

# O RE 1.055.941: um Pretexto para Explorar Alguns Limites à Transmissão, Distribuição, Comunicação, Transferência e Difusão de Dados Pessoais pelo COAF

**HELOISA ESTELITA<sup>1</sup>**

Fundação Getúlio Vargas (FGV/SP).

**RESUMO:** Em dezembro de 2019, o Supremo Tribunal Federal decidiu que o COAF poderia revelar informações sigilosas (financeiras) para as autoridades de persecução penal sem a necessidade de autorização judicial prévia (RE 1.055.941). Essa decisão é utilizada no presente trabalho como pretexto para examinar o tratamento de dados pessoais pelo COAF sob a luz da gramática da proteção de dados pessoais. Analisa-se o tratamento de dados pessoais, sensíveis e sigilosos no âmbito das tarefas desempenhadas pelo COAF, especialmente sob o viés das comunicações que esse órgão faz para autoridades nacionais e internacionais. O exame evidencia que há atividades sendo desempenhadas sem normas autorizativas de intervenção em direitos fundamentais, apontando para a necessidade de reforma legislativa para adequar o tratamento de dados pessoais aos *standards* atuais de proteção desse direito fundamental.

**PALAVRAS-CHAVE:** Lavagem de dinheiro; unidade de inteligência financeira; proteção de dados; sigilo financeiro.

**ABSTRACT:** In December 2019, the Brazilian Supreme Court, ruled that the Brazilian Financial Intelligence Unit – FIU (COAF) could share confidential (financial) information to law enforcement authorities without prior judicial authorization (RE 1.055.941). This decision is used in the present paper as the background to review the processing of personal data by COAF under the grammar of personal data protection. The processing of personal, sensitive, and confidential data is analyzed vis-à-vis the tasks performed by COAF, particularly regarding the reports this agency makes to national and international authorities. The examination shows that there are activities being carried out without the authorizing norms for intervention in fundamental rights, which points towards the need for legislative reform to adapt the processing of personal data to the current standards of protection of this fundamental right.

---

1 Ocid: <http://orcid.org/0000-0002-5054-4116>.

KEYWORDS: Money laundering; financial intelligence unit; data protection; bank secrecy.

SUMÁRIO: I – Introdução: A matéria discutida no STF no RE 1.055.941; II – As premissas; II.1 Proteção de direitos fundamentais: legalidade e proporcionalidade; II.1.a) Dever de abstenção e exigência de normas autorizativas; II.1.b) Normas autorizativas e normas de competência (atribuição); II.1.c) Proteção de dados pessoais como direito fundamental; II.1.d) Separação informacional; II.1.e) Proteção de dados no Brasil; II.2 Privacidade e proteção de dados no tratamento para as medidas de controle e prevenção da lavagem de capitais; II.2.a) Direito à privacidade, direito à proteção de dados e autodeterminação informacional; II.2.b) Dados pessoais, dados pessoais sensíveis e dados pessoais sigilosos; II.3 O tratamento de dados pessoais pelo COAF; II.3.a) Competências e tarefas atribuídas ao COAF; II.3.b) Dados pessoais; II.3.c) Dados pessoais financeiros sigilosos; III – Consequências; III.1 RIFs de ofício (“disseminação espontânea”); III.2 RIFs a pedido (“disseminação a pedido”); III.3 Intercâmbio internacional entre UIFs; IV – À guisa de conclusão; Referências.

## I – INTRODUÇÃO: A MATÉRIA DISCUTIDA NO STF NO RE 1.055.941

Em dezembro de 2019, o Supremo Tribunal Federal (STF), ao decidir, com repercussão geral, as controvérsias a ele submetidas no Recurso Extraordinário nº 1.055.941, estabeleceu (1) ser “constitucional o compartilhamento dos relatórios de inteligência financeira da UIF [...] 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”; e (2) que o “compartilhamento pela UIF [...] 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”<sup>2</sup>.

O ponto central era saber se a revelação de informações sigilosas (financeiras) pelo Conselho de Controle de Atividades Financeiras (doravante COAF) às autoridades de persecução penal por meio dos relatórios de inteligência financeira (RIFs) necessitaria ou não de autorização judicial prévia<sup>3</sup>. A resposta foi negativa, pois haveria permissão legal para isso (art. 15 da Lei nº 9.613/1998 [Lei de Lavagem de Dinheiro, adiante LLD]).

O tribunal também apreciou as modalidades de relatórios de inteligência financeira: espontâneos (de ofício ou de disseminação espontânea) ou “por encomenda” (disseminação a pedido), muito embora não tenha

2 Ementa do acórdão proferido pelo STF no RE 1.055.941, Tribunal Pleno, Rel. Min. Dias Toffoli, J. 04.12.2019, DJe 06.10.2020. O tema não era objeto de discussão na formulação originária do RE (cf. fl. 2699).

3 STF, RE 1.055.941, fl. 2706.

se formado maioria para que pudesse cravar uma posição sobre a admissibilidade deste último (Borges, 2021, p. 85)<sup>4</sup>, tendo os ministros ao menos concordado quanto à “proibição da realização pelo COAF de investigações criminais prospectivas (e.g., *fishing expeditions*)” (Borges, 2021, p. 90).

A discussão envolvia, essencialmente, dois diplomas legais: a LLD e a Lei Complementar nº 105/2001 (adiante, LC 105). Lembremos que, em dezembro de 2019, quando a decisão foi proferida, nem a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) estava em vigor, nem mesmo o STF tinha julgado as ADIns 6.387-MC-Ref/DF, 6.388-MC-Ref/DF, 6.389-MC-Ref/DF, 6.390-MC-Ref/DF e 6.393-MC-Ref/DF, nas quais veio a reconhecer, em maio de 2020, que

o tratamento e a manipulação de dados pessoais não de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecutorias da liberdade individual (art. 5º, *caput*), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos.<sup>5</sup>

Tampouco a PEC 17/2019, que inclui a proteção de dados pessoais no rol dos direitos fundamentais, tinha sido aprovada.

Isso ajuda a explicar a razão pela qual, na discussão, a Corte não se fez uso, de forma geral<sup>6</sup>, da gramática da proteção de dados pessoais, que viria a ser incorporada com mais força em seu discurso a partir de 2020. Uma outra explicação se deve, evidentemente, à exclusão, do âmbito de regência da LGPD, do tratamento de dados pessoais “realizado para fins exclusivos de [...] segurança pública” ou de “atividades de investigação e repressão de infrações penais” (art. 4º, III, da LGPD).

Fixado esse contexto, pretendo analisar, de uma forma um pouco mais ampla, a questão empregando a dogmática dos direitos fundamentais – especialmente do direito fundamental à proteção de dados pessoais –, cujos elementos centrais são a imposição de um dever de abstenção do Estado frente a direitos fundamentais e a exigência de que as intervenções sejam veiculadas por lei autorizativa proporcional.

---

4 Neste artigo, o autor faz um exame exaustivo das questões debatidas no julgamento do RE.

5 STF, ADIn 6.387-MC-Ref, Tribunal Pleno, Min. Rosa Weber, DJe 12.11.2020, J. 07.05.2020. Um exame detalhado em Souto; Rosal, 2021.

6 A exceção fica por conta do voto do Ministro Gilmar Mendes, que contém tópico dedicado ao direito fundamental à privacidade e ao sigilo de dados bancários e fiscais (fls. 3043 e ss.).

A intenção não é fazer uma crítica *ex post facto* – o que seria injusto –, mas ampliar o olhar, examinando o rendimento da aplicação dessa dogmática à matéria examinada<sup>7</sup>. Essa ampliação é necessária na medida em que o COAF não trata apenas dados pessoais *sigilosos*, como os financeiros, mas também (muitos) dados pessoais não protegidos por sigilo, como, por exemplo, os dados pessoais relativos a transações com joias, imóveis etc.<sup>8</sup> O assento constitucional dessa gramática e sua aplicação *específica* à proteção de dados na esfera penal foi desenvolvida entre nós, recentemente, por Greco (2019) e por Gleizer, Montenegro e Viana (2021), de cujas premissas partirei.

O trabalho se divide em duas grandes partes: premissas e consequências. Na primeira, serão abordadas as ferramentas normativas e dogmáticas necessárias para enfrentar a questão das comunicações feitas pelo COAF. Na segunda, essas ferramentas serão empregadas para abordar, especificamente, as comunicações do COAF para autoridades competentes.

## II – AS PREMISSAS

As atividades desempenhadas pelo COAF no tratamento de dados pessoais intervêm em direitos fundamentais e têm a finalidade de convocar o aparato penal contra pessoas suspeitas da prática de infrações penais, que poderão dar ensejo a uma segunda intervenção em direitos fundamentais da mais alta gravidade. Por essas razões, o ponto de partida da análise deve ser o da teoria dos direitos fundamentais (Greco, 2019, p. 30 e ss.) ou da dogmática constitucional da proteção de dados (Gleizer; Montenegro; Viana, 2021, p. 11 e ss.; Greco; Gleizer, 2019, p. 1485-1488).

### II.1 PROTEÇÃO DE DIREITOS FUNDAMENTAIS: LEGALIDADE E PROPORCIONALIDADE

#### II.1.a) Dever de abstenção e exigência de normas autorizativas

Direitos fundamentais são, em primeiro lugar, direitos de defesa dirigidos contra o Estado: a um direito fundamental corresponde um dever

---

7 Já em 1991, ou seja, há 30 anos (!), Rogall identificava o efeito que o direito constitucional e o direito de proteção de dados passaram a ter no fortalecimento dos direitos fundamentais dos afetados por investigações e ações penais (Rogall, 1991, p. 907).

8 Serão considerados dados financeiros sigilosos aqueles disciplinados na LC 105. Muitas das pessoas obrigadas a comunicar operações em espécie e suspeitas ao COAF (art. 9º da LLD) não estão abarcadas pelo espectro de proteção do sigilo financeiro estabelecido pelo art. 1º da LC 105, cujo critério de proteção não é a natureza dos dados, mas quem os trata: as instituições financeiras.

do Estado de se abster de intervir em seu âmbito de proteção<sup>9</sup>. Sendo a regra a abstenção e a exceção a intervenção, toda intervenção em direito fundamental tem de ser justificada. Essa justificação se assenta em três pressupostos: um formal e dois materiais. A intervenção tem de ser veiculada em lei em sentido formal, ou seja, uma autorização democrática dada pelo legislador por meio de uma norma autorizativa como exige, entre nós, o art. 5º, II, da CF<sup>10</sup>; “não pode atingir o núcleo dos direitos fundamentais” (Greco; Gleizer, 2019, p. 1487), e, finalmente, tem de ser proporcional, ou seja, idônea, necessária, adequada e proporcional em sentido estrito para a promoção de um fim legítimo<sup>11</sup>.

Dentre esses pressupostos, chamo a atenção para o primeiro, pois, segundo adverte Greco, “até hoje não descobrimos todo o potencial desse dispositivo [o art. 5º, II, da CF] [...] [um] verdadeiro gigante adormecido” (2019, p. 36)<sup>12</sup>. A exigência de reserva legal “significa que, sem lei específica que preveja de forma relativamente clara a intervenção e lhe imponha limites materiais e procedimentais, não será lícito intervir no direito fundamental” (Greco, 2019, p. 37)<sup>13</sup>. Exige-se, assim, que a intervenção seja autorizada em lei em sentido formal que a veicule de forma precisa, sendo vedada sua extensão a hipóteses nela não previstas<sup>14</sup>.

### II.1.b) Normas autorizativas e normas de competência (atribuição)

E é neste ponto que a distinção entre normas *autorizativas* e normas de *competência*<sup>15</sup> mostra toda sua importância. Nesse sentido, quando fixa competências, “o Estado simplesmente distribui entre os seus o que incumbe a quem. Parece claro, contudo, que uma distribuição interna de tarefas

---

9 Greco, 2019, p. 35; Gleizer; Montenegro; Viana, 2021, p. 103, 118-123; Dimoulis; Martins, 2021, p. 179 e ss.

10 CF, art. 5º, II: “ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei”.

11 Greco, 2019, p. 36; Gleizer; Montenegro; Viana, 2021, p. 49 e ss.; Silva, 2021, p. 103, 118-123; Dimoulis; Martins, 2021, p. 225 e ss.; Mendes; Branco, 2018, Capítulo 2, 1.3. O exame dessa exigência não será feito nesta oportunidade, mas apenas registro que não há dúvidas sobre o fato de que o Estado precisa de informações para cumprir seus deveres de prover segurança e de perseguir aqueles que praticam crimes (nesse sentido, Rogall, 1991, p. 925), o que tem um papel central no juízo de proporcionalidade.

12 No mesmo sentido, Gleizer; Montenegro; Viana, 2021, p. 41.

13 Também Silva, 2021, p. 119-120.

14 Greco; Gleizer, 2019, p. 1487. Sobre intervenções bagatelares e autorizações veiculadas por meio de cláusulas gerais, cf. Greco, 2019, p. 39-40; Gleizer; Montenegro; Viana, 2021, p. 48, 85-86, 97-99, com ulteriores referências.

15 Usarei o termo competência no decorrer do texto para ser fiel à escolha linguística feita por Greco, que não o limita à competência jurisdicional, mas abrange também normas que determinam as *tarefas, funções e atribuições* de órgãos e agentes estatais, muito embora talvez o termo atribuição fosse mais adequado ao ambiente jurídico brasileiro.

não dá a ninguém um direito de adentrar na esfera de um terceiro”, o que exige, como visto, autorização clara e taxativa. Do que decorre que não se pode “derivar da existência de uma competência uma autorização” (Greco, 2019, p. 37-38).

Greco assim exemplifica essa diferença: “Incumbe ao Ministério Público proceder à investigação preliminar tão logo existam pontos de apoio fáticos no sentido do possível cometimento de um delito”; essas “normas de competência não dão ao Ministério Público, contudo, o direito de intervir na esfera jurídica de quem quer que seja”, assim, se for necessária uma interceptação telefônica ou uma busca, “terá de atender aos pressupostos dos dispositivos específicos que fundamentam cada uma dessas medidas, isto é, às normas autorizativas específicas” (Greco, 2019, p. 38<sup>16</sup>). Ajustando o exemplo ao direito positivo brasileiro, o fato de o Ministério Público ter competência para “promover, privativamente, a ação penal pública, na forma da lei” e, para isso, “requisitar diligências investigatórias e a instauração de inquérito policial, indicados os fundamentos jurídicos de suas manifestações processuais” (art. 129, I e VIII, da CF), não autoriza seus membros a entrarem em domicílios, apreenderem objetos, interceptarem comunicações, acessarem comunicações privadas armazenadas, compartilharem dados pessoais sem autorização legal, terem acesso a dados pessoais financeiros protegidos por sigilo etc.<sup>17</sup> Seguindo nessa linha, o fato de “o constituinte atribuir às polícias militares a competência para exercer policiamento ostensivo e preservação da ordem pública (art. 144, § 5º, da CF) não implica, automaticamente, autorização para entrada no domicílio dos cidadãos, mesmo que isso seja necessário para o exercício de tais competências” (Gleizer; Montenegro; Viana, 2021, p. 42)<sup>18</sup>, o mesmo valendo para as atribuições que o art. 6º do Código de Processo Penal (CPP) endereça à

---

16 E acrescenta: “Isso significa que, como regra, a norma tem de prever a concreta medida interventiva, e isso não apenas por meio de uma conceituação ‘funcional’ (obter informações, descobrir, esclarecer etc.), que é a linguagem das normas determinadoras de tarefas ou de competências, e sim com termos mais ‘naturalísticos’, que descrevam o concreto meio de que as instâncias de persecução se valerão para cumprir a função que lhes é legalmente atribuída” (2019, p. 39).

17 Em sentido similar, reportando-se ao § 161, I, S. 1, StPO (Código de Processo Penal alemão), que garante ao Ministério Público o poder de realizar diligências investigativas diante da suspeita da prática de crime ou de fazê-lo por meio da polícia, afirma Rogall que tal norma não autoriza a intervenção em direitos fundamentais, que só podem ser feitas pelo Ministério Público diante de normas legais de autorização veiculadas de forma clara (Rogall, 1985, p. 6-7).

18 Essa mesma dicotomia se vê no direito de polícia alemão (Greco, 2019, p. 40-41).

autoridade policial quando tiver conhecimento da prática de infração penal: apreender objetos, colher provas, ouvir pessoas etc.<sup>19</sup>

A força dessa verdadeira *decorrência lógica* do regime constitucional de proteção de direitos fundamentais fica clara quando pensamos que seria muito fácil atraiçoar a garantia dos direitos fundamentais do art. 5º da CF (cláusulas pétreas) se, logo à frente, o Constituinte, por meio de meras regras de competência, negasse todo o catálogo de direitos fundamentais antes consagrados. Mais concretamente: se se entendesse que normas (ainda que constitucionais) de competência consubstanciassem uma “carta branca” aos agentes estatais para que, a pretexto de “bem” cumpri-las, por exemplo, aplicassem uma sanção penal sem o devido processo legal (art. 5º, LIV, da CF) ou privassem o cidadão de parte de seu patrimônio (art. 5º, *caput* e XXII, da CF), o sistema constitucional de proteção de direitos fundamentais ruiria duas ou três páginas à frente de sua consagração, pois as regras de competência se sobreporiam às normas garantidoras de direitos fundamentais. A CF traria, já em seu âmago, uma contradição evidente, uma espécie de *back door* para a negação dos direitos que acabara de garantir. Também o disposto no art. 60, § 4º, da CF se tornaria letra morta, inútil. Daí que, se levamos a sério o que dispõem os arts. 5º (especialmente seu inciso II<sup>20</sup>) e o 60, § 4º, IV, da CF, a afirmação de que *de uma regra de competência (atribuição) não decorre uma norma autorizativa* é uma decorrência lógica (também) de nosso direito (constitucional) positivo<sup>21</sup>.

### II.1.c) Proteção de dados pessoais como direito fundamental

Essas ideias se aplicarão à proteção de dados pessoais, seja ela entendida como um (novo) direito fundamental, seja como uma nova forma de proteção dos direitos gerais de personalidade<sup>22</sup>.

Seu reconhecimento tem como marco histórico decisões tomadas pela Corte Constitucional Federal alemã<sup>23</sup> que reconheceram que o livre

---

19 Manifestação clara dessa confusão no Parecer oferecido pela PGR no ARE 1.042.075, em 08.10.2021, e que trata do acesso ao conteúdo de *smartphone* apreendido pela polícia. Ali se toma a norma de competência/atribuição do art. 6º do CPP como se fosse uma norma autorizadora de intervenção em direitos fundamentais.

20 Cf. Greco, 2019, p. 40.

21 Cf. Gleizer; Montenegro; Viana, 2021, p. 41-43, com ulteriores referências, e também Greco, 2019, p. 36-37.

22 Gleizer, Montenegro e Viana (2021, p. 37-39) entendem que são vários os direitos conformando a proteção de dados pessoais; em sentido similar, Rogall, 1991, p. 926-927.

23 Sobre a origem e o desenvolvimento conceitual deste direito, além das obras já citadas, cf., ilustrativamente, entre nós, Mendes, 2020. Questionamentos acerca do acerto dessa decisão ao invocar um novo direito subjetivo em Rogall, 1985, p. 11-12, e 1991, p. 919-924.

desenvolvimento da personalidade depende do estabelecimento de limitações à obtenção, armazenamento, utilização e transferência de dados pessoais no contexto da capacidade atual de processamento, especialmente automatizado, de dados<sup>24</sup>. Como direito fundamental, também está sujeito a intervenções (restrições<sup>25</sup>), mas que devem estar previstas em lei e serem proporcionais.

É importante ter em mente que cada forma ou fase do tratamento de dados – a obtenção, o armazenamento, a utilização, a transferência etc.<sup>26</sup> – configura uma intervenção *autônoma* no direito à autodeterminação informacional, um direito que garante ao seu titular o controle sobre cada uso (tratamento) que é feito de seus dados. Por isso, cada forma de tratamento tem de ser objeto de autorização legal autônoma: “Uma norma que autoriza a obtenção de um dado não autoriza já automaticamente a utilização ou o armazenamento, muito menos a transferência” (Greco, 2019, p. 44<sup>27</sup>). Ademais, esse direito dá a seu titular o poder de saber para qual *finalidade* seus dados são coletados. Como “uma *alteração de finalidade* é um ato interventivo autônomo”, que necessita de expressa autorização legal (Gleizer; Montenegro; Viana, 2021, p. 50), tanto a coleta de um dado para fins de inteligência ou segurança pública (uma finalidade) como, por exemplo, a sua transmissão e utilização para fins de persecução penal (outra finalidade) têm de estar autorizadas em lei.

#### II.1.d) Separação informacional

O vínculo entre *finalidade* e *autorização* de tratamento de dados mostra toda sua força por meio da ideia de *separação informacional*. No que nos interessa, da separação entre atividades de inteligência, prevenção e persecução penais: “Os dados de inteligência não podem ser usados pela polícia preventiva, os da polícia preventiva não podem ser usados repressivamente, e vice-versa, sem expressa previsão legal” (Greco, 2019, p. 45). Como a alteração de finalidade é uma nova intervenção, tem de estar prevista em lei.

---

24 Greco, 2019, p. 43.

25 Interessante o ponto de vista de Rogall no sentido de que esse direito não deve ser entendido como um domínio sobre dados, mas um direito limitado de disposição sobre informações pessoais, que pode variar de acordo com os riscos para os interesses pessoais (Rogall, 1985, p. 11-12).

26 Cf. LGPD, art. 5º, X.

27 Em sentido diverso, diferenciando as formas de tratamento, sustenta Rogall que a coleta (*Erhebung*) e o armazenamento (*Speicherung*) são sempre intervenções em direitos fundamentais; a utilização ou a análise (*Nutzung oder Auswertung*) de dados coletados lícitamente não são intervenções, e a transmissão (*Übermittlung*) é uma intervenção, a não ser quando isso é feito dentro da mesma agência ou órgão que a coletou e desde que não haja mudança de finalidade (1991, p. 929-930).



Seria uma ousadia tentar, nesta oportunidade, delimitar os conceitos de *inteligência*, *segurança pública* e *persecução penal* em um ambiente normativo que não só não definiu (ou não o fez de forma clara) esses conceitos<sup>28</sup>, como no qual não há uma separação clara quanto às atividades por eles abarcadas<sup>29</sup>, e no qual há muitos resquícios normativos de nossa herança ditatorial<sup>30</sup>. Se a ausência de lineamentos normativos é, de um lado, perniciosa, de outro, confere certa liberdade para carregar as expressões com conteúdo semântico ligado às suas finalidades, pois finalidades diversas fundamentam amplitudes diversas de tratamento de dados, especialmente no que diz respeito à coleta.

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” (Gleizer; Montenegro; Viana, 2021, p. 54). Estão voltadas à precaução, razão pela qual não é necessário um ensejo (um incidente de segurança, uma prática criminosa etc.) para suas atividades. Por isso, há uma ampla margem de coleta, já que a missão aqui é, justamente, a reunião de informações, num estágio prévio à atividade policial<sup>31</sup>. Para que essa amplitude não se torne uma ameaça aos direitos fundamentais em um Estado Democrático<sup>32</sup>, os órgãos de inteligência não podem agir, mas devem transmitir as informações aos órgãos de investigação/persecução penal para que estes atuem<sup>33</sup>. As atividades de *segurança pública* têm finalidade de proteção contra perigos, um olhar prospectivo e *preventivo* e são condicionadas por um interesse em proteger bens jurídicos contra pe-

---

28 Estellita; Gleizer; Montenegro, 2020.

29 O Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Persecução Penal reflete essa insegurança quando inclui serviços de inteligência tanto no conceito de segurança pública como no de persecução penal (art. 5º, XXI e XXII), no que certamente precisa de aprimoramento; todavia, a inclusão foi feita justamente em virtude da indefinição quanto a essas atividades para que não se alegasse, à frente, que os serviços de inteligência operariam ao largo de uma lei geral de proteção de dados em matéria penal.

30 Lima; Bueno; Mingardi, 2016, p. 50.

31 Greco, 2019, p. 52.

32 Muito bem percebida pelo Ministro Édson Fachin no “Caso ABIN” (STF, MC-ADIn 6.529, Tribunal Pleno, Relª Min. Cármen Lúcia, DJe 15.10.2020, p. 58).

33 A finalidade da inteligência aqui tratada é diversa daquela regulada pela Lei nº 9.883/1999, que criou o Sistema Brasileiro de Inteligência, e que, apesar de refletir essa mesma ideia de coleta e disseminação de informações, parece liminar a inteligência àquela destinada à segurança do Estado (cf. art. 1º, § 1º). Daí que Abreu, ao analisar as expressões do art. 4º, III, da LGPD, conecte as ações de inteligência justamente ao âmbito da alínea c, “segurança do Estado” (Abreu, 2021, p. 594). Para um apanhado histórico da regulação dos serviços de inteligência entre nós, cf. Mota; Herkenhoff; Lira, 2018. Uma crítica minuciosa à indeterminação das normas de compartilhamento de dados no âmbito da Lei nº 9.833/1999 pode ser encontrada no voto do Ministro Gilmar Mendes no “Caso ABIN” (STF, MC-ADIn 6.529, Plenário, Relª Min. Cármen Lúcia, DJe 15.10.2020, p. 88).

rigos (Gleizer; Montenegro; Viana, 2021, p. 52-53<sup>34</sup>). A *persecução penal*, por fim, está voltada para a confirmação de uma suspeita, tem um olhar retrospectivo e condicionado por um interesse repressivo<sup>35</sup>.

Essas diferentes finalidades dão azo a diferentes autorizações de intervenção. As “normas autorizativas ou de faculdades autorizam ou facultam aos serviços de inteligência em primeira linha intervenções no direito à autodeterminação informacional”, e, por isso, as transferências de informações de um “órgão de inteligência a um órgão de polícia é regulada por lei e limitada em vários sentidos” (Greco, 2019, p. 54-55). Na relação entre segurança pública e persecução penal, por exemplo, a polícia pode utilizar câmeras para monitorar manifestantes em uma passeata, utilizando, assim, seu efeito inibidor para evitar lesões ao patrimônio (prevenção de perigos), mas, terminada a manifestação, não pode armazenar essas imagens, a não ser que exista uma norma legal autorizando a manutenção das imagens caso algum crime tenha sido cometido e os dados sejam necessários para a persecução penal (interesse repressivo)<sup>36</sup>.

### II.1.e) Proteção de dados no Brasil

Resumindo: o instrumental normativo até aqui reunido e que também se encontra em vigor entre nós compõe-se dos seguintes elementos: *dever de abstenção* frente a direitos fundamentais; *intervenções apenas quando autorizadas por lei proporcional*, do que decorre que *normas de competência (atribuição) não veiculam autorizações*; direito fundamental à proteção de dados pessoais/autodeterminação informacional que se insere nessa mesma gramática, exigindo *autorização em lei para cada forma de tratamento* com estrito atendimento à *finalidade legalmente prevista* para o tratamento, do que também decorre a exigência de *separação informacional*. Esse instrumental, é bom dizer, *independe* de uma lei federal de proteção de dados para o âmbito penal, muito embora uma tal lei seja desejável<sup>37</sup>.

34 Os autores dedicam todo um capítulo ao tema das intervenções informacionais para fins de segurança pública (p. 77 e ss.) e para o qual remeto o leitor. Cf. também Greco, 2019, p. 51-52; e Abreu, 2021, p. 595.

35 Gleizer; Montenegro; Viana, 2021, p. 52-53. No mesmo sentido, Abreu, 2021, p. 595.

36 O exemplo é de Gleizer; Montenegro; Viana, 2021, p. 53-54.

37 Especialmente para regular de forma geral, expressa e detalhada alguns aspectos dessa proteção específicos desse âmbito, como, por exemplo, prazos de eliminação, exercício direto e indireto dos direitos dos titulares, autoridade nacional de proteção de dados etc. No mesmo sentido, Abreu, 2021, p. 599. Esses aspectos foram tratados pelo Anteprojeto de Lei de Proteção de Dados para a segurança pública e a persecução penal, cf. Comissão de Juristas da Câmara dos Deputados, 2020.

Foi nessa estrutura normativa constitucional de proteção de direitos fundamentais, em vigor desde 1988, que o STF assentou o reconhecimento da proteção de dados pessoais<sup>38</sup> e o fez reconhecendo-o como um direito fundamental no qual só se pode intervir mediante autorização prevista em lei que observe os pressupostos de proporcionalidade da intervenção (devido processo legal material, nas palavras da Corte). Isso aconteceu no julgamento das ADIn 6.387-MC-Ref/DF, 6.388-MC-Ref/DF, 6.389-MC-Ref/DF, 6.390-MC-Ref/DF e 6.393-MC-Ref/DF<sup>39</sup>, sob relatoria da Ministra Rosa Weber, e no qual se discutia acerca da legalidade do compartilhamento de dados pessoais não anonimizados de usuários de empresas de telecomunicação com o IBGE (MP 954/2020)<sup>40</sup>. O ônus argumentativo que pesou sobre a Corte será bem mais leve a partir da promulgação da PEC 17/2019, aprovada pelo Senado em 20.10.2021, que inclui a proteção de dados pessoais no rol dos direitos fundamentais (art. 5º da CF).

## **II.2 PRIVACIDADE E PROTEÇÃO DE DADOS NO TRATAMENTO PARA AS MEDIDAS DE CONTROLE E PREVENÇÃO DA LAVAGEM DE CAPITALS**

### **II.2.a) Direito à privacidade, direito à proteção de dados e autodeterminação informacional**

Independentemente da discussão acerca da autonomia do direito à proteção de dados<sup>41</sup>, há consenso quanto ao fato de que esse direito vai além da ideia clássica de privacidade como direito de estar só, de se afastar da multidão - baseada numa dicotomia entre o público e o privado<sup>42</sup> -,

---

38 Rogall chama a atenção para essa mesma situação na Alemanha quando proferida a famosa “Decisão do Censo” (1983) pela Corte Constitucional, a qual, segundo ele, nada mais fez que estender ao âmbito das relações informacionais os princípios já reconhecidos no âmbito da proteção de direitos fundamentais frente a intervenções informacionais estatais (Rogall, 1991, p. 930).

39 Mas também no “Caso ABIN”, STF, MC-ADIn 6.529, Tribunal Pleno, Relª Min. Cármen Lúcia, DJe 15.10.2020. Cf. especialmente o voto do Ministro Édson Fachin, p. 57, e do Ministro Gilmar Mendes, p. 77 e ss.

40 Um relato detalhado em Souto; Rosal, 2021.

41 Sobre essa discussão, cf., entre nós, o trabalho pioneiro de Doneda, 2020, *passim*. Silva registra que talvez “não haja outro direito que tenha passado por transformações tão profundas e tão rápidas em seu significado nas últimas décadas como o direito à privacidade” (Silva, 2021, p. 203). Para Bioni, 2020, p. 95, trata-se de um “novo direito da personalidade”. Cf. Para Gleizer, Montenegro e Viana (2021), é uma decorrência dos direitos fundamentais que conformam a garantia ao livre desenvolvimento da personalidade (p. 38-39). A LGPD optou por assentar a proteção de dados pessoais tanto no respeito à privacidade como na autodeterminação informativa e na inviolabilidade da intimidade, da honra e da imagem (art. 2º, I, II e IV, respectivamente).

42 Bioni, 2020, p. 91-94.

para manifestar um direito de controle<sup>43</sup> do titular sobre os próprios dados (“pessoa-informação-circulação-controle” – Bioni, 2020, p. 94). Nesse âmbito, dados compartilhados com o público, que não gerariam por si questões atinentes à privacidade no sentido clássico, podem, “quando agregados a outros fatos (dados), revelar detalhes precisos sobre a personalidade de um indivíduo” (Bioni, 2020, p. 95). Os direitos de acesso e retificação que tem o titular de dados pessoais mesmo quando “transitam na esfera pública” (Bioni, 2020, p. 95) são um exemplo claro de que essa tutela não se confunde com a da privacidade entendida no seu sentido originário de “afastamento da multidão” (Doneda, 2020, p. 181-182)<sup>44</sup>. Passamos, assim, da lógica segundo a qual “dados que não são ‘sigilosos’... não são protegidos” (Abreu, 2021, p. 588), para uma de proteção ampla de dados pessoais contra todas as formas de tratamento. Essas considerações são importantes no âmbito do tratamento de dados para fins de controle e prevenção da lavagem de capitais, especialmente no tratamento dado pelo COAF, objeto da decisão do STF.

### **II.2.b) Dados pessoais, dados pessoais sensíveis e dados pessoais sigilosos**

Os dados pessoais podem ser divididos em categorias segundo certas restrições impostas a seu tratamento.

A LGPD define dado pessoal como a “informação relacionada a pessoa natural identificada ou identificável” (art. 5º, I), e dado pessoal sensível como aquele “sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (art. 5º, II). O tratamento destes últimos está sujeito a uma série de restrições, como, por exemplo, um consentimento qualificado do titular (arts. 11 a 13 da LGPD).

No âmbito das medidas de prevenção à lavagem (adiante, PLD), há tratamento de grande quantidade de dados pessoais e de dados pessoais sensíveis. No cumprimento de suas obrigações de PLD (arts. 10, I, II, 11, I e II, da LLD), as pessoas obrigadas (art. 9º da LLD) devem proceder a várias operações de tratamento de dados pessoais em quantidades nada desprezíveis. Usando a linguagem do art. 5º, X, da LGPD, elas devem, *pelo me-*

43 Mas não de domínio ou propriedade, como sustenta Rogall, 1985, p. 11-12.

44 Também Abreu, 2021, p. 584.

nos, coletar, produzir, recepcionar, classificar, utilizar, acessar, reproduzir, transmitir, distribuir, processar, arquivar, armazenar, avaliar, controlar, modificar, comunicar, transferir e difundir dados pessoais<sup>45</sup>.

Dentre os dados pessoais tratados pelo COAF, haverá também dados *sensíveis* e *sigilosos*.

Dados pessoais *sensíveis* serão objeto de tratamento quando relativos a “presidentes e tesoureiros nacionais, ou equivalentes, de partidos políticos”, pois considerados pessoas politicamente expostas (art. 1º, § 1º, VI, da Resolução COAF nº 29, de 7 de dezembro de 2017) e relativos, portanto, à filiação a organização de caráter político (art. 5º, II, da LGPD). Nesse caso, as pessoas obrigadas devem adotar providências especiais para o acompanhamento de operações ou propostas de operações com pessoas expostas politicamente (art. 1º, *caput*, da Resolução COAF nº 29). Elas devem “dedicar especial atenção às operações ou propostas de operações envolvendo pessoa exposta politicamente, bem como com seus familiares, estreitos colaboradores e/ou pessoas jurídicas de que participem, observando, nos casos de maior risco” (art. 2º, *caput*, da Resolução COAF nº 29).

Além dessas atividades de coleta de dados pessoais feitas no âmbito do *know your customer* (KYC) ou *customer due diligence* (CDD), uma das obrigações mais relevantes para a prevenção e repressão à lavagem é a de *comunicação* de operações em espécie (COE) e de operações suspeitas (COS) ao COAF. Os dados transmitidos (para usar a linguagem da LGPD, art. 5º, X) pelas pessoas obrigadas ao cumprirem seus deveres de comunicação de operações em espécie (art. 11, II, *a*, da LLD) e suspeitas (que possam “constituir-se em sérios indícios dos crimes previstos nesta lei, ou com eles relacionar-se” – art. 11, II, *b*, da LLD), envolverá, por definição, dados pessoais. Isso é assim porque virão, necessariamente, acompanhadas de informações relacionadas às pessoas naturais envolvidas nas transações<sup>46</sup>, pois

---

45 Para que se tenha uma ideia da quantidade e amplitude dos dados tratados, basta consultar a Resolução COAF nº 36, de 10 de março de 2021, que se aplica *apenas* às pessoas obrigadas sujeitas à supervisão do COAF (arts. 7º a 12). Um apanhado geral da regulação no âmbito de competência regulatória do Bacen e da CVM em Oliveira, 2020. A CVM acaba de atualizar sua regulação setorial de PLD, cf. Resolução CVM nº 50, de 31 de agosto de 2021. A amplitude dos dados tratados é objeto de preocupação no ambiente europeu há algum tempo, cf. ilustrativamente, Autoridade Europeia para Proteção de Dados, 2017; Preziosi, 2017; Malish, 2018; Khan, 2016; Peña Zafra, 2016.

46 Cf. Nota Técnica nº 40.241 do COAF referida no voto do Ministro Gilmar Mendes no RE 1.055.941, fl. 3073-3074: “O primeiro tipo de comunicação reporta operações individuais, sem a necessidade de maiores detalhamentos. A COE informa o valor da operação, a identificação do titular da conta, a pessoa que efetuou a operação, o proprietário do dinheiro e dados cadastrais bancários, tais como conta, agência, banco e cidade”; o “segundo tipo de comunicação (COS) assim se define segundo critérios emanados da lei e de

apenas elas<sup>47</sup> estão sujeitas à responsabilidade penal e são, portanto, os alvos finais de toda a legislação de controle, prevenção e repressão à lavagem de capitais e ao financiamento ao terrorismo<sup>48</sup>.

Além de dados pessoais sensíveis, é da essência da atividade do COAF o tratamento de dados sujeitos a *sigilo*: um dever imposto, por lei ou ato privado, ao recipiente do dado ou informação de não revelá-lo a outras pessoas, senão àquelas expressamente autorizadas pelo titular, pelo ato privado ou pela lei<sup>49</sup>. O sigilo, de forma geral, restringe certas formas de tratamento que impliquem *revelação* a terceiros não autorizados do conteúdo da informação sigilosa, ou seja, na linguagem do art. 5º, X, da LGPD, a *transmissão, a distribuição, a comunicação, a transferência, a difusão*.

Há vários sigilos, médico, profissional, comercial, financeiro etc., instituídos sobre diversos fundamentos jurídicos<sup>50</sup>, e sua violação (leia-se: a revelação da informação protegida) é conduta criminalizada, entre nós, de forma geral, pelos arts. 154 e 325 do CP<sup>51</sup>. Especificamente no que diz respeito ao sigilo *financeiro*, segundo opinião majoritária, serve à preservação do direito à privacidade<sup>52</sup>, recebendo tutela penal específica, atualmente, no âmbito da LC 105<sup>53</sup>, que incrimina a “quebra de sigilo, fora das hipóteses

---

regulamentos aplicáveis”. O detalhamento dos dados que devem compor as duas espécies de comunicação é feito por cada regulação setorial. No caso dos bancos, por exemplo, cf. Bacen, Circular nº 3.978, de 23 de janeiro de 2020, arts. 48 a 55.

47 Exceção feita às pessoas jurídicas no âmbito dos crimes ambientais, Lei nº 9.605/1998.

48 Greenleaf; Tyree, 2017, p. 45.

49 A LGPD não define o que sejam dados sigilosos, mas indica as limitações em seu tratamento e as medidas de segurança para evitar revelação que devem ser aplicadas, cf. arts. 46 a 49.

50 Sobre os diversos fundamentos do sigilo no âmbito do § 53 do StPO (Código de Processo Penal alemão), cf. Rogall, 2018, especialmente números marginais 10 e seguintes. Sobre o sigilo médico e sua orientação à proteção de interesse individual do paciente, cf., Soares, 2020.

51 Os dois tipos penais indicam como conduta incriminada a de *revelar* segredo ou fato que deva permanecer em segredo.

52 Cf. Baltazar Júnior, 2005, p. 60; Salomão Neto, 2020, p. 678; Belloque, 2003, p. 73; Abreu, 2021, p. 584-585. Ferraz Júnior, por sua vez, parece assentar o sigilo bancário no disposto no art. 5º, XII, da CF (2020, p. 170, nota 6). No próprio RE 1.055.941, o Ministro Gilmar Mendes, por exemplo, assenta-o no art. 5º, X, da CF (fl. 3043). Como a LC 105 institui o sigilo em função das operações e dos detentores dos dados (instituições financeiras), ela não o limita às pessoas naturais, mas alcança também pessoas jurídicas. Isto poderia colocar em xeque o entendimento segundo o qual o fundamento desse sigilo é a privacidade caso se reconheça que as pessoas jurídicas não têm um direito fundamental à privacidade. Isso indicaria a correção do entendimento que vê neste sigilo uma espécie de sigilo *profissional* fundado na liberdade geral de ação, como se faz na Alemanha (Kalkbrenner; Koch, 2019, número marginal 3; que alertam para o fato de que a proteção do sigilo bancário é mais ampla quanto aos sujeitos protegidos do que a da proteção de dados pessoais, nm. 7).

53 Quanto à relação entre o art. 10 da LC 105/2001 e o art. 18 da Lei nº 7.492/1986, entende-se que os dois estão em vigor e têm abrangência distinta em função do âmbito de sujeitos abrangidos pela LC 105 e pela Lei nº 7.492/1986, cf. Baltazar, 2005, p. 172-173.

autorizadas” na lei, punindo-a com pena de reclusão, de um a quatro anos, e multa (art. 10)<sup>54</sup>.

### II.3 O tratamento de dados pessoais pelo COAF

É tempo de examinar as possíveis consequências das ideias até aqui apresentadas para o tratamento de dados pessoais pelo COAF, exame que deve ser feito em conformidade com as premissas até aqui estabelecidas e que recapitulo brevemente: (a) as competências e tarefas atribuídas ao COAF não são autorizações para intervenção em direitos fundamentais, do que decorre (b) a necessidade de que todo tratamento de dados realizado por esse órgão tenha de estar previamente autorizado por lei proporcional<sup>55</sup>, que é aquela (c) que estabelece, de forma clara, tanto a modalidade de tratamento autorizada como a finalidade da intervenção (sendo cada nova forma de tratamento uma intervenção autônoma), e que, (d) no caso de dados pessoais protegidos por sigilo financeiro, ademais, formas de tratamento que impliquem revelação<sup>56</sup> (*transmissão, distribuição, comunicação, transferência, difusão*) devem cumprir rigorosamente o que dispõe a LC 105.

#### II.3.a) Competências e tarefas atribuídas ao COAF

A LLD criou, em 1998, o COAF com “a finalidade de disciplinar, aplicar penas administrativas, receber, examinar e identificar as ocorrências suspeitas de atividades ilícitas previstas nesta lei, sem prejuízo das competências de outros órgãos e entidades” (art. 14, *caput*)<sup>57</sup>. O órgão tem como atribuições, ainda, “coordenar e propor mecanismos de cooperação e de troca de informações que viabilizem ações rápidas e eficientes no combate à ocultação ou dissimulação de bens, direitos e valores” (art. 14, § 2º). Para isso, tem autorização (“poderá”) para “requerer aos órgãos da Administração Pública as informações cadastrais bancárias e financeiras de pessoas

---

54 Outras violações graves ao regime de proteção de dados pessoais ainda carecem de tutela penal entre nós, mas já foram contempladas, por exemplo, em Portugal, na Lei nº 59/2019, arts. 53 a 60; na Itália, no Decreto Legislativo nº 51, de 18 de maio de 2018, arts. 43 a 45; na Alemanha, na *Bundesdatenschutzgesetz* – BDSG (Lei Federal de Proteção de Dados), par. 42; na Suíça, no StGB (Código Penal), arts. 143, 143-bis, 179-novies; e na Espanha, nos arts. 197 e 198 do Código Penal.

55 Em virtude dessa exigência é que o Decreto nº 9.663, de 1º de janeiro de 2019, que aprova o Estatuto do COAF, não oferece fundamento legal para tratamento de dados, razão pela qual não será objeto de exame nesta oportunidade.

56 A LC 105 fala em “conservar sigilo” (art. 1º), “violação de sigilo” (art. 1º, § 3º), “revelação de informações sigilosas” (art. 1º, § 3º, V), “quebra de sigilo” (art. 1º, § 4º), “dever de sigilo extensivo” (art. 2º), “preservação do sigilo mediante acesso restrito às partes” (art. 3º), “levantamento do sigilo” (art. 7º), “quebra de sigilo” (art. 10, que define a conduta a partir de uma metáfora).

57 Uso a redação em vigor em 20.09.2021.

envolvidas em atividades suspeitas” (§ 3º). Por fim, o órgão “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” (art. 15).

A par dessas normas, em 7 de janeiro de 2020, foi promulgada a Lei nº 13.974, que, além de vincular o órgão ao Banco Central do Brasil (art. 2º), estabelece sua estrutura organizacional e atribuições, dentre elas as de “produzir e gerir informações de inteligência financeira para a prevenção e o combate à lavagem de dinheiro” e a de “promover a interlocução institucional com órgãos e entidades nacionais, estrangeiros e internacionais que tenham conexão com suas atividades” (art. 3º, I e II). Esse diploma legal, porém, não veicula autorizações legais para a intervenção em direitos fundamentais, mas trata da estrutura interna e funcionamento do órgão (norma de *competência*, portanto, no sentido acima empregado III, 1, *b*). Sob esse ponto de vista, por exemplo, a “produção e gestão de informações de inteligência financeira” que envolvam dados pessoais (art. 3º, I, acima) poderá ser feita desde que haja uma autorização legal, seja na LLD, seja em outra lei federal. Inexistindo autorização, a produção e a gestão não poderão envolver dados pessoais, mas, sim, por exemplo, dados anonimizados para fins estatísticos, de construção de tipologias etc. Isso vale também para a interlocução institucional com órgãos nacionais e estrangeiros (cf. *infra* IV, 3).

As tarefas atribuídas ao COAF parecem misturar elementos de *inteligência*, de *segurança pública* e de *persecução penal*. O órgão coleta e analisa informações necessárias para formular políticas de prevenção de lavagem (*inteligência*), fiscaliza o cumprimento das medidas de controle e prevenção da lavagem pelas pessoas obrigadas para, assim, prevenir perigos contra bens jurídicos (*segurança pública*) e, finalmente, se volta para o passado, ao apurar operações suspeitas de lavagem e as comunicar aos órgãos de persecução penal (*persecução penal*). Esta última faceta poderá ser ainda mais acentuada se se admitir a elaboração de RIFs a pedido (cf. *infra* IV, 2). Esse acúmulo de atribuições com finalidades diversas, que veicula uma coleta de dados de amplitude singular em nosso sistema jurídico, torna difícil alocar o órgão sob este ou aquele pilar e, conseqüentemente, pode gerar riscos para a proteção de dados pessoais, especialmente sob o ponto de vista da separação informacional<sup>58</sup>.

---

58 O supervisor de proteção de dados europeu vem alertando para os perigos dessa falta de clareza e determinação quanto à natureza das funções das unidades de inteligência financeira desde, pelo menos, 2017: cf. European



### II.3.b) Dados pessoais

Sob o ponto de vista do tratamento de dados pessoais, os arts. 11, 14 e 15 da LLD sugerem o seguinte regime: a) o art. 11 veicula a norma autorizativa que autoriza as pessoas obrigadas (do art. 9º) a transmitirem ao COAF dados pessoais não sujeitos a sigilo financeiro;<sup>59</sup> b) o art. 14, *caput*, lido com benevolência (já que a linguagem se aproxima mais da de uma norma de competência do que de uma norma de autorização<sup>60</sup>), autoriza o COAF ao tratamento (“receber, examinar e identificar”) interno de dados pessoais recebidos das pessoas obrigadas exclusivamente para a finalidade de apuração da ocorrência de suspeita de prática de lavagem de dinheiro e financiamento ao terrorismo (“as ocorrências suspeitas de atividades ilícitas previstas nesta lei”), vedado o tratamento para qualquer outra finalidade;<sup>61</sup> c) uma especial forma de tratamento, a comunicação (também chamada de “disseminação”), só pode ser realizada *pele* COAF *para* as “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” (art. 15); d) o dever imposto ao órgão de “coordenar e propor mecanismos de cooperação e de troca de informações que viabilizem ações rápidas e eficientes no combate à ocultação ou dissimulação de bens, direitos e valores” (art. 14, § 2º)<sup>62</sup>, não parece veicular norma autorizativa para compartilhamento de dados pessoais (sigilosos ou não) com pessoas que não as indicadas no art. 15, pois o que a lei autoriza é que o órgão *coordene e proponha*, mas não que *troque* informações, ou seja, que as transmita, distribua, comunique, transfira, difunda ou dissemine.

---

Data Protection Supervisor, 2017, parágrafo 52; e, mais recentemente, European Data Protection Supervisor, 2020, parágrafos 35 e 36.

- 59 “Art. 11. As pessoas referidas no art. 9º: [...] II – deverão comunicar ao COAF, abstenendo-se de dar ciência de tal ato a qualquer pessoa, inclusive àquela à qual se refira a informação, no prazo de 24 (vinte e quatro) horas, a proposta ou realização: a) de todas as transações referidas no inciso II do art. 10, acompanhadas da identificação de que trata o inciso I do mencionado artigo; e b) das operações referidas no inciso I.”
- 60 Neste sentido, cf. o § 28 da *Geldwäschegesetz* (adiante, GwG), que detalha, em 13 incisos, todas as atividades da UIF alemã, seguido do § 29, que disciplina o tratamento de dados pessoais pela UIF.
- 61 “Art. 14. Fica criado, no âmbito do Ministério da Economia, o Conselho de Controle de Atividades Financeiras – COAF, com a finalidade de disciplinar, aplicar penas administrativas, receber, examinar e identificar as ocorrências suspeitas de atividades ilícitas previstas nesta Lei, sem prejuízo das competências de outros órgãos e entidades.” (Redação dada pela Medida Provisória nº 886, de 2019)
- 62 Art. 15: “§ 2º O COAF deverá, ainda, coordenar e propor mecanismos de cooperação e de troca de informações que viabilizem ações rápidas e eficientes no combate à ocultação ou dissimulação de bens, direitos e valores”.

### II.3.c) Dados pessoais financeiros sigilosos

Além de dados pessoais comuns e sensíveis, o COAF recebe e trata também dados pessoais financeiros *sigilosos*, submetidos, até 2001, ao regime do art. 38 da Lei nº 4.595/1964, e, a partir de 2001, ao regime da LC 105. A regra é que as operações ativas e passivas e os serviços prestados pelas instituições financeiras indicadas no art. 1º, § 1º, da LC 105 sejam sigilosos, no sentido de que as informações a elas relativas *não possam ser reveladas* (transmitidas, distribuídas, comunicadas, transferidas, difundidas ou disseminadas) a terceiros.

A relação entre a LLD (e suas alterações) e a LC 105 habita o problemático ambiente das relações entre leis ordinárias e leis complementares. A partir de 1988, o art. 192, *caput*, da CF passou a determinar que o sistema financeiro nacional fosse regulado por lei complementar. Por essa razão, a Lei nº 4.595, de 31 de dezembro de 1964, que tratava da matéria, foi recepcionada pela nova ordem constitucional como lei complementar<sup>63</sup>. E era seu art. 38 que, até 2001, instituía o sigilo financeiro. Em 2001, como dito, sobreveio nova lei complementar disciplinando, de forma mais detalhada, o sigilo financeiro, a LC 105.

Muito embora o STF tenha reconhecido, por maioria, que não existe, em regra, hierarquia entre uma lei ordinária e uma lei complementar, há certa distribuição constitucional material (*ratione materiae*) entre as espécies legislativas<sup>64</sup>: uma reserva constitucional de lei complementar limitada a certas matérias. Assim, uma lei ordinária poderia dispor em sentido contrário do disposto em uma lei complementar e, assim, revogar seus dispositivos, *desde que* não trate de matéria privativa desta<sup>65</sup>. *A contrario sensu*, uma lei complementar que trate de matéria a ela não reservada pela CF vale como lei ordinária<sup>66</sup>.

E por que isso importa?

Porque, tendo sido o sigilo financeiro estabelecido em lei complementar, se houver, para essa matéria, reserva constitucional de lei comple-

---

63 Baltazar, 2005, p. 73.

64 STF, RE 377.457, Tribunal Pleno, Rel. Min. Gilmar Mendes, DJe 18.11.2008.

65 STF, RE 377.457, Tribunal Pleno, Rel. Min. Gilmar Mendes, DJe 18.11.2008, fl. 1819.

66 STF, RE 377.457, Tribunal Pleno, Rel. Min. Gilmar Mendes, DJe 18.11.2008, fl. 1834. A complexidade dessa discussão se mostra com toda sua força na discussão travada no plenário por ocasião deste julgamento e que não pode ser captada nesta oportunidade.

mentar<sup>67</sup>, as normas da LLD não revogariam nem as da Lei nº 4.595/1964 (até 2001), nem as da LC 105 (após 2001), que regeriam, soberanas, as autorizações para a revelação de dados financeiros sigilosos. Em outras palavras: a revelação de dados financeiros sigilosos *para* o COAF e *pelo* COAF dependeriam das autorizações expressas da LC 105. Nesse caso, tanto as comunicações de operações (em espécie e suspeitas) feitas pelas pessoas obrigadas *para* o COAF contendo dados financeiros sigilosos como *do* COAF para as autoridades competentes para a persecução penal (por meio de RIFs no sentido do art. 15 da LLD) dependeriam de norma autorizativa na LC 105.

Sob esse entendimento, teríamos o seguinte quadro à luz da LC 105:

a) haveria uma autorização para “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” (art. 1º, § 3º, IV, da LC 105), aplicável a quaisquer pessoas submetidas à LC 105, dentre elas parte das pessoas obrigadas do art. 9º da LLD. Essa seria a norma que veicularia autorização legal para a comunicação de operações suspeitas (COS) pelas pessoas obrigadas sujeitas à LC 105 ao COAF; b) haveria autorização para que o Bacen e a CVM, no exercício de suas atribuições e quando verificassem “a ocorrência de crime definido em lei como de ação pública, ou indícios da prática de tais crimes”, informassem o Ministério Público sobre tais fatos juntando à comunicação os documentos necessários à apuração ou comprovação dos fatos (art. 9º, *caput*, da LC 105); ou seja, haveria uma autorização para comunicação não ao COAF, mas ao MP, sobre eventual suspeita de prática de crime; c) haveria autorização para que o Bacen e a CVM e demais órgãos de fiscalização (mas não as instituições financeiras), nas áreas de suas atribuições, fornecessem ao COAF “as informações cadastrais e de movimento de valores relativos às operações previstas no inciso I do art. 11 da referida lei”, que são as que “possam constituir-se em sérios indícios dos crimes previstos nesta lei, com eles relacionar-se” (art. 11, I, da LLD). O dispositivo, portanto, só alcança operações suspeitas (art. 2º, § 6º, da LC 105); d) quanto às comunicações de operações em espécie, disciplinadas em dois dispositivos da LLD<sup>68</sup>, a LC 105 não teria veiculado autorização para que as pes-

67 Um tema que merece estudo mais aprofundado, inviável aqui.

68 O art. 10, II, e o art. 11, II, que distingue, em suas alíneas *a* e *b*, entre operações em espécie (que geram as comunicações denominadas COE) e as suspeitas (que geram comunicações denominadas COS).

soas obrigadas pela LLD, mas submetidas ao sigilo financeiro, fizessem tais comunicações, a não ser que se entenda que toda operação em espécie é suspeita, em um sentido mais amplo deste termo, diverso do sentido que lhe é dado pela LLD; e) por fim, a LC 105 instituiu o sigilo de dados financeiros, mas não tratou da comunicação do COAF *para* as “autoridades competentes” (art. 15 da LLD) que contenham dados protegidos por sigilo financeiro, como fez, expressamente, quanto ao Bacen, à CVM e à Receita Federal<sup>69</sup>. Esse pernicioso silêncio pode dar azo a disputas quanto à possibilidade de o COAF incluir dados cobertos por sigilo financeiro em seus relatórios para autoridades de persecução penal.<sup>70</sup>

A questão ficou ainda mais complexa com o advento da mudança do COAF para âmbito do Bacen por força da Lei nº 13.974, de 7 de janeiro de 2020. Se se entender que, a partir de então, o órgão e seus agentes fazem parte do Bacen, a eles se estende o dever de sigilo (art. 2º, § 5º, da LC 105) e também a autorização para a comunicação prevista no art. 9º, o que tornaria inquestionável a possibilidade de que os RIFs contivessem dados protegidos por sigilo financeiro. A complexidade criada pelo art. 2º da Lei nº 13.974, que “vinculou administrativamente” o COAF ao Bacen, mas manteve sua “autonomia técnica e operacional”, está a merecer melhor exame, especialmente sob o viés da separação informacional.

Se, porém, se entender que a matéria do sigilo financeiro, apesar de veiculada em lei complementar, não está a ela reservada, então tanto as normas da Lei nº 4.595/1964 como as da sua sucessora, a LC 105, valeriam como lei ordinária, e as normas da LLD teriam o condão de regular a matéria, criando permissões de revelação desses dados não contempladas na LC 105. Neste caso, o art. 11 da LLD, na redação recebida por força da Lei nº 12.683/2012, seria a base legal que autorizaria todas as pessoas obrigadas – dentre elas também aquelas sujeitas à LC 105, que é anterior à Lei nº 12.683/2012 – a comunicar dados pessoais financeiros sigilosos ao COAF; e o art. 15 da LLD autorizaria este órgão a comunicá-los, nos RIFs, às autoridades competentes.

Até aqui, a bem ver, tratamos de revelação de dados pessoais *financeiros sigilosos* limitados a certas operações (suspeitas, em espécie, indica-

---

69 Cf. LC 105/2001, art. 1º, § 3º, VI, c/c, especialmente, com o art. 9º.

70 Essa incerteza não é um privilégio do Brasil, como registra Maillart em tom crítico, quanto aos cinco países analisados em abrangente estudo comparativo sobre a regulação da lavagem de capitais concluído em 2020 (Vogel; Maillart, 2020, p. 848).

tivas da prática de crime), do que decorre uma delimitação clara dos dados que podem ser revelados em termos de tempo, espaço, pessoas envolvidas, montantes, espécie de operação ou serviços, pois a *finalidade* é clara. Embora, como dito, configurem intervenções no direito à proteção de dados pessoais e na privacidade, a severidade dessas intervenções, em si mesmas, é mais limitada do que a revelação de dados financeiros não conectados a certas operações, mas, sim, a lapsos temporais. Neste último caso, trata-se de revelar aspectos amplos não só da privacidade da pessoa afetada, mas de sua intimidade, além de dados de terceiros insuspeitos<sup>71</sup>. Enquanto a comunicação de uma prática criminosa está limitada (finalidade) apenas às informações necessárias para a comprovação da suspeita, por exemplo, o recebimento de certa quantia, em certa data, envolvendo certas pessoas etc.; o que conhecemos por “quebra” do sigilo bancário por ordem judicial ou de comissões parlamentares de inquérito implica revelação indiscriminada da privacidade e da intimidade tanto da pessoa que é alvo da “quebra” como de terceiros insuspeitos dentro do espectro temporal coberto pela determinação. Trata-se, assim, de uma intervenção muito mais severa no âmbito do direito fundamental à privacidade e é por essa razão que, nestes casos, a LC 105 não veicula uma autorização direta para que agentes públicos os acessem, mas exige uma autorização judicial individualizada (*reserva de jurisdição* – art. 1º, § 4º) ou a aprovação por órgão colegiado no âmbito das comissões parlamentares de inquérito (art. 4º, § 2º), e, ademais, determina que o caráter sigiloso seja mantido mediante “acesso restrito às partes, que delas não poderão servir-se para fins estranhos à lide” (art. 3º, *caput*, da LC 105)<sup>72</sup>.

### III – CONSEQUÊNCIAS

Estabelecidas todas essas premissas, cumpre delas extrair as consequências para aquela que é a questão central examinada neste texto: os limites

---

71 Cf. Estellita; Gleizer, 2020.

72 Este é só um dentre os inumeráveis fundamentos que evidenciam a ilegalidade da determinação feita pela PGR, em meados de 2020, às Forças-Tarefa da Operação Lava-Jato no Rio de Janeiro, São Paulo e Curitiba para que lhe entregassem “todas as bases de dados estruturados e não estruturados utilizadas e obtidas em suas investigações, por meio de sua remessa atual, e para dados pretéritos e futuros, à Secretaria de Perícia, Pesquisa e Análise do gabinete do procurador-geral da República” (Disponível em: <https://g1.globo.com/politica/noticia/2020/08/03/fachin-revoga-decisao-de-toffoli-que-permitia-compartilhamento-de-dados-entre-pgr-e-forcas-tarefa-lava-jato.ghtml>. Acesso em: 11 set. 2021), seguida da Portaria Conjunta PGR/MPF – CMPF nº 1, de 7 de janeiro de 2021. Outras considerações em Luz, 2021. A determinação é objeto de disputa no STF, na RCL 42.050, que tramita sob sigilo.

da transmissão, distribuição, comunicação, transferência e difusão (ou disseminação, no jargão do COAF) de dados pessoais *pelo* COAF.

### III.1 RIFs DE OFÍCIO (“DISSEMINAÇÃO ESPONTÂNEA”)

Como visto, tanto a LLD como a LC 105 contêm autorizações<sup>73</sup> para que o COAF receba, classifique, utilize, processe, archive, armazene, avalie e controle dados pessoais, sigilosos ou não. Quanto às operações de transmissão, distribuição, comunicação, transferência e difusão (que evidentemente incluem a “disseminação”), norma autorizativa para essas formas de tratamento é o art. 15 da LLD, que as limita à comunicação às autoridades competentes, quando o próprio órgão concluir pela existência ou fundados indícios da prática de crimes previstos na LLD, ou qualquer outro ilícito<sup>74</sup>. Nada mais é dito sobre a forma e o conteúdo dessas comunicações<sup>75</sup>.

### III.2 RIFs A PEDIDO (“DISSEMINAÇÃO A PEDIDO”)

Os dois diplomas legais que regulam a atividade do COAF não parecem lhe impor um dever de compartilhar dados pessoais *a pedido de autoridades públicas*<sup>76</sup>.

Com relação a eventuais pedidos de representantes do Ministério Público, muito embora seja sua “função institucional” “promover, privativamente, a ação penal pública, na forma da lei” e “requisitar diligências investigatórias e a instauração de inquérito policial, indicados os fundamentos jurídicos de suas manifestações processuais” (art. 129, I e VIII, da CF)<sup>77</sup>, dessas atribuições não derivam autorizações para intervenção em direitos

---

73 Muito embora com linguagem fraca em termos da clareza e da determinação que se deve exigir das normas autorizativas de intervenções em direitos fundamentais (cf. acima II, 1, a e b).

74 A referência a “qualquer outro ilícito”, prevista no final do art. 15, *caput*, da LLD, merece reparo, pois poderia levar a transformar o órgão de combate e prevenção à lavagem de dinheiro e ao financiamento do terrorismo em agência de inteligência de quaisquer ilícitos, penais ou administrativos, praticados no País. Sobre a importância de rigorosa observância da finalidade do tratamento de dados pelas unidades de inteligência financeira, cf. European Data Protection Supervisor, 2020, parágrafos 8 a 10.

75 O dispositivo é lacônico, beirando o descumprimento do princípio da clareza e determinação e merece atenção do legislador. Nesse sentido, vale conferir o detalhado § 32, 5, GwG.

76 Em sentido similar, Bottini, 2021. Sobre a situação nos cinco países objeto da pesquisa coordenada por Vogel e Maillart, cf. Vogel; Maillart, 2020, p. 848-849.

77 A Lei Complementar nº 75/1993 repete essa regra de competência (art. 6º, V) e contém outra regra de competência no art. 7º. A Lei Orgânica Nacional nº 8.625/1993 reproduz essa linguagem no art. 26, II e IV.

fundamentais, as quais, como dito e repetido, têm de ser autorizadas por lei (art. 5º, II, da CF)<sup>78</sup>.

O Ministério Público tem, assim, competência para fazer essas requisições, mas o atendimento que implique tratamento de dados pessoais só pode ser efetuado se houver autorização legal proporcional. Um entendimento que autorizasse aos membros do MP a obtenção direta, junto às instituições financeiras ou ao COAF, de informações cobertas por sigilo financeiro permitiria que, como dito, pela porta dos fundos (*back door*), fosse corroído o regime constitucional (e infraconstitucional) de proteção de direitos fundamentais. Isso implicaria, ademais, verdadeira  *fusão informacional* entre os dois órgãos<sup>79</sup>, pois, por essa via, o Ministério Público obteria acesso a um imenso conjunto de dados que o legislador outorgou  *apenas* ao COAF<sup>80</sup>. Esses mesmos limites valem, logicamente, para as autoridades policiais.

Conforme explicações fornecidas pelo COAF ao STF no RE aqui analisado, o Sistema SEI-C, além de ser utilizado para as comunicações do COAF para as autoridades competentes, também é utilizado como um canal de comunicação na via oposta: das autoridades competentes para o COAF. Nele, essas autoridades registram dados sobre pessoas investigadas, os crimes dos quais são suspeitas e a descrição do modo como os teriam praticado. Essas novas informações, incorporadas ao acervo informacional que o COAF já tem<sup>81</sup>, podem ser objeto de análise, com a conclusão da existência de operações suspeitas de lavagem. Neste caso, o COAF pode, naturalmente, gerar um RIF e comunicar as operações suspeitas individualizadas às autoridades competentes, nos exatos termos da autorização que lhe é dada pelo art. 15 da LLD. Esta foi, inclusive, a posição do relator do RE 1.055.941 (cf. fl. 2738 do acórdão) no STF e que parece acertada, pois aqui, na verdade, não se

---

78 A teoria dos poderes implícitos discutida no STF quando chamado a decidir se membros do Ministério Público poderiam investigar não é incompatível com o que aqui se afirma, pois seus poderes de investigar só podem ser exercidos desde que respeitados os direitos e garantias fundamentais (cf. STF, RE 593.727, Tribunal Pleno, Rel. Min. Cezar Peluso, DJ 08.09.2015).

79 Em sentido similar, Greco; Leite, 2019.

80 Badaró chama a atenção para esse ponto considerando equivocada a decisão do STF no RE por não separar adequadamente “quem detém a informação” de “quem detém o poder de persecução penal” (Badaró, 2021). Em sentido diverso, aparentemente, Bottini, 2021.

81 Questão que está a merecer atenção diz respeito à necessidade de maior transparência quanto às fontes de dados. Sobre isso, cf. Bialski; Vento; Messina; Wiegierinck, 2021.

trata de um RIF ou “disseminação” “a pedido”, mas de RIF de ofício (“disseminação espontânea”)<sup>82</sup>.

### III.3 INTERCÂMBIO INTERNACIONAL ENTRE UIFs

A questão é bem mais delicada quando se trata do intercâmbio de dados pessoais (dentre eles, também financeiros sigilosos) com unidades de inteligência financeira de outros países, como no âmbito do chamado Grupo Egmont. Segundo informações públicas do próprio COAF<sup>83</sup>, a cooperação com as UIFs estrangeiras dá-se no âmbito do próprio SEI-C, onde podem ser transmitidos e transferidos (e também obtidos) dados como comunicações de operações suspeitas, comunicações de operações em espécie, identificação de pessoas naturais e jurídicas (suspeitas e relacionadas a suspeitas), identificação de beneficiários finais, de sócios e representantes de empresas, participações societárias, lista de bens móveis e imóveis, histórico criminal etc.

Como dito, nem o dever imposto ao órgão de “coordenar e propor mecanismos de cooperação e de troca de informações” (art. 14, § 2º), nem mesmo sua competência para, “em todo o território nacional”, “promover a interlocução institucional com órgãos e entidades nacionais, estrangeiros e internacionais que tenham conexão com suas atividades” (art. 3º, II, da Lei nº 13.974/2020) lhe franqueiam autorização legal para compartilhar dados pessoais (sigilosos ou não) com pessoas que não as do art. 15 da LLD. A cooperação e a troca de informações, assim, não poderia envolver dados pessoais (sigilosos ou não), a não ser que houvesse diploma legal (reserva de lei) autorizando o órgão a fazê-lo<sup>84</sup>, como poderia ser, por exemplo, um

---

82 Razão pela qual seria recomendável não o denominar de “RIF decorrente de intercâmbio”, expressão que sugere um RIF produzido por provocação de autoridades públicas, tratamento de dados que, como visto, não está autorizada pela LLD.

83 COAF – CONSELHO CONTROLE DE ATIVIDADES FINANCEIRAS. Inteligência Financeira: Aspectos práticos do intercâmbio internacional via Rede Egmont. [s.l.: s.n., s.d.]. Disponível em: [https://www.youtube.com/watch?v=i5N\\_LqLmewl](https://www.youtube.com/watch?v=i5N_LqLmewl). Acesso em: 8 ago. 2021.

84 Segundo Teixeira, Wehrs e Madruga, a troca de dados entre unidades de inteligência financeira integrantes do Grupo Egmont não é regulada por convenção ou tratado internacional, mas apenas pelas normas e princípios do próprio Grupo (Teixeira; Wehrs; Madruga, 2019, p. 22). O site do órgão igualmente não indica uma base legal para a cooperação, cf. <https://www.gov.br/coaf/pt-br/aceso-a-informacao/Institucional/articulacao-institucional/articulacao-internacional-em-pld-ft>. Acesso em: 11 set. 2021. As Convenções de Mérida e de Palermo incentivam a cooperação, mas sempre observada a legislação interna (Convenção de Mérida, art. 14, 1, b; Convenção de Palermo, art. 7, 1, b).



tratado internacional incorporado ao nosso direito positivo com hierarquia de lei federal<sup>85</sup>.

Poder-se-ia, talvez, deduzir essa permissão do próprio art. 15, que não teria limitado o rol de autoridades competentes às domésticas, a par de estar em conformidade com as recomendações do GAFI. Esse entendimento, porém, é questionável por algumas razões.

De um lado, o GAFI é um órgão intergovernamental, um fórum, que emite orientações e diretrizes para o combate à lavagem de capitais e financiamento do terrorismo. Suas recomendações não têm impacto vinculante em nosso direito positivo (“*soft law*”). De outro, dentro do regime de proteção de direitos, também as transferências internacionais devem ser veiculadas por norma legal proporcional, pois se trata de intervenção especialmente severa envolvendo alvos que estarão privados da tutela jurisdicional prestada pelo Poder Judiciário brasileiro<sup>86</sup>, feita sem exigência de que o receptor tenha um nível adequado de proteção de dados pessoais<sup>87</sup>. Além disso, “autoridades competentes para a instauração dos procedimentos cabíveis” têm sido compreendidas como autoridades competentes para a investigação e persecução penal de infrações penais<sup>88</sup>, algo que nem todas UIFs são, como serve de exemplo o próprio COAF. Quanto aos dados pessoais financeiros sigilosos, a LC 105, além de dever ser interpretada de forma restritiva<sup>89</sup>, não autorizou o COAF a transmitir esses dados para autoridades estrangeiras. Por fim, uma eventual invocação de atos normativos inferiores à lei (decretos, convênios, acordos de cooperação etc.) não supriria o que determina o art. 5º, II, da CF, pois “não há autorização constitucional a agentes não

---

85 Pressuposto ligado à validade da cooperação ativa, mas que não necessariamente habilitaria o Brasil a receber dados de Estados estrangeiros, dada a inexistência de infraestrutura legal de proteção de dados pessoais nesse âmbito. Nesse sentido, cf. Aras, 2020, p. 14-31, p. 26 e ss. Um panorama do direito positivo brasileiro, do ambiente legal da União Europeia e da Convenção de Budapeste em Domingos, Abreu e Silva; Oliveira, 2020, p. 140-162. Sobre as exigências de adequação ao *standard* de proteção europeu, cf. Morán Martínez, 2020, p. 163-196 e European Data Protection Board, 2021.

86 No mesmo sentido, Teixeira; Wehrs; Madruga, 2019, p. 24. Os autores lembram, ilustrativamente, as autorizações expressas e detalhadas dadas pela lei alemã de lavagem de dinheiro, bem como pela portuguesa.

87 Como é feito, por exemplo, no âmbito da União Europeia, onde se exige uma decisão de adequação prévia da Comissão Europeia (art. 36 da Diretiva UE nº 680/2018). Cf. European Data Protection Board, 2021. Ainda que se leve em conta o disposto no art. 33 da LGPD, o inciso VII, que poderia amparar a transferência, não faz tal exigência ao destinatário dos dados. De outro lado, o inciso III não se aplica à hipótese ora analisada, pois o Grupo Egmont não é um órgão público e nem sequer há um acordo de cooperação internacional que permita a invocação do inciso VI.

88 Cf. RE 1.055.941, voto do Ministro Gilmar Mendes, fl. 3073, 3075.

89 Cf. STF, RE 1.055.941, voto do Ministro Gilmar Mendes, fl. 3049, 3072.

parlamentares para que decidam, à margem do processo democrático, impor restrições a direitos de defesa que valem, principalmente, contra eles”<sup>90</sup>.

Em um mundo no qual já se reconhece que não há dados irrelevantes, no qual a proteção de dados pessoais é um direito fundamental, no qual os diplomas legais nacionais e regionais que regulam a proteção de dados impõem uma série de requisitos para o intercâmbio internacional de dados e criam diversos mecanismos de proteção dos titulares afetados<sup>91</sup>, uma tal interpretação do art. 15 merece ser revista, por obsoleta e incompatível com essa nova realidade<sup>92</sup>.

Essas objeções não impedem, evidentemente, que uma autorização legal expressa e proporcional venha a ser veiculada pelo Poder Legislativo. Até lá, porém, a prática, nos limites das parcas informações acessíveis publicamente, não parece ser admissível.

#### IV – À GUIA DE CONCLUSÃO

Ao fim deste exercício, fica patente que há muito a fazer em termos de observância do princípio da legalidade e do respeito à proteção de dados pessoais num ambiente cujo tratamento de dados é tão amplo e intenso como o do COAF e feito para fins que podem conduzir à privação da liberdade de seus alvos.

Para que esse labor possa ser feito sem causar prejuízos irreparáveis às atividades de inteligência, de segurança pública e de persecução penal, poderíamos muito bem nos aproveitar daquilo que os alemães chamam de *bônus de transição*<sup>93</sup>, e que nós chamamos de modulação de efeitos<sup>94</sup>, con-

---

90 Gleizer; Montenegro; Viana, 2021, p. 44. Como dito, o Decreto nº 9.663, de 1º de janeiro de 2019, que aprova o Estatuto do COAF, não oferece fundamento legal para a transmissão, a distribuição, a comunicação, a transferência, a difusão ou a disseminação de dados pessoais, sigilosos ou não, devendo a troca limitar-se a tipologias, dados estatísticos anonimizados etc. (cf. art. 16).

91 Apenas ilustrativamente, cf. LGPD, arts. 33 a 36; Regulamento (UE) nº 2.016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados), arts. 41 a 45; Diretiva (UE) nº 2.016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016, arts. 35 a 40. O já mencionado Anteprojeto também sugeriu disciplina para a matéria em seus arts. 53 a 58.

92 Incompatibilidade que, a rigor, afeta, como um todo, o ambiente brasileiro relativo à prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais. O Brasil, neste momento, não reúne condições mínimas para conseguir uma decisão de adequação para ser recipiente de dados oriundos do ambiente europeu (cf. o guia para adequação preparado pela autoridade europeia de proteção de dados, European Data Protection Board, 2021).

93 Trata-se da concessão de um prazo ao legislador para que implemente as exigências relativas à proteção de dados. Cf. Greco; Leite, 2019; Greco, 2019, p. 47; Wolter, 2019, p. 167.

94 O Anteprojeto contém uma cláusula temporal de adequação no prazo da *vacatio* ali sugerida, que é de 365 dias (arts. 67 e 68). Talvez esse prazo deva ser ampliado dado o trabalho que deverá ser feito por juristas e parlamentares para adequar a legislação às exigências constitucionais no trato com dados pessoais.

cedendo um prazo razoável para a adaptação da legislação às exigências da proteção de dados pessoais.

Enquanto essa legislação não vem e no atual ambiente, no qual apenas se aguarda a promulgação da PEC 17/2019, no qual a LGPD já está em vigor e, por fim, no qual o STF já tomou importantes decisões em prol da proteção de dados pessoais, é de se esperar que a Corte adote uma abordagem mais rigorosa tanto no que diz respeito à exigência de autorização legal como no que tange à estrita observância dos limites legais para o tratamento de dados pessoais nos âmbitos da inteligência, da segurança pública e da persecução penal. No que interessa a este artigo, isso poderá ter impactos na questão da admissibilidade dos RIFs a pedido e na do intercâmbio internacional entre UIFs, podendo também conduzir a um reexame dos limites do compartilhamento de dados financeiros sigilosos.

## REFERÊNCIAS

ABREU, Jacqueline de Souza. Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-LGPD. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang *et al.* (Org.). *Tratado de proteção de dados pessoais*. São Paulo: Forense, p. 583-603, 2021.

ARAS, Vladimir Barros. A título de introdução: segurança pública e investigações criminais na era da proteção de dados. In: DE MENDONÇA, Andrey Borges; CAPANEMA, Walter Aranha; ARAS, VLADIMIR BARROS, Augusto *et al.* (Org.). *Proteção de dados pessoais e investigação criminal*. Brasília: ANPR, p. 14-31, 2020.

AUTORIDADE EUROPEIA PARA PROTEÇÃO DE DADOS. Síntese do Parecer da Autoridade Europeia para a Proteção de Dados relativo à proposta da Comissão que altera a Diretiva (UE) nº 2015/849 e a Diretiva nº 2009/101/CE – Acesso a informações sobre os beneficiários efetivos e implicações para a proteção de dados, 2017.

BADARÓ, Gustavo. O debate constitucional sobre privacidade, intimidade e proteção de dados no Brasil. In: CRUZ, Francisco Brito; SIMÃO, Bárbara (Ed.). *Direitos fundamentais e processo penal na era digital* [livro eletrônico]. São Paulo: InternetLab, 2021 (sem paginação).

BALTAZAR JUNIOR, José Paulo. *Sigilo bancário e privacidade*. Porto Alegre: Livraria do Advogado, 2005.

BELLOQUE, Juliana Garcia. *Sigilo bancário: análise crítica da LC 105/2001*. São Paulo: Revista dos Tribunais, 2003.

BIALSKI, André; VENTO, Antonio; MESSINA, Eduardo; WIEGERINCK, Oliver. *Transparência no tratamento de dados por UIFs: em busca de um benchmark*. São Paulo: FGV-Data Privacy Brasil, 2021 (no prelo).

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020.

BORGES, Ademar. O relatório de inteligência financeira como meio de obtenção de prova no processo penal. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 176, p. 69-105, 2021.

BOTTINI, Pierpaolo Cruz. Os limites da atuação do COAF. *Consultor Jurídico*, 29.03.2021. Disponível em: <https://www.conjur.com.br/2021-mar-29/direito-defesa-limites-atuacao-coaf>. Acesso em: 8 ago. 2021.

COAF – CONSELHO CONTROLE DE ATIVIDADES FINANCEIRAS. *Inteligência financeira: aspectos práticos do intercâmbio internacional via Rede Egmont*. [s.l.: s.n., s.d.]. Disponível em: [https://www.youtube.com/watch?v=i5N\\_LqLmewl](https://www.youtube.com/watch?v=i5N_LqLmewl). Acesso em: 8 ago. 2021.

COMISSÃO DE JURISTAS DA CÂMARA DOS DEPUTADOS. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal, 2020.

DIMOULIS, Dimitri; MARTINS, Leonardo. *Teoria geral dos direitos fundamentais*. 8. ed. São Paulo: Revista dos Tribunais, 2021.

DOMINGOS, Fernanda Teixeira Souza; ABREU E SILVA, Melissa Garcia Blagitz; OLIVEIRA, Neide M. Cavalcanti Cardoso de. Transferência internacional de dados pessoais para fins de investigações criminais à luz das leis de proteção de dados pessoais. In: ARAS, Vladimir Barros; DE MENDONÇA, Andrey Borges; CAPANEMA, Walter Aranha (Org.). *Proteção de dados pessoais e investigação criminal*. Brasília: ANPR, p. 140-162, 2020.

DONEDA, Danilo. *Da privacidade à proteção de dados*. 2. ed. São Paulo: Revista dos Tribunais, 2020.

ESTELLITA, Heloisa; GLEIZER, Orlandino. A investigação penal de insuspeitos. *Folha de S. Paulo*, p. A3, 2020.

\_\_\_\_\_; \_\_\_\_\_. MONTENEGRO, Lucas. Por um direito de segurança pública. *Estadão*, 05.10.2020. Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/por-um-direito-de-seguranca-publica/>. Acesso em: 9 set. 2021.

EUROPEAN DATA PROTECTION SUPERVISOR. *Opinion 1/2017* – EDPS Opinion on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC Access to beneficial ownership information and data protection implications. [s.l.: s.n.], 2017.

\_\_\_\_\_. Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing. [s.l.: s.n.], 2020.

EUROPEAN DATA PROTECTION BOARD. Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive – Adopted on 2 February 2021. 2021.

FERRAZ JÚNIOR, Tércio Sampaio. Comunicação de dados e proteção aos sigilo. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Boas (Coord.). *Lei geral de proteção de dados (Lei nº 13.709/2017): a caminho da efetividade*. São Paulo: Thomson Reuters Brasil, p. 165-176, 2020.

GRECO, Luís, O inviolável e o intocável no direito processual penal: considerações introdutórias sobre o processo penal alemão (e suas relações com o direito constitucional, o direito de polícia e o direito dos serviços de inteligência). In: WOLTER, Jürgen. *O inviolável e o intocável no direito processual penal: reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da perseguição penal*. Madri; Barcelona; Buenos Aires; São Paulo: Marcial Pons, p. 21-82, 2019.

\_\_\_\_\_; GLEIZER, Orlandino. A infiltração online no processo penal – Notícia sobre a experiência alemã. *Revista Brasileira de Direito Processual Penal*, v. 5, n. 3, p. 1483-1518, 2019.

\_\_\_\_\_; LEITE, Alaor. Discussão do Supremo sobre caso COAF joga luz em lacuna legislativa. *Folha de S. Paulo*, 19.11.2019. Disponível em: <https://www1.folha.uol.com.br/poder/2019/11/discussao-do-supremo-sobre-caso-coaf-joga-luz-em-lacuna-legislativa.shtml>. Acesso em: 23 set. 2021.

GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. *O direito de proteção de dados no processo penal e na segurança pública*. São Paulo: Marcial Pons, 2021.

GREENLEAF, Graham; TYREE, Alan. Bankers' Duties and Data Privacy Principles: Global Trends and Asia-Pacific Comparisons. In: BOOYSEN, Sandra; NEO, Dora (Org.). *Can Banks Still Keep a Secret?: Bank Secrecy in Financial Centres Around the World*. Cambridge: Cambridge University Press, p. 31-61, 2017.

KALKBRENNER, Arndt; KOCH, Christian. *Bankgeheimnis und Datenschutz*. 4. ed. Wiesbaden: DG Verlag, 2019.

KHAN, Sana. The Fourth AML Directive and the EU's Approach to Data Protection: a precautionary warning. *ACAMS Today*, 15.07.2016. Disponível em: <https://www.acamstoday.org/fourth-aml-directive-eus-approach-to-data-protection/>. Acesso em: 23 set. 2021.

LIMA, Renato Sérgio de; BUENO, Samira; MINGARDI, Guaracy. Estado, polícias e segurança pública no Brasil. *Revista Direito GV*, v. 12, n. 1, p. 49-85, 2016.

LUZ, Yuri. Bancos de dados públicos e o compartilhamento com agências penais. In: CRUZ, Francisco Brito; SIMÃO, Bárbara (Ed.). *Direitos fundamentais e processo penal na era digital* [livro eletrônico]. São Paulo: InternetLab, 2021 (sem paginação).

MALISH, Richard. *Financial crime and compliance management under GPR (White Paper)*. [s.l.]: Nice Actimize, 2018.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional*. 13. ed. São Paulo: Saraiva Educação, 2018 (livro eletrônico).

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. *Pensar – Revista de Ciências Jurídicas*, v. 25, n. 04, p. 1-18, 2020.

MORÁN MARTÍNEZ, Rosa Ana. Garantías requeridas en la UE para la transferencia internacional de datos a terceros países en la cooperación judicial penal. In: ARAS, Vladimir Barros; DE MENDONÇA, Andrey Borges; CAPANEMA, Walter Aranha (Org.). *Proteção de dados pessoais e investigação criminal*. Brasília: ANPR, p. 163-196, 2020.

MOTA, Gibran Ayupe; HERKENHOFF, Henrique Geaquinto; LIRA, Pablo *et al.* Constitucionalização da atividade de inteligência – Perspectivas e desafios brasileiros. *Revista Brasileira de Segurança Pública*, v. 12, n. 1, p. 134-150, 2018.

OLIVEIRA, Nina Ribeiro Nery. As novas resoluções do Banco Central e da Comissão de Valores Mobiliários e o sigilo dos dados compartilhados na forma da Lei 9.613/98. *Revista de Direito Penal Econômico e Compliance*, v. 4, p. 162-193, 2020.

PEÑA ZAFRA, Manuel. Vinculación entre protección de datos de carácter personal y prevención de blanqueo de capitales. In: *Estudios sobre controle del fraude fiscal y prevención del blanqueo de capitales*. Navarra: Thomson Reuters Aranzadi, p. 227-239, 2016.

PREZIOSI, Camilleri. Finding the balance between data protection and AML requirements. Lexology. Disponível em: <https://www.lexology.com/library/detail.aspx?g=8aabfbf8-33c1-456d-869b-ef1f56ec0e08>. Acesso em: 29 set. 2021.

ROGALL, Klaus. Moderne Fahndungsmethoden im Lichte gewandelten Grundrechtsverständnisses. *Goldammer's Archiv für Strafrecht*, v. 1985, p. 1-27.

\_\_\_\_\_. Informationseingriff und Gesetzesvorbehalt im Strafprozeßrecht. *Zeitschrift für die gesamte Strafrechtswissenschaft*, v. 103, n. 4, 1991.

\_\_\_\_\_. § 53. In: WOLTER, Jürgen (Org.). *Kommentar SK-StPO*. [s.l.]: Carl Heymanns, 2018.

SALOMÃO NETO, Eduardo. *Direito bancário*. 3. ed. São Paulo: Trevisan, 2020.

SILVA, Virgílio Afonso da. *Direito constitucional brasileiro*. São Paulo: Editora Universidade de São Paulo, 2021.

SOARES, Hugo. Estupro, dever de comunicação às autoridades e titularidade da ação penal: reflexões derivadas da Resolução do Cremerj nº 296/2019, que estabelece a notificação de estupros aos órgãos competentes investigativos em casos atendidos por médicos no Estado do Rio de Janeiro. In: ESTELLITA, Heloisa;

SIQUEIRA, Flávia (Org.). *Direito Penal da Medicina*. São Paulo: Marcial Pons, p. 347-356, 2020.

SOUTO, Gabriel; ROSAL, Isabela. O direito à proteção de dados pessoais à luz da jurisprudência do STF. *Lapin*, 31.03.2021. Disponível em: <https://lapin.org.br/2021/03/31/o-direito-fundamental-a-protECAo-de-dados-pessoais-a-luz-da-jurisprudencia-do-supremo-tribunal-federal/>. Acesso em: 8 ago. 2021.

SUPREMO TRIBUNAL FEDERAL. RE 377.457, Tribunal Pleno, Rel. Min. Gilmar Mendes, DJe 18.11.2008.

\_\_\_\_\_. RE 593.727, Tribunal Pleno, Rel. Min. Cezar Peluso, DJ 08.09.2015.

\_\_\_\_\_. RE 1.055.941, Tribunal Pleno, Rel. Min. Dias Toffoli, J. 04.12.2019, DJe 06.10.2020.

\_\_\_\_\_. MC-ADIn 6.529, Tribunal Pleno, Rel<sup>a</sup> Min. Cármen Lúcia, DJe 15.10.2020.

\_\_\_\_\_. ADIn 6.387-MC-Ref, Tribunal Pleno, Rel<sup>a</sup> Min. Rosa Weber, DJe 12.11.2020.

TEIXEIRA, Adriano; WEHRS, Carlos; MADRUGA, Antenor. O valor processual das informações de inteligência financeira obtidas por meio do Grupo Egmont. *JCC*, v. 2, n. 2, p. 21-30, 2019.

VOGEL, Benjamin; MAILLART, Jean-Baptiste (Ed.). *National and international anti-money laundering law: developing the architecture of criminal justice, regulation and data protection*. Cambridge, Antwerp, Chicago: Intersentia, 2020.

WOLTER, Jürgen. *O inviolável e o intocável no direito processual penal: reflexões sobre a dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal*. São Paulo: Marcial Pons, 2019.

#### Sobre a autora:

**Heloísa Estelita** | E-mail: [heloisa.estelita@fgv.br](mailto:heloisa.estelita@fgv.br)

Professora da Escola de Direito da Fundação Getúlio Vargas e Coordenadora do Grupo de Ensino e Pesquisa em Direito Penal Econômico e da Empresa na mesma instituição. Bolsista da Alexander von Humboldt Stiftung. Doutora em Direito Penal pela Universidade de São Paulo. Mestre em Direito pela Universidade Estadual Paulista.

Data de submissão: 30 de setembro de 2021.

Data de aceite: 10 de dezembro de 2021.