

# DIREITOS FUNDAMENTAIS E PROCESSO PENAL NA ERA DIGITAL /

---

*DOCTRINA E PRÁTICA EM DEBATE < VOL.4 >*

---

FRANCISCO BRITO CRUZ (ED.) / BÁRBARA SIMÃO (ED.) / CAROLINA  
RICARDO / DIOGO MALAN / ELOÍSA MACHADO / FERNANDA TEIXEIRA  
SOUZA DOMINGOS / GUSTAVO BADARÓ / JAQUELINE ABREU / MAURÍCIO  
DIETER / MELISSA GARCIA BLAGITZ DE ABREU E SILVA / NEIDE  
MARA CARDOSO DE OLIVEIRA / ORLANDINO GLEIZER / SARAH LAGESON  
/ TERCIO SAMPAIO FERRAZ JR. / YURI LUZ

**INTERNETLAB**  
pesquisa em direito e tecnologia

# DIREITOS FUNDAMENTAIS E PROCESSO PENAL NA ERA DIGITAL /

-----  
*DOCTRINA E PRÁTICA EM DEBATE < VOL.4 >*  
-----

FRANCISCO BRITO CRUZ (ED.) / BÁRBARA SIMÃO (ED.) / CAROLINA  
RICARDO / DIOGO MALAN / ELOÍSA MACHADO / FERNANDA TEIXEIRA  
SOUZA DOMINGOS / GUSTAVO BADARÓ / JAQUELINE ABREU / MAURÍCIO  
DIETER / MELISSA GARCIA BLAGITZ DE ABREU E SILVA / NEIDE  
MARA CARDOSO DE OLIVEIRA / ORLANDINO GLEIZER / SARAH LAGESON  
/ TERCIO SAMPAIO FERRAZ JR. / YURI LUZ

**INTERNETLAB**  
pesquisa em direito e tecnologia

# DIREITOS FUNDAMENTAIS E PROCESSO PENAL NA ERA DIGITAL /

*DOCTRINA E PRÁTICA EM DEBATE < VOL.4 >*

FRANCISCO BRITO CRUZ (ED.) / BÁRBARA SIMÃO (ED.) / CAROLINA  
RICARDO / DIOGO MALAN / ELOÍSA MACHADO / FERNANDA TEIXEIRA  
SOUZA DOMINGOS / GUSTAVO BADARÓ / JAQUELINE ABREU / MAURÍCIO  
DIETER / MELISSA GARCIA BLAGITZ DE ABREU E SILVA / NEIDE  
MARA CARDOSO DE OLIVEIRA / ORLANDINO GLEIZER / SARAH LAGESON  
/ TERCIO SAMPAIO FERRAZ JR. / YURI LUZ

**INTERNETLAB**  
pesquisa em direito e tecnologia

SÃO PAULO, 2021

O InternetLab é uma organização sem fins lucrativos dedicada à produção de pesquisa acadêmica aplicada com impacto em políticas públicas de tecnologia e Internet no Brasil.

### **Citação sugerida**

BRITO CRUZ, Francisco; SIMÃO, Bárbara (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. IV. São Paulo. InternetLab, 2021.

Este trabalho está licenciado sob uma licença Creative Commons CC BY-NC-SA 4.0 BR. Esta licença permite que outros remixem, adaptem e criem obras derivadas sobre a obra original, desde que com fins não comerciais e contanto que atribuam crédito aos autores e licenciem as novas criações sob os mesmos parâmetros. Toda nova obra feita a partir desta deverá ser licenciada com a mesma licença, de modo que qualquer obra derivada, por natureza, não poderá ser usada para fins comerciais.

Avenida Ipiranga 344 cj 11B  
01046-010 | São Paulo | SP | Brasil

ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA

[www.internetlab.org.br](http://www.internetlab.org.br)

09 .

---

TRANSFERÊNCIA  
INTERNACIONAL DE  
DADOS PARA FINS  
DE INVESTIGAÇÕES  
CRIMINAIS: À LUZ  
DAS LEIS DE PROTEÇÃO  
DE DADOS PESSOAIS

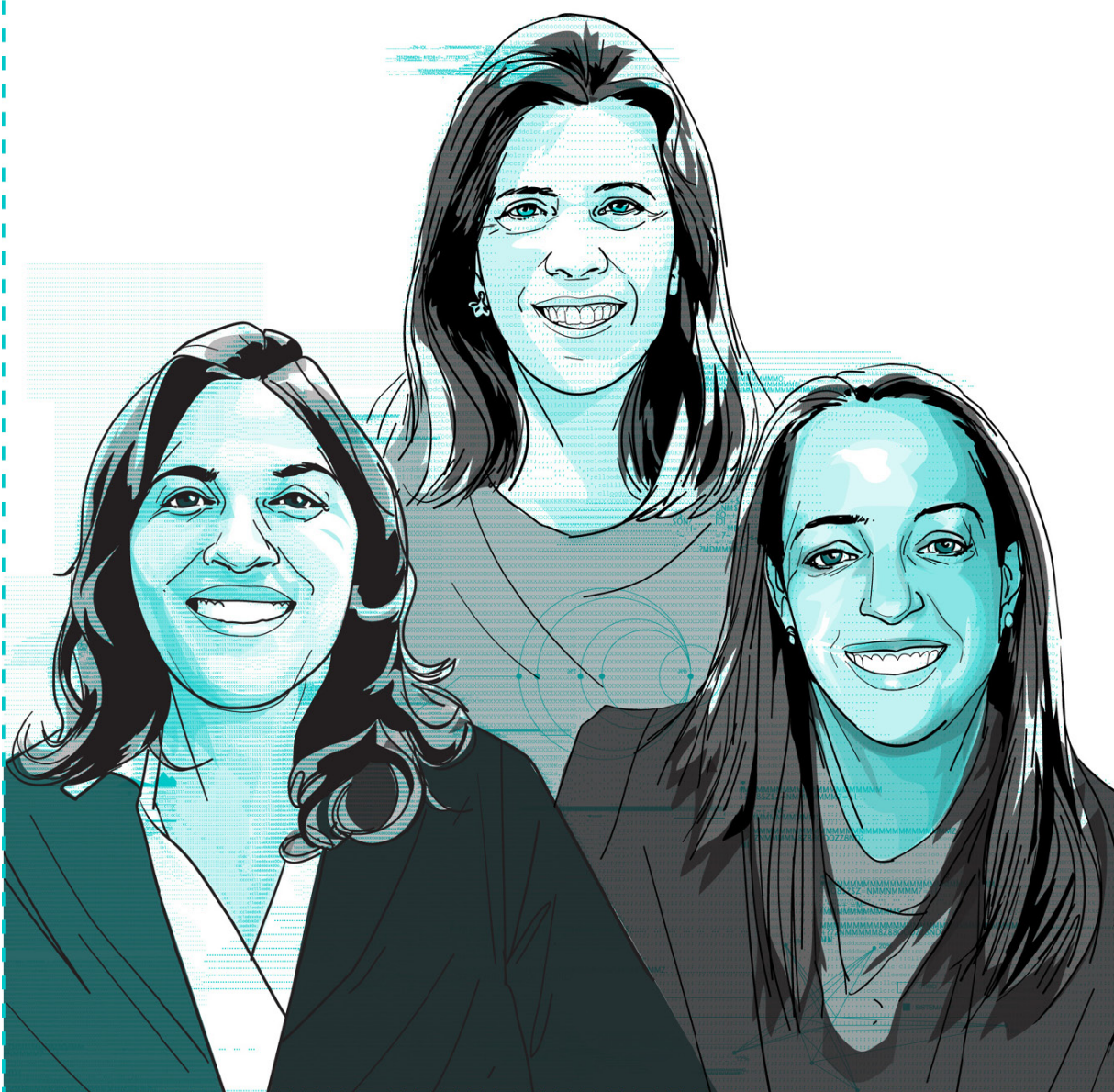
---

**Fernanda Teixeira Souza Domingos**  
**Melissa Garcia Blagitz de Abreu e Silva**  
**Neide M. Cavalcanti Cardoso de Oliveira**

---



Fernanda Teixeira Souza Domingos, Melissa Garcia Blagitz de Abreu e Silva  
e Neide M. Cavalcanti Cardoso de Oliveira



## 1. Introdução

Para discorrer sobre proteção aos dados de investigação e cooperação jurídica internacional criminal é essencial contextualizar a Lei Geral de Proteção de Dados brasileira e seus desdobramentos, no âmbito da cooperação jurídica internacional. Nesse contexto, relativamente à matéria penal, é necessário informar que o Brasil se encontra em processo de adesão à Convenção do Conselho da Europa contra a Cibercriminalidade, também conhecida como Convenção de Budapeste.

A Convenção sobre Cibercriminalidade do Conselho da Europa – ETS n° 185 (CONSELHO DA EUROPA, 2001) é atualmente o principal instrumento internacional para a persecução de crimes cibernéticos e obtenção de provas eletrônicas. As principais economias do mundo já a ratificaram ou estão em processo de adesão, excetuando-se China e Rússia. São membros da Convenção, além dos países do Conselho da Europa, Estados Unidos, Austrália, Japão, Canadá, Argentina e Chile dentre outros. O Brasil foi convidado a aderir em dezembro de 2019 e, atualmente, enquanto em processo de ratificação,<sup>25</sup> possui *status* de observador.

Além de conter a tipificação de condutas penais referentes a crimes cibernéticos próprios e de outros facilitados pelo meio eletrônico (artigos 2° a 10°), a **Convenção traz ainda em seus artigos 14° a 35° instrumentos de investigação e compartilhamento de dados e provas eletrônicas entre os Estados-membros.**

O pedido de adesão do Brasil, encaminhado por meio do Ministério das Relações Exteriores (MRE), foi resultado de anos de trabalho do Ministério Público Federal junto a esse órgão, analisando-os os benefícios a serem proporcionados ao Brasil pela Convenção e sobre sua compatibilidade com a legislação brasileira.<sup>26</sup> A **principal vantagem será o estabelecimento de uma cooperação jurídica internacional, mais eficiente e confiável, com os países membros da Convenção.**

Além disso, **espera-se conseguir mais agilidade na transferência de provas relacionadas a crimes cibernéticos, bem como de provas eletrônicas, o que**

inclui, na maioria das vezes, a transferência de dados pessoais de investigados. Necessário, assim, analisar os dois regimes de proteção de dados pessoais, o brasileiro e o europeu, a fim de se determinar o arcabouço atual de transferência de dados para fins penais.

## 2. O Regime Brasileiro de Proteção de Dados

A LGPD, Lei nº 13.709, foi aprovada em 14 de agosto de 2018, com um período de *vacatio legis* de dois anos. Após a indefinição sobre a sua entrada em vigor, inicialmente prevista para 14 de agosto de 2020, se não fosse o artigo 4º da Medida Provisória (MP) nº 959, para maio de 2021, a norma passou a ter vigência em 18 de setembro, quando sancionada em lei a MP, que restou aprovada sem aquele dispositivo. No entanto, as sanções administrativas (artigos 52 a 54) nela previstas foram postergadas para 1º de agosto de 2021, devido à aprovação da Lei nº 14.010/2020, que trata do Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado.

Seguindo o regulamento geral de proteção de dados europeu – *General Data Protection Regulation* (GDPR) – Regulamento (UE) n. 2016/679 do Parlamento Europeu e do Conselho da União Europeia, a LGPD prevê várias regras com o fim de garantir a máxima proteção e segurança na transferência internacional de dados. E da mesma forma que a legislação europeia, a lei brasileira disciplina três regimes diferentes de salvaguardas para transferências internacionais de dados, que seriam:

- < i > a declaração de existência de grau de proteção de dados pessoais, adequado ao previsto na LGPD;
- < ii > a existência de garantias de cumprimento dos preceitos da LGPD;
- < iii > derrogações específicas do regime da LGPD, casuisticamente listados com vistas a promover algum objetivo de interesse público. (...) a manutenção de três regimes diferentes está – ao menos em tese – em consonância com o ponto de vista de que a proteção de dados pessoais está



intimamente relacionada à proteção de direitos fundamentais. (CARVALHO, 2019, p. 624).

Para melhor compreensão do assunto aqui tratado, faz-se necessária uma breve análise de cada um deles.

### 2.1. Da Transferência de Dados para Países com Regime Adequado de Proteção

No inciso I do art. 33 da LGPD está prevista a permissão de transferência internacional de dados para países, ou organismos internacionais, que proporcionem nível adequado de proteção. Esse dispositivo, entretanto, não esclarece os detalhes para a qualificação de determinado sistema legal como “adequado” aos preceitos da lei brasileira. Tal função é reservada à autoridade nacional, no art. 34, que em seus incisos prevê as bases que devem ser levadas em consideração.

Assim, a lei brasileira não exige que ordenamentos estrangeiros contem com uma legislação específica sobre proteção de dados, mas que, “*em última análise, o núcleo fundamental da LGPD possa ser encontrado, ainda que difusamente, no ordenamento destinatário dos dados a serem transferidos*”. (CARVALHO, 2019, p. 626).

Essa análise caberá à Autoridade Nacional de Proteção de Dados e sua decisão, com efeitos amplos e gerais, significará sua postura diante daquele ordenamento, e deverá ser considerada como declaração de idoneidade daquele ordenamento, por determinado período de tempo, sobre o qual esse posicionamento pode ser alterado (CARVALHO, 2019, p. 626).

### 2.2. Da Transferência de Dados Quando Há Garantias de Cumprimento dos Preceitos da LGPD

O segundo regime de transferência internacional de dados, trazido no art. 33, inc. II, do diploma, prevê essa possibilidade mediante “*a existência de garantias de cumprimento dos preceitos da LGPD*”. Isso permite, mesmo em um quadro normativo com um nível de proteção menor que a legislação brasileira, a transferência de dados com base em salvaguardas apresentadas

pela parte requerente dos dados, aprovadas pela autoridade nacional, conforme previsto na LGPD, em observância aos padrões fixados por autoridades de controle independentes e desvinculadas de governos. (CARVALHO, 2019, p. 627).

Nesse caso, mesmo que o país estrangeiro para onde os dados se destinem não dê todas as salvaguardas necessárias ao atendimento dos padrões protetivos previstos pela LGPD, é possível que o controlador específico ofereça e comprove garantias de cumprimento dos preceitos da lei brasileira, seja por meio de cláusulas contratuais (padrão ou específicas), normas corporativas globais, ou selos, certificados e códigos de conduta regularmente emitidos.

### 2.3. Transferência de Dados em Razão do Interesse Público

Por fim, a LGPD prevê um terceiro regime para a transferência internacional de dados, disposto nos seus incisos III a VIII do art. 33, que são situações específicas, não abrangidas pelos incisos anteriores, que visam outros objetivos de interesse público, *in verbis*:

- < III > quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
- < IV > quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- < V > quando a autoridade nacional autorizar a transferência;
- < VI > quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
- < VII > quando for necessária para a execução de política pública ou atribuição legal do serviço público;
- < VIII > quando o titular tiver fornecido o seu consentimento específico para a transferência, com informação prévia sobre o

caráter internacional da operação, distinguindo claramente essa de outras finalidades;

< IX > quando necessário para atender às hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

## 2.4 Transferência de Dados em razão da Segurança Pública, Atividades de Investigação e Repressão de Infrações Penais

Nos termos do art. 4º, III da LGPD, os dados pessoais destinados à segurança pública e às atividades de investigação e repressão de infrações penais, bem como à segurança pública e à defesa nacional estão excepcionados das regras de proteção previstas na LGPD, à semelhança da redação do GDPR, que também os excepciona. Em ambos os regimes, há a previsão da edição de normas específicas para regulamentar a proteção e transferência de dados pessoais para fins de persecução penal.

A União Europeia já tem um regulamento próprio trazido pela Diretiva (UE) n. 2016/680 (UNIÃO EUROPEIA, 2016) do Parlamento Europeu e do Conselho da União Europeia, que trata da proteção dos dados referentes à prevenção, investigação e persecução penal, bem como repressão de infrações penais e execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. Mas o Brasil, não. Embora o artigo 33 faça expressa menção à possibilidade de transferência internacional de dados “quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional”, dentre outras situações, o artigo 4º, §1º da LGPD dispõe que deve haver legislação específica para a matéria.

Assim, em notícia publicada pela Câmara dos Deputados (JÚNIOR, 2019), em novembro de 2019, foi criada, pelo seu presidente, uma Comissão Parlamentar na Câmara dos Deputados formada por juristas renomados no tema, para propor projeto de lei sobre o uso de dados pessoais em investigações penais e segurança pública.

Com a entrada em vigor da LGPD e a esperada breve ratificação pelo Brasil da Convenção de Budapeste, almeja-se que essa Comissão possa acelerar a retomada dos trabalhos, interrompida com a pandemia da Covid-19. Pretende-se que o projeto de lei sobre a proteção de dados pessoais referentes a segurança pública, defesa nacional e investigações criminais seja finalizado e aprovado o mais breve possível.

As previsões das exceções devem observar os princípios previstos no art. 6º da Lei, principalmente os da finalidade e da segurança. Alguns princípios presentes na LGPD, também constam em outras leis de primeira e segunda geração, segundo Doneda (2011), uma vez que são universais e facilitam a transferência internacional de dados.

### **3. O Regime Europeu de Transferência Internacional de Dados**

Conforme exposto, a LGPD se inspira em diversos dispositivos do GDPR para regular a proteção de dados. Em linhas gerais, em seu artigo 45, o regulamento europeu também permite a transferência de dados quando há o reconhecimento de que o ordenamento jurídico do país recipiente possui nível de proteção adequado, ou quando o controlador apresenta salvaguardas apropriadas – art. 46.

Entretanto, conforme descrito acima, a transmissão de dados para fins de persecução penal entre países regidos pelo GDPR e outros deverá obedecer ao regramento próprio trazido pela Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho da União Europeia.

#### **3.1. O Regime da Diretiva “Policial” (UE) 2016/680**

Com a regulação da proteção dos dados pessoais no âmbito da União Europeia, surge a questão relativa ao tratamento a ser dispensado aos dados pessoais coletados com os fins de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais - salvaguardas e prevenção de ameaças à segurança pública.

**Evidente que tais dados não poderiam seguir o mesmo regime dos dados comuns, delineado no Regulamento (UE) 2016/679 do Parlamento Europeu**

e do Conselho – o GDPR, uma vez que, para estes dados, com finalidade específica voltada à segurança pública, há uma imposição na coleta e tratamento que não se coaduna com o consentimento, um dos pilares da nova regulação. Logo, o consentimento do titular dos dados não pode ser o fundamento jurídico do tratamento desses dados pelas autoridades competentes. Isso não significa que tais dados estarão isentos de proteção na sua coleta, tratamento e compartilhamento.

Dessa maneira, os dados coletados pelas autoridades competentes com os fins de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais - salvaguardas e prevenção de ameaças à segurança pública devem circular livremente entre as autoridades competentes congêneres justamente para permitir a eficiência na manutenção da ordem e segurança públicas. É isso o que a Diretiva (UE) n. 2016/680 aponta no item (4) da sua explanação de motivos ao dizer que a transferência desses dados para países terceiros e organizações internacionais deve ser facilitada, assegurando-se simultaneamente um elevado nível de proteção dos dados pessoais.

Assim, a proteção de dados pessoais no domínio da cooperação jurídica em matéria penal e da cooperação policial assenta-se em garantir que as autoridades estrangeiras e/ou organismos internacionais dispensarão aos dados compartilhados o mesmo nível de proteção e tratamento que lhes é dispensado pelas autoridades que os detêm. Isso diz respeito, por exemplo, à finalidade específica de uso desses dados pessoais, que deve ser permitida pela autoridade que os compartilha, não podendo ser reutilizados para outros fins sem sua prévia autorização; à confidencialidade e segurança que devem ser garantidos a tais dados, de forma que o acesso, a utilização desses dados e do equipamento empregada para o seu tratamento somente estejam franqueados a pessoas autorizadas.

O item 31 da explanação de motivos da Diretiva esclarece ainda que, ao se levar em conta a circulação desses dados em cooperação jurídica em matéria penal e em cooperação policial, é esperada, quando aplicável, a



distinção entre dados pessoais de diferentes categorias de titulares de dados como: suspeitos, pessoas condenadas, vítimas, terceiros, assim entendidos testemunhas e informantes e outras pessoas consideradas relevantes para as investigações. Podem, ainda, ser previstas condições reputadas necessárias pelas autoridades transmissoras dos dados, como proibição de notificação do titular dos dados ou garantias adicionais quando os dados transmitidos forem considerados dados sensíveis que toquem direitos e liberdades fundamentais.

A autoridade competente para remessa e recebimento dos dados pessoais regulados pela Diretiva, nos termos do seu art. 3º, número 7, são precisamente as autoridades públicas competentes para exercer as atividades de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.

Assim, o diploma apresenta como formas de validar a transferência internacional dos dados a ela pertinentes:

- a decisão de adequação, que reconhece no país terceiro, no organismo internacional ou em um ou mais setores específicos desse país terceiro um nível de proteção de dados pessoais adequado;
- o fornecimento de garantias adequadas para essa proteção mediante um instrumento juridicamente vinculativo;
- a derrogação das regras da diretiva no caso de situações específicas: se a transferência for necessária para proteger interesses vitais do titular dos dados e/ou seus legítimos interesses, para prevenir ameaça iminente e grave contra a segurança pública de um Estado-membro ou país terceiro, e em outros em que haja justificativa, inclusive exercício ou defesa de um direito num processo judicial.

De notar-se que a decisão de adequação pode ser dada em relação a um país terceiro ou a um ou mais setores específicos desse país.

Esse dispositivo se encontra descrito no art. 36 da Diretiva e nos itens 66 a 70 da Explicação de Motivos. Ele traz os critérios adotados para decidir pela adequação, abrindo a possibilidade para a transferência de dados pessoais para um setor específico do país que já atenda o nível esperado de proteção, mesmo que o país não tenha completamente se adequado a todas as regras de proteção. Ele possibilita, portanto, que as transferências de dados pessoais para esse setor específico do país terceiro ocorram sem necessidade de autorização específica, facilitando sobremaneira a circulação dos dados pessoais e permitindo a fluidez tão desejada e necessária no âmbito da prevenção, investigação, detecção e repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.

Embora as disposições mais estritas concernentes à transferência internacional de dados pessoais para fins de investigações criminais ainda não estejam sendo aplicadas na prática, à medida que em alguns Estados se movimentaram para aumentar o grau de proteção desses dados, os demais Estados passaram a reformular suas legislações para acompanhar a evolução na sofisticação das medidas.

#### **4. Os Mecanismos de Transferência Internacional de Dados previstos na Convenção de Budapeste**

A Convenção de Budapeste indica, basicamente, duas formas de transferência internacional de dados para fins de investigações criminais, por meio de cooperação internacional e por meio de acesso direto.

##### **4.1. Cooperação Internacional**

A cooperação internacional prevista na Convenção é regida pelos arts. 23 e seguintes, podendo caracterizar-se pela transmissão espontânea de dados, art. 26,<sup>27</sup> quando um Estado-parte identifica elementos que possam justificar o início de investigação criminal por outro Estado-parte, e pelo cumprimento de pedidos de cooperação. Nesse contexto, regulado pelos

arts. 27 e seguintes, a própria Convenção pode servir como tratado disciplinador da cooperação, caso os dois envolvidos optem por utilizá-la ou caso não possuam entre si instrumento próprio de cooperação internacional.

A cooperação jurídica em matéria penal regida pela Convenção possui mecanismos próprios para assegurar a rapidez na execução dos pedidos, como a possibilidade de transmissão das solicitações entre autoridades judiciais diretamente responsáveis pelo pedido e pelo cumprimento,<sup>28</sup> com simples aviso para a autoridade central em caso de urgência, e a preservação rápida de provas,<sup>29</sup> tudo em razão da natureza volátil das provas eletrônicas. Entretanto, de maneira geral, a cooperação prevista na Convenção segue os mesmos preceitos da cooperação jurídica em matéria penal, com análise de cabimento caso a caso, e atendimento individualizado, com ou sem a imposição de condições para uso da prova.

#### 4.2. O Acesso Direto Transfronteiriço

Já os mecanismos de acesso direto trazidos pela Convenção contém avanços considerados significativos na época de sua elaboração, em 2001, embora hoje necessitem de revisão.

Os arts. 18 e 32 permitem o acesso direto a dados:

##### Artigo 18 - Requisição

< 1 > Cada Estado-Parte adotará as medidas legislativas e outras providências necessárias para dar poderes a suas autoridades competentes para ordenar:

< a > a qualquer pessoa em seu território a entrega de dados de computador especificados sob seu controle ou posse, que estejam armazenados em um sistema de computador ou em qualquer meio de armazenamento de dados de computador;

< b > a qualquer provedor de serviço que ofereça serviços no território da Parte para entregar as informações cadastrais de

usuários relacionadas a tais serviços, que estejam sob a posse ou controle do provedor.

< 2 > Os poderes e procedimentos referidos neste artigo estão sujeitos aos artigos 14 e 15.

< 3 > Para fins deste artigo, o termo “informações cadastrais do usuário” indica qualquer informação em forma eletrônica ou em qualquer outra, que esteja em poder do provedor de serviço e que seja relativa a usuários de seus serviços, com exceção dos dados de tráfego e do conteúdo da comunicação, e por meio da qual se possa determinar:

< a > o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas para esse fim e o período de serviço;

< b > a identidade do usuário, endereço postal ou geográfico, o telefone e outros números de contato e informações sobre pagamento e cobrança, que estejam disponíveis de acordo com os termos de prestação de serviço;

< c > qualquer outra informação sobre o local de instalação do equipamento de comunicação, disponível em razão dos termos de prestação de serviço,

Artigo 32 - Acesso transfronteiriço a dados de computador armazenados mediante consentimento ou quando acessíveis publicamente

Uma Parte pode, sem autorização de outra Parte:

< a > acessar dados de computador armazenados disponíveis ao público (fonte aberta), independentemente de onde os dados estejam geograficamente localizados; ou

< b > acessar ou receber, por meio de um sistema de computador em seu território, dados de computador armazenados localizados no território de outra Parte, se a

Parte obtiver o legítimo e voluntário consentimento de uma pessoa que tenha autoridade legal para entregar os dados à Parte por meio daquele sistema de computador.  
(PARLAMENTO EUROPEU E DO CONSELHO DA EUROPA, 2016).

O segundo dispositivo lida com situações aparentemente corriqueiras, mas que eram de grande valia quando da entrada em vigor da Convenção.

A alínea *a* reconhece que as autoridades dos Estados-parte podem acessar, de seu território, dados disponíveis ao público, mas que sejam guardados em outro território. A alínea *b* permite que esse acesso se estenda a dados privados desde que haja expresse consentimento do titular dos dados.

Em outras palavras, o dispositivo permite que autoridades de um país acessem e coletem como prova válida dados publicados em sítios mantidos em outro país. Condição para isso é que esses dados sejam públicos ou que seu uso seja consentido, de modo “*legítimo e voluntário*”, pelo titular.

Ao condicionar o acesso à natureza pública dos dados ou ao consentimento do titular, o dispositivo não distingue quanto ao tipo de dado, permitindo o acesso direto transfronteiriço a qualquer dado eletrônico, inclusive conteúdo de comunicações, desde que observadas as duas condições mencionadas.

Por outro lado, o art. 18 determina que os Estados-parte, em suas legislações locais, estabeleçam mecanismo que permita às autoridades judiciais a requisição de quaisquer dados armazenados sob a posse ou controle de provedores localizados em seu território (1. a) e de dados cadastrais de usuários que estejam sob a posse ou controle de provedores que prestam serviço em seu território, ainda que estrangeiros (1. b).

Há aqui, portanto, duas situações: uma que permite o acesso, mediante o cumprimento da legislação local, a todos os dados armazenados por provedores locais, incluindo conteúdo; e outra, que permite acesso a dados cadastrais de usuários controlados por provedores estrangeiros, desde que estes prestem serviço no território do Estado requisitante. Admite-se, assim,



o acesso direto a dados localizados em outro território e controlados por provedor estrangeiro desde que: a) as informações buscadas se restrinjam a dados cadastrais; e b) e o provedor estrangeiro preste serviço no território da autoridade requisitante.

A legislação brasileira, mesmo antes da adesão formal à Convenção, já permite o acesso direto a dados eletrônicos localizados fora do território brasileiro em termos semelhantes, mas mais amplos. O artigo 11 do Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014 determina que, mediante prévia ordem judicial, as autoridades brasileiras tenham acesso a dados armazenados, inclusive conteúdo de comunicações, por empresas brasileiras, ou por empresas estrangeiras desde que: a) ofereçam serviços ao público brasileiro ou b) tenham ao menos um integrante do grupo econômico com estabelecimento no Brasil.

O citado dispositivo 11 é, portanto, mais amplo que a previsão do art. 18. Enquanto este permite o acesso apenas a dados cadastrais de usuários controlados por empresas estrangeiras que prestam serviço no território do Estado-parte, aquele permite o acesso a todos os dados, inclusive conteúdo armazenado por empresa estrangeira, desde que ela ofereça serviços a brasileiros ou aqui mantenha estabelecimento de um dos componentes de seu grupo econômico.

## **5. As Consequências do Regime de Proteção de Dados para a Transferência de Dados em Investigações Criminais – Nova Proposta**

O atual sistema de proteção de dados, mesmo com regras específicas para a persecução penal, afeta diferentemente o regime de transferência de dados, dependendo do tipo de transferência utilizada.

Para as transferências por meio de cooperação internacional, os acordos de cooperação continuam servindo como base, pois a Diretiva (UE) n. 2016/680, no art. 61 expressamente ressaltou a manutenção dos tratados internacionais em vigor até que sejam alterados, substituídos ou revogados.<sup>30</sup>

Essa disposição permite a continuidade da troca de informações no âmbito da cooperação policial e da cooperação judiciária internacional. Se tal não fosse, toda a circulação de dados para fins de persecução penal a prevenção às infrações penais estaria paralisada em razão das exigências desta normativa, uma vez que o nível de proteção dos dados exigido dos países terceiros não é passível de ser alcançado no curto prazo devido às inúmeras adequações que precisam ser feitas.

Tal solução, porém, é provisória, sendo indispensável buscar solução definitiva que passa pela decisão de adequação.

Quanto ao acesso direto, os efeitos da ausência de decisão de adequação podem começar a ser sentidos imediatamente. Como mencionado, a Convenção de Budapeste prevê dois tipos. O previsto no art. 32 não é afetado pelas disposições da Diretiva porque se refere a dados públicos, não abrangidos pelo regime de proteção de dados, ou a dados privados que são acessados mediante o consentimento do titular. Não há, assim, problema para a transferência.

Entretanto, o assunto adquire outra relevância quando se trata de acesso direto à prova eletrônica, nos termos do art. 18 da Convenção de Budapeste e do art. 11 do Marco Civil. Nesses casos, sem decisões prévias de adequação ou de reconhecimento de salvaguardas, as empresas europeias que aqui prestam serviços a usuários brasileiros podem se considerar impedidas de transferir os dados, com sérias consequências para investigações penais em andamento.

Enquanto a decisão sobre a adequação do regime brasileiro de proteção de dados não vem, e na pendência da ratificação da Convenção de Budapeste, que poderá servir como respaldo jurídico para a transferência de dados pessoais, faz-se necessário o estabelecimento de outro modelo, que permita que o fluxo de dados para fins de persecução penal não seja interrompido.<sup>31</sup> Nesse sentido, propõe-se ao Ministério Público Federal adequação ao quanto exigido pela Diretiva e pelo GDPR, recebendo em nome próprio a decisão de adequação.

Como exposto, nos termos do art. 36 da Diretiva (UE) n. 2016/680, a decisão de adequação pode ser concedida não apenas a países terceiros, mas a territórios ou a um ou mais setores específicos de um determinado país. Exemplo disso, é a decisão de adequação, ainda vigente apesar de baseada na antiga Diretiva (UE) n. 95/46 - substituída pelo GDPR -, que reconhece apenas os setores abrangidos pela lei canadense de dados pessoais e documentos eletrônicos como adequados à regulação europeia.<sup>32</sup> É possível, assim, que determinados setores sejam reconhecidos como adequados, ainda que o país como um todo não o seja.

Neste ponto é que se propõe que o sistema nacional de Justiça, em especial o Ministério Público e o Poder Judiciário, busquem a adequação exigida pelo GDPR e pela Diretiva (UE) n. 2016/680.

Enquanto o Brasil, como Nação, não obtém a decisão de adequação, o que hoje depende, em grande parte, da estrutura da Autoridade Nacional de Proteção de Dados - ANPD, tanto o Ministério Público, quanto o Poder Judiciário, podem buscar essa adequação para fins de acesso direto de dados em investigações criminais, como um setor específico.

Embora ainda não tenha sido editada lei regulamentando a proteção de dados referentes a segurança pública e investigações criminais, é certo que o sistema de Justiça brasileiro tem todas as condições de se adequar ao regime da diretiva. O acesso a dados pessoais somente é feito mediante ordem judicial, por meio de decisão fundamentada, em casos específicos e para a investigação de condutas determinadas. Os dados obtidos são mantidos sob sigilo durante todo o processo penal, com acesso restrito às partes. O uso em outros feitos depende também de autorização judicial, o que estabelece sistema robusto de proteção. Ademais, o titular dos dados é informado da obtenção e do uso, ainda que de forma diferida, possuindo mecanismos legais para excluir os dados a qualquer momento, seja nos próprios autos, ou por meio de ações autônomas, como *habeas corpus* e mandado de segurança.

Importante notar que o sistema legal, em vigor, não precisa ser uma cópia, ou o reconhecimento item por item das previsões do sistema europeu, bastando que as proteções sejam equivalentes. Ademais, a análise da adequação do setor funda-se nos aspectos específicos desse setor. O item 67 da exposição de motivos determina que:

De acordo com os valores fundamentais em que a União assenta, particularmente a defesa dos direitos humanos, a Comissão deverá, na sua avaliação do país terceiro ou de um território ou de um setor específico num país terceiro, ter em consideração em que medida um determinado país respeita o primado do Estado de direito, o acesso à justiça, bem como as regras e normas internacionais no domínio dos direitos humanos e a sua legislação geral e setorial, nomeadamente a legislação relativa à segurança pública, à defesa e à segurança nacional, bem como a lei da ordem pública e a lei penal. *A adoção de uma decisão de adequação relativa a um território ou um setor específico num país terceiro deverá ter em conta critérios claros e objetivos, tais como as atividades de tratamento específicas e o âmbito das normas jurídicas aplicáveis, bem como a legislação em vigor no país terceiro.* Este deverá dar garantias de assegurar um nível adequado de proteção, essencialmente equivalente ao *segurado na União*, em particular quando os dados são tratados num ou em vários setores específicos. Em especial, o país terceiro deverá garantir o controle efetivo e independente da proteção dos dados e estabelecer mecanismos de cooperação com as autoridades de proteção de dados dos Estados-Membros, e ainda conferir aos titulares dos dados direitos efetivos e oponíveis e vias efetivas de recurso administrativo e judicial (UNIÃO EUROPEIA, 2016 - Grifos nossos)

Vê-se, portanto, que para fins de investigações e processos criminais, o arcabouço legal, em vigor, no Brasil, já atende ao quanto exigido pela


diretiva e pelo GDPR. Embora ainda não haja legislação específica sobre o assunto, como exigido pela LGPD, as limitações impostas pela Constituição Federal, pelo Marco Civil e pela legislação processual penal já são suficientes para assegurar proteção adequada aos dados e demonstrar adequação ao sistema europeu. Assim, o reconhecimento dessa adequação é medida que pode ser buscada pelo Poder Judiciário e Ministério Público, como um setor à parte.

## 6. Conclusão

O novo sistema de proteção de dados pessoais introduzido pelo GDPR, pela Diretiva (UE) n. 2016/680, e pela LGPD precisa ser levado em consideração na busca de provas em investigações e processos criminais.

Esse sistema pode gerar consequências para a correta aplicação do art. 11 do Marco Civil da Internet, em especial, quanto à obtenção de dados de empresas europeias, que prestam serviço no Brasil, e que, por estarem submetidas aos diplomas normativos da UE, podem criar empecilhos para o acesso direto aos dados, na forma da lei brasileira.

Solução de longo prazo, e que precisa ser buscada, é o reconhecimento da adequação da legislação brasileira ao quanto exigido pelas normas europeias. Enquanto essa adequação não é obtida, o Poder Judiciário e o Ministério Público podem buscar o reconhecimento da adequação como setor específico, que já cumpre o quanto exigido.

Isso permitirá que os dados sejam transferidos sem interrupção para fins de persecução penal, possibilitando a continuidade de investigações em andamento e assegurando a celeridade exigida pela natureza da prova eletrônica. 

---

**25** O pedido de ratificação foi encaminhado à Câmara dos Deputados, no dia 22 de julho de 2020, após o convite do Conselho da Europa para a adesão pelo Brasil à referida Convenção.

---

**26** Disponível em: <http://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/notas-tecnicas>. Acesso em 14 out.2020.



---

**27** Art. 26 - Uma Parte pode, dentro dos limites de sua legislação interna e sem pedido anterior, transmitir, para outra Parte, informações obtidas por seu próprio sistema investigativo, quando considerar que o encaminhamento de tais informações pode auxiliar a Parte destinatária a iniciar ou a levar adiante investigações ou procedimentos relativos a crimes tipificados de acordo com esta Convenção ou possa levar a um pedido de cooperação por aquela Parte, em conformidade com este capítulo (...). (Tradução nossa).

---

**28** Art. 27, 9 a.

---

**29** Art. 29.

---

**30** Art. 61. Os acordos internacionais que impliquem a transferência de dados pessoais para países terceiros ou para organizações internacionais, celebrados pelos Estados-Membros antes de 6 de maio de 2016, e que sejam conformes com o direito da União tal como aplicável antes dessa data, continuam a vigorar até serem alterados, substituídos ou revogados.

---

**31** Tratados internacionais podem servir de base legal para permitir a transferência de dados, incluindo a Convenção de Budapeste (CETS 185 – CONSELHO DA EUROPA, 2001).

---

**32** Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002D0002&from=en>. *(esse link pode não funcionar corretamente em alguns leitores – nesse caso, acesse através de um celular ou computador)*. Acesso em: 14 out.2020.

---