimento desses dados atender a interesses pessoais ou privados; b) qualquer solicitação de dados deverá ser devidamente motivada para eventual controle de legalidade pelo Poder Judiciário; c) mesmo presente interesse público, os dados referentes às comunicações telefônicas ou dados sujeitos à reserva de jurisdição não podem ser compartilhados na forma do dispositivo legal, decorrente do imperativo de respeito aos direitos fundamentais; d) nas hipóteses cabíveis de fornecimento de informações e dados à ABIN, são imprescindíveis procedimento formalmente instaurado e existência de sistemas eletrônicos de segurança e registro de acesso, inclusive para efeito de responsabilização em caso de eventual omissão, desvio ou abuso.

Repare que esses filtros foram aplicados em uma fase de processamento e compartilhamento de dados entre órgãos de inteligência, cuja transferência deverá ter, por

definição, sempre os fins previstos no § 2º do art. 1º da Lei n. 9.883/1999: “[inteligência é] a atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado”.

Trata-se, portanto, de atividade de inteligência clássica, que é essencialmente grave, com potencial de restringir direitos, dado que trabalha no campo prévio, de forma ágil, para auxiliar em processo decisório que envolva interesses de extrema relevância, como segurança nacional, segurança da sociedade, etc.

Como aqui já ilustrado, na Europa, o debate sobre essa compatibilidade entre o direito à proteção aos dados pessoais e a expansão do fluxo informacional das unidades de inteligência financeira já se encontra no campo interno da própria atividade de inteligência, como, por exemplo, os limites de compartilhamento de dados entre UIFs.

É natural que, nessa esfera entre órgãos de inteligência, haja uma incidência mais branda de direitos constitucionais, como o direito de acesso à informação (art. 5º, XIV e XXXIII, CF), de *habeas data* (art. 5º, LXXII, CF), de sigilo de dados e comunicações (art. 5º, XII, CF) e a própria proteção de dados pessoais (art. 5º, LXXIX, CF), diante da própria finalidade dos serviços de inteligência – auxiliar, de forma célere ou mesmo imediata, no processo decisório ou ação governamental para garantir a segurança da sociedade e do Estado –, sob pena de colocar em risco a própria inteligência.

Sobre o ponto, as lições de Orlandino Gleizer, Lucas Montenegro e Eduardo Viana¹⁴ ensinam que “sendo diferentes as funções desempenhadas na inteligência, na segurança pública e no processo penal, são também diferentes os parâmetros que autorizam o Estado a levantar dados em cada um desses âmbitos”, explicando, então, a distinção entre as atividades de inteligência e as de persecução penal:

O tratamento dos dados está limitado à finalidade que fundamentou o seu levantamento. O próximo passo consiste então em saber quais são essas finalidades. Para o nosso tema, interessa saber como se distinguem as atividades de inteligência, garantia da segurança pública e persecução penal. Afinal, por meio dessas atividades, o Estado exerce determinadas *funções*, ou seja, busca realizar fins específicos. Dessa diferença de fins decorrem também *diferentes critérios para adequação dos meios*, os quais, no nosso caso, são medidas de tratamento de dados. Em outras palavras: sendo

¹⁴ GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. O direito de proteção de dados no processo penal e na segurara pública. 1. ed. Rio de Janeiro: Marcial Pons, 2021. p. 51/53.

diferentes as funções desempenhadas na inteligência, na segurança pública e no processo penal, são também diferentes os parâmetros que autorizam o Estado a levantar dados em cada um desses âmbitos. Portanto, há que se perguntar, em primeiro lugar, no que consiste a diferença de funções entre persecução penal, segurança pública e inteligência.

A persecução penal está voltada para a confirmação de uma *suspeita* (em detalhes, D.I.2). É a suspeita que dá ensejo à atuação dos órgãos de persecução penal. A atividade desenvolve-se desde um ponto de vista *retrospectivo*; trata-se de desvendar a ocorrência de um fato pretérito. (...) As atividades de inteligência têm como função a coleta e a análise de informações necessárias para antecipar-se a perigos ou formular políticas de segurança interna ou externa. Na realização dessa atividade, os serviços de inteligência dispõem de ampla margem de investigação com alto potencial interventivo na esfera dos dados pessoais, por atuarem em um *campo prévio (Vorfeld)* à existência de perigos ou suspeitas. A inteligência está voltada à *precaução*.

Ora, se já se discute uma harmonização desse processamento e compartilhamento interno de dados por órgãos de inteligência com o direito à proteção de dados pessoais, com muito mais razão, a nosso entender, deverá incidir essa garantia constitucional na transmissão de dados entre agência de inteligência e autoridade de investigação penal, porquanto a finalidade de sua transmissão não é de “*resguardar à segurança da sociedade ou do Estado*”, mas de propiciar eventual abertura de processo sancionador criminal, com a futura aplicação da lei penal.

No caso do COAF, compreendemos, não deverá ser diferente, de modo que sejam garantidos, em maior grau, direitos fundamentais nessa etapa de tratamento de dados (disseminação às autoridades investigativas). É o que pretendemos explorar no próximo tópico, avaliando também suas consequências diretas.

4. Limites objetivos ao intercâmbio de informações entre COAF e Autoridades Investigativas

O Conselho de Controle de Atividades Financeiras (COAF), enquanto instituição integrante do sistema brasileiro de inteligência (SISBIN), parece ter uma natureza *sui generis*: ao mesmo tempo em que exerce um serviço clássico de inteligência, analisando dados, não para investigar uma suspeita previamente definida, mas com fins de resguardar a segurança da sociedade e do Estado, o COAF também tem o objetivo de prevenir e combater determinados crimes (hipótese previamente definida), o que poderia aproximar sua atuação a investigações penais clássicas.

O órgão trabalha em 3 (três) etapas de processamento de dados: recebimento, processamento e disseminação. Para os fins do presente artigo, interessa a etapa final, de disseminação de dados, normalmente na forma de relatórios de inteligência, às autoridades de investigação penal, atividade que, de certa forma, carrega consigo uma finalidade última de persecução penal.

Adotando-se a premissa de que haverá maior incidência de direitos fundamentais nos intercâmbios entre COAF e autoridades de investigação penal do que nas atividades de inteligência clássica, podemos concluir que, no mínimo, os filtros desenvolvidos pelo Supremo Tribunal Federal, na ADI 6.529, ao compartilhamento entre agências do SISBIN e ABIN deverão também ser aplicados na disseminação de dados entre COAF e órgãos de persecução penal – resguardadas, é claro, suas particularidades.

Desta forma, podemos dizer que, para o COAF compartilhar dados pessoais com autoridades investigativas, deve a) estar comprovado o interesse público, aí compreendido o interesse estatal, por dever de ofício, de investigar e eventualmente punir crimes; b) a solicitação de compartilhamento deve ser motivada para eventual controle de legalidade pelo Poder Judiciário, aí se tratando da hipótese de “relatório a pedido” de autoridade investigativa; c) impossibilidade de transferência de dados sujeitos à reserva de jurisdição; d) e a existência de procedimentos formalmente instaurados e de um sistema seguro, com registro de acesso.

Parte dessas limitações, de certa forma, já foram estabelecidas pelo Supremo Tribunal Federal, ao fixar as teses, no julgamento do RE 1.055.941/SP:

1. É constitucional o compartilhamento dos relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil - em que se define o lançamento do tributo - com os órgãos de persecução penal para fins criminais sem prévia autorização judicial, devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional;
2. O compartilhamento pela UIF e pela RFB referido no 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.

No mencionado julgamento, o Plenário do STF explorou consideravelmente os pontos “c” e “d”, estabelecendo que c) as informações constantes em relatórios de inteligência financeira disseminados a autoridades investigativas não violam o sigilo bancário e d) que o

compartilhamento dessas informações deve ocorrer apenas quando houver procedimento formalmente instaurado e por meio de canais oficiais.

Quanto aos pontos “a” e “b” (interesse público e solicitação de compartilhamento motivada), aqui cabem algumas considerações. Em primeiro lugar, essas duas limitações foram estabelecidas pelo Supremo Tribunal Federal, na ADI 6.529, por proposição da Ministra Carmen Lúcia, justamente se preocupando com casos de pedidos de compartilhamento de dados a órgãos de inteligência feitos por autoridades externas, que desejem se utilizar do poder informacional desses órgãos de inteligência, para atender a fins particulares e “bisbilhotar” a vida privada.

Discorreu a Ministra: *“Inteligência é atividade sensível e grave do Estado. “Arapongagem” não é direito, é crime. Praticado pelo Estado é ilícito gravíssimo. O agente que adotar prática de solicitação e obtenção de dados e conhecimentos específicos sobre quem quer que seja fora dos estritos limites da legalidade comete crime”*.

Tal como naquele precedente, aqui, no caso de intercâmbio de dados entre COAF e autoridades de investigação penal, parece-nos também que a preocupação maior fica a cargo dessas hipóteses de pedidos de compartilhamento de relatório.

Primeiro, porque não há previsão legal para esse compartilhamento por solicitação de autoridades investigativas, mas tão somente para a transferência de ofício pelo COAF, conforme prevê artigo 15 da Lei nº 9.613/98¹⁵, fato que, por si só, já deveria obstaculizar esse formato de disseminação de informações pelo órgão.

É verdade, no entanto, que o Supremo Tribunal Federal, no RE 1.055.941/SP, chancelou essa hipótese, entendendo não haver óbice para que autoridades investigativas façam pedidos ao COAF, o qual, por sua vez, poderá buscar informações já constantes em seu banco de dados, a fim de elaborar e compartilhar, se for o caso, relatório de inteligência financeira.

Dado esse entendimento do Supremo Tribunal Federal, forçoso reconhecer que o direito constitucional à proteção de dados se projetará de maneira tal sobre esse intercâmbio que deverão ser exigidas: a) a comprovação do interesse público da medida, afastada qualquer possibilidade de o fornecimento desses dados atender a interesses pessoais ou privados; b) e

¹⁵ Lei nº 9.613/98, art. 15: O COAF comunicará às autoridades competentes para a instauração dos procedimentos cabíveis, quando concluir pela existência de crimes previstos nesta Lei, de fundados indícios de sua prática, ou de qualquer outro ilícito.

que a solicitação de dados esteja devidamente motivada para eventual controle de legalidade pelo Poder Judiciário.

Em outras palavras, nesses casos de pedido/comunicação de autoridades investigativas ao COAF, o compartilhamento somente será válido quando na solicitação ficar demonstrado o interesse público e a devida motivação. Nessa demonstração, portanto, compreende-se, a nosso entender, a exposição bem fundamentada da hipótese investigada, as pessoas investigadas, os indícios já existentes, o procedimento já instaurado – sem prejuízo de outros aspectos ainda a serem desenvolvidos.

Segundo o relatório de atividades do COAF referente ao ano de 2021, esse é um procedimento que já ocorre nessas hipóteses de “comunicação de autoridades competentes”, ou seja, pedidos de eventuais relatórios. Segundo o relatório:

As informações sobre indícios da prática do crime de lavagem de dinheiro devem ser apresentadas pela autoridade responsável pela correspondente investigação, na forma de Comunicação de Autoridade Competente, indicando o número e a natureza do procedimento instaurado, os fundados indícios da existência do ilícito investigado, bem como a identificação das pessoas envolvidas.¹⁶

É a fundamentada exposição dos indícios do ilícito investigado que demonstrará o interesse público-institucional na obtenção dos dados, autorizando que COAF busque, em seu banco de dados, por informações eventualmente úteis à investigação penal. Por certo que essa motivação da solicitação não se confunde com a fundamentação em ambiente judicial, mas que seja capaz de demonstrar, para cada pessoa apontada, que a obtenção dos dados é de interesse público, para fins de prosseguimento de investigação penal já existente.

Caso contrário, não sendo realizada essa exposição de motivos, ou não justificando o pedido quanto a esta ou aquela pessoa, a busca pelo COAF se traduzirá em *fishing expedition*¹⁷ ou, nas palavras da Ministra Carmen Lúcia, “arapongagem”, porquanto autoridades de

¹⁶ Disponível em <https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/RACoaf2021publica20220311.pdf>. Acesso em 20 maio 2022.

¹⁷ Alexandre Morais da Rosa e Thiago Bunning Mendes assim definem *fishing expedition*: *Fishing expediton* ou “pescaria probatória” é o meio de “investigação especulativa indiscriminada, sem objetivo certo ou declarado que, de forma ampla e genérica, ‘lança’ suas redes com esperança de ‘pescar’ qualquer prova para subsidiar uma futura acusação ou para tentar justificar uma investigação/ação já iniciada. Na doutrina alemã, Bernd Schunemann chama de “efeito hidra”, consistente na busca permanentemente ampliada (estendida) e com isso invasiva, com a finalidade de alcançar vestígios de fatos que inclusive se desconhece (SCHÜNEMANN, Bernd. **La Reforma del Proceso Penal**. Madrid: Dykinson, 2005, p. 33). Disponível em <http://www.ibadpp.com.br/uma-proposta-de-limites-para-evitar-o-fishing-expedition-a-partir-da-decisao-do-min-celso-de-mello-no-inq-4-831-df-por-alexandre-morais-da-rosa-e-tiago-mendes/>. Acesso em 20 maio 2022.

persecução estarão se utilizando do poder informacional do órgão de inteligência para injustificadamente invadir a vida privada, o que afronta, de maneira profunda, o Estado Democrático de Direito.

A imposição desses limites da solicitação motivada e do interesse público é o que garantirá a tão importante separação informacional entre unidade de inteligência financeira e órgãos de persecução, de modo que as respectivas instituições tenham acesso a dados de forma constitucionalmente compatível com as suas finalidades.

Sobre essa separação, Orlandino Gleizer, Lucas Montenegro e Eduardo Viana¹⁸ explicam que a sua necessidade se deve justamente ao fato de os serviços de inteligência terem a faculdade de “devassar a vida dos cidadãos”:

Há, no direito alemão, uma intensa discussão em torno do denominado *imperativo de separação* (*Trennungsgebot*). Sob essa rubrica, são discutidas diferentes formas de separação, p. ex. em relação às faculdades, à organização, ao corpo de servidores, às informações etc. Em especial, esse imperativo de separação faz-se valer entre as atividades de inteligência, de um lado, e as atividades de segurança pública e persecução penal, de outro. A razão para isso reside no vasto campo de atuação dos serviços de inteligência, que lhes confere amplo poder de acesso a informações dos cidadãos. Conforme afirmado, serviços de inteligência atuam em um campo prévio, sem que estejam submetidos a um ensejo para entabular investigação, levantar e analisar dados. Essa faculdade de devassar a vida dos cidadãos sem um ensejo concreto põe sob tensão a noção de Estado de Direito. A forma de equalizar essa desproporção do poder do Estado consiste em submetê-lo a um imperativo de separação.

A imposição de balizas objetivas nesse intercâmbio entre COAF e autoridades de investigação penal, a nosso entender, é o que garantirá essa separação informacional, de modo que o compartilhamento se dê rigorosamente dentro do Estado Democrático de Direito.

5. O acesso às comunicações entre COAF e Autoridades Investigativas como controle de legalidade diferido acerca do tratamento de dados pessoais

Como aqui já afirmado pela doutrina de Laura Schertel e Ingo Sarlet, o reconhecimento do direito à proteção de dados, especialmente em sua face de direito à autodeterminação

¹⁸ GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. O direito de proteção de dados no processo penal e na segurança pública. 1. ed. Rio de Janeiro: Marcial Pons, 2021. p. 53.

informativa, transcende a esfera do direito à privacidade, nele compreendido a sua esfera íntima e individual.

A privacidade, antes compreendida como um direito estático e negativo, de ser deixado em paz, impondo a terceiros um “não fazer”, um “não invadir”, adquire um regime jurídico tal que confere ao titular dos dados pessoais, nas palavras de Ingo Sarlet, “*poderes positivos e dinâmicos com vistas ao controle sobre a coleta e o processamento dos dados que lhe digam respeito*”. Nas palavras do Ministro Gilmar Mendes, em voto na ADI 6.529, corolário da proteção aos dados pessoais é a preservação a um “*devido processo informacional*”, no qual o titular dos dados possa ter “*o direito de evitar exposições de seus dados sem possibilidades mínimas de controle*”.

É verdade que certas atividades – como as de inteligência e de investigação criminal – não poderão se submeter a um pleno e completo regime de proteção aos dados pessoais, sob pena de se tornarem inócuas. A comunicação ao titular sobre o tratamento e compartilhamento, por exemplo, poderá gerar prejuízos à própria finalidade das instituições.

Isso não significa que o processamento e compartilhamento de dados pessoais para fins de persecução penal ou segurança pública não se submeta a um regime de controle – ainda que mínimo – pelo titular. Se, por um lado, postulados como transparência e consentimento não deverão ter plena incidência, por outro, o controle diferido acerca da regularidade no tratamento desses dados deve ser garantido.

Nesse sentido, Orlandino Gleizer, Lucas Montenegro e Eduardo Viana¹⁹ ensinam que, como forma de reduzir efeitos prejudiciais provocados por intervenções ocultas – tais como as de investigação – em dados pessoais, é direito do titular ter acesso a esse processamento, “*tão logo inexistam razões para mantê-lo em segredo*”. Vejamos:

(...) é preciso que todos os titulares afetados sejam informados a respeito das intervenções que sofreram, a fim de que, sentindo-se lesados, possam tomar providências jurídicas a respeito. Para tanto, é necessário que também lhes sejam garantidos mecanismos jurídico-procedimentais suficientes para ver apreciadas as lesões ou ameaças a seus direitos (como garante o art. 5º XXXV CF).

Assim, o reconhecimento de direitos ao titular de dados é uma forma de mitigação dos prejuízos estruturais causados pelo levantamento e pelos demais processamentos de seus dados pessoais, frequentemente ocorridos sem sua ciência e, por consequência, sem seu consentimento. Como é perceptível, esses direitos são apenas mais uma consequência lógica da proteção de dados pessoais por meio de

¹⁹ GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. O direito de proteção de dados no processo penal e na segurara pública. 1. ed. Rio de Janeiro: Marcial Pons, 2021. p. 53.

cláusulas de direitos fundamentais, em razão do princípio da proporcionalidade. A ideia aqui é tentar reduzir os desnecessários efeitos prejudiciais do processamento de dados ao indivíduo por meio da garantia de *transparência* do processamento e de *oposição jurídica* por parte do titular dos dados; em outras palavras, permitindo sua *compreensão e controle* dos dados pessoais.

(...)

Os âmbitos da segurança pública e do processo penal, especificamente, são casos que merecem tratamento especial em relação aos direitos do titular. E isso pela simples razão de que a efetividade da proteção contra perigos e do processo penal, muitas vezes, depende de *meios de investigação secretos ou ocultos*, os quais, por sua natureza, restringem a tomada de conhecimento da intervenção informacional pelo afetado. Isso, por si só, agrava significativamente a intensidade da intervenção, porque, sem ciência a seu respeito, não pode o afetado opor-se juridicamente ao processamento. Por essas razões, essas medidas preveem, em regra, um direito do afetado de ser notificado sobre o processamento oculto *tão logo inexistam razões para mantê-lo em segredo*, garantindo ao afetado a possibilidade de verificar judicialmente a legitimidade do processamento realizado e as demais formas de controle cabíveis.

Não se sustenta, aqui, que haja acesso pelo titular de dados compartilhados pelo COAF a toda a cadeia de produção dos relatórios de inteligência, desde o envio pelas entidades obrigadas, muito menos acesso aos tratamentos internos conferidos pelas fases de análise do órgão.

Compreendemos, na verdade, na linha da premissa adotada de que haverá maior incidência de direitos fundamentais nas etapas procedimentais com finalidade de persecução penal, que assistirá direito de acesso às comunicações entre COAF e autoridades investigativas, como exercício do poder de controle do titular sobre a forma pela qual seus dados pessoais foram tratados pelas instituições públicas brasileiras.

Afinal, a partir do momento em que a persecução penal se desenvolveu a ponto de chegar ao conhecimento formal do titular dos dados compartilhados, parece-nos que o acesso às comunicações, isto é, o rastreamento do caminho pelo qual seus dados percorreram, integra o direito de acesso à informação do indivíduo.

Nesse sentido, o artigo 5º, XXXIII, CF, prevê que *todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado*. A exceção é para compartilhamento com fim de segurança da sociedade e do Estado, hipóteses típicas de atividade de inteligência. O compartilhamento com fins de investigação penal – como é o caso de disseminação de relatórios de inteligência financeira a órgãos de persecução – não está contido nessa exceção

constitucional, de modo que a comunicação desse canal pode, e deve, ser considerada objeto do direito ao acesso à informação.

Portanto, o pleno exercício do direito à proteção dos dados pessoais, a nosso entendimento, confere o *poder positivo* de ter um controle diferido acerca desse compartilhamento, podendo o titular tomar conhecimento das peças que compuseram essa transmissão entre COAF e autoridades investigativas.

Se, a partir da filtragem constitucional aqui já exposta, o compartilhamento de dados pelo COAF deve observar, ao menos, esses quatro limites – a) interesse público; b) solicitação motivada; c) impossibilidade de transferência de dados sujeitos à reserva de jurisdição; d) procedimento formalmente instaurado e canal seguro –, parece-nos de extrema relevância garantir um controle mínimo – ainda que diferido – ao titular dos dados compartilhados, concedendo-lhe acesso às comunicações para controle de legalidade à luz desses parâmetros objetivos.

Em especial, nos casos de solicitações de informações por autoridades investigativas ao COAF, o acesso à motivação apresentada, com datas, número de procedimentos, exposição dos indícios, certificação do autor, dentre outros fatores, é o que cumprirá com o dever de transparência sobre o tratamento de dados pessoais.

Em um paralelo aplicável a esse intercâmbio entre COAF e autoridades de investigação, o voto do Ministro Luís Roberto Barroso, na ADI 6.529, embora não tenha se fundamentado na proteção de dados pessoais, propõe, como *obiter dictum*, a necessidade de a solicitação dos dados – por agentes da ABIN – ser documentada, para “*que se saiba sempre quem entregou e quem recebeu, porque isso é importante para o controle da cadeia de legalidade*”. Com mais razão ainda esse raciocínio deve ser aplicado às disseminações de relatórios do COAF para órgãos de persecução, tendo em vista a sua finalidade de investigação penal.

Aliás, do filtro aplicado pelo Supremo Tribunal Federal, vê-se que essa solicitação motivada poderá ser submetida a *eventual controle de legalidade pelo Poder Judiciário*. Por certo que esse controle pelo Poder Judiciário deverá ocorrer com a participação do titular dos dados, sujeito da garantia constitucional de proteção à privacidade/personalidade, justamente conferindo-lhe acesso a essa solicitação/comunicação. Afinal, incide aqui o princípio da inafastabilidade da jurisdição, prescrito no artigo 5º, XXXV, CF: “*a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito*”.

Esse ponto, portanto, reforça o que aqui sustentamos: que, após a transmissão desses dados, o titular dos dados compartilhados deverá ter acesso a essa solicitação, para, perante o Poder Judiciário, exercer controle de legalidade.

6. Conclusão

Em suma, podemos concluir que, passando o compartilhamento de dados pelo COAF às autoridades investigativas pelo filtro constitucional da proteção de dados pessoais, parece que alguns impactos objetivos podem ser identificados, especialmente à luz da interpretação conforme conferida pelo Supremo Tribunal Federal, na ADI 6.529.

A partir da premissa de que o compartilhamento de dados do COAF para fins de investigação penal deverá ter uma incidência maior de direitos fundamentais do que o intercâmbio de informações para fins de inteligência (segurança da sociedade e do Estado), tudo indica que os limites impostos ao compartilhamento de dados entre agências de inteligência, julgado na ADI 6.529, também terão aplicação na transmissão de informações pelo COAF às autoridades investigativas.

Exigências como a) comprovação do interesse público; b) a solicitação de compartilhamento ser motivada para eventual controle de legalidade pelo Poder Judiciário; c) impossibilidade de transferência de dados sujeitos à reserva de jurisdição; d) e a existência de procedimentos formalmente instaurados e de um sistema seguro, com registro de acesso; devem ser aplicadas a essa etapa do tratamento de dados pelo COAF (disseminação aos órgãos de persecução), resguardadas as devidas particularidades.

Como expressão do direito constitucional à proteção de dados pessoais, faz sentido que o titular dos dados compartilhados exerça um controle mínimo sobre essa transmissão, ainda que de forma diferida, isto é, após o atingimento dos fins desse compartilhamento, para que se certifique da sua legalidade ou não.

Focalizando nessa etapa do tratamento de dados pelo COAF (disseminação), entendemos que esse controle sobre a transmissão pelo seu titular deve ser aperfeiçoar por meio do acesso às comunicações entre unidade de inteligência financeira e autoridade de persecução penal, sobretudo à solicitação de compartilhamento eventualmente feitas por essas autoridades.

Afinal, de nada adiantaria – ou praticamente nada – se se impuser limites objetivos para o compartilhamento, em observância aos direitos da personalidade, sem que se disponibilizem meios de controle ao titular dos dados.

Garantir a proteção de dados pessoais, como visto, não se trata só de um direito negativo e estático de ser deixado em paz, mas de consagrar poderes positivos de manter o controle do titular sobre seu tratamento, mesmo que na forma de uma transparência posterior ao processamento.

O tema – aplicação do direito à proteção de dados pessoais ao compartilhamento de dados pelo COAF às autoridades investigativas –, de modo geral, é de extremas amplitude e profundidade, estando, por isso, cada vez mais, sendo alvo de estudos acadêmicos para aperfeiçoar essa atividade que tem adquirido protagonismo no combate a crimes de lavagem de dinheiro, terrorismo, entre outros.

As contribuições do presente trabalho, embora pontuais diante da imensidão teórica que permeia o tema, exploram questões ainda controvertidas, que sem dúvida merecerão maiores aprofundamentos.

7. Bibliografia

ALEMANHA. Tribunal Constitucional Federal. *BVerfGE* 65, 1 (1983).

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 maio 2022.

_____. Emenda Constitucional 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 20 maio 2022.

_____. Lei Complementar 102, de 11 de julho de 2000. Altera dispositivos da Lei Complementar no 87, de 13 de setembro de 1996, que "dispõe sobre o imposto dos Estados e do Distrito Federal sobre operações relativas à circulação de mercadorias e sobre prestações de serviços de transporte interestadual e intermunicipal e de comunicação, e dá outras providências". Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp102.htm#:~:text=Altera%20dispositivos%20

da%20Lei%20Complementar,%2C%20e%20d%C3%A1%20outras%20provid%C3%AAs%22. Acesso em: 20 maio 2022.

_____. Lei 9.883, de 7 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/19883.htm. Acesso em: 20 maio 2022.

_____. Lei 9.613, de 3 de março de 1998. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/19613.htm. Acesso em: 20 maio 2022.

_____. Lei 12.683, de 9 de julho de 2012. Altera a Lei nº 9.613, de 3 de março de 1998, para tornar mais eficiente a persecução penal dos crimes de lavagem de dinheiro. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/12683.htm. Acesso em: 20 maio 2022.

_____. Supremo Tribunal Federal (Plenário). ADI 6.529/MC. Voto do Ministro Edson Fachin. Rel. Min. Cármen Lúcia. Brasília, 11 de outubro de 2021. Diário de Justiça, Brasília-DF, 21 de outubro de 2021. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5972837>. Acesso em: 20 maio 2022.

_____. Supremo Tribunal Federal (Plenário). RE 1.055.941/SP.. Min. Dias Toffoli. Brasília, 4 de dezembro 2019. Diário de Justiça, Brasília-DF, 5 de outubro de 2020. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5213056>. Acesso em: 20 maio 2022.

CONSELHO DE CONTROLE DE ATIVIDADES FINANCEIRAS (Brasil). **Relatório de Atividades Coaf 2021**. Brasília, 2021. Disponível em <https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/RACoaf2021publica20220311.pdf>. Acesso em: 17 maio 2022.

EUROPEAN DATA PROTECTION SUPERVISOR (União Europeia). **Opinion 12/2021: on the anti-money laundering and countering the financing of terrorism.** Bruxelas, 2021. Disponível em https://edps.europa.eu/data-protection/our-work/publications/opinions/anti-money-laundering-and-countering-financing_en. Acesso em: 19 maio 2022.

LEGISLATIVE OBSERVATORY: EUROPEAN PARLIAMENT (União Europeia). **2021/0250(COD) - Prevention of the use of the financial system for the purposes of money laundering or terrorist financing: mechanisms to be put in place by the Member States.** Estrasburgo, 2021.

UNIÃO EUROPEIA. Diretiva 95/46/CE, 24 de outubro de 1995. Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <https://www.conjur.com.br/dl/diretiva-europeia.pdf>. Acesso em: 20 maio 2022.

GARFINKEL, SIMSON. **Database Nation: the death of privacy in the 21th Century.** California: O'Reilly Media, 2000.

GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. **O direito de proteção de dados no processo penal e na segurara pública.** 1. ed. Rio de Janeiro: Marcial Pons, 2021.

MENDES, Laura Schertel. **Autodeterminação informativa: a história de um conceito.** Pensar: Revista de Ciências Jurídicas, Fortaleza, V 25, nº 4, out/dez 2020.

_____, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva, 2014.

MORAIS, Alexandre; MENDES, Tiago. **Uma proposta de limites para evitar o fishing expedition a partir da decisão do Min. Celso de Mello no Inq. 4.831/DF.** Instituto Baiano de Direito Processual Penal. Disponível em <http://www.ibadpp.com.br/uma-proposta-de-limites-para-evitar-o-fishing-expedition-a-partir-da-decisao-do-min-celso-de-mello-no-inq-4-831-df-por-alexandre-morais-da-rosa-e-tiago-mendes/>. Acesso em 20 maio 2022.

SARLET, Info Wolfgang; Fundamentos Constitucionais: O Direito Fundamental à Proteção de Dados. *In: Tratado de proteção de dados pessoais*, coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021.