O IMPACTO DA REGULAÇÃO GERAL DE PROTEÇÃO DE DADOS DA UE EM EMPRESAS BRASILEIRAS

BAPTISTA LUZ
ADVOGADOS

/ O IMPACTO DA REGULAÇÃO GERAL DE PROTEÇÃO DE DADOS DA UE EM EMPRESA BRASILEIRA

Eficácia extraterritorial e transferência internacional de dados

Renato Leite Monteiro

O presente estudo visa analisar possíveis impactos na aplicação da nova Regulação Europeia a partir de 2018 para empresas brasileiras. A ideia é abordar os principais impactos (as alterações) e entender o que é aplicável de acordo com o nível de interação entre as empresas brasileiras e europeias. Dentre os pontos que foram abordados, foi incluído se aplicabilidade/impacto é igual para os dados de titulares europeus armazenados/tratados no Brasil.

Entretanto, antes de adentrar nas novas obrigações impostas aos responsáveis pelo processamento de dados pessoais, discorreremos sobre o escopo de aplicação da Regulação, as condições que permitem a transferência internacional de dados, a sua eficácia extraterritorial e como Autoridade de Proteção de Dados Pessoais podem fazer valer a Regulamentação a empresas que não se localizam na União Europeia, para verificar se esta se aplica a empresas brasileiras.

Um ponto crucial deve ser primeiramente destacado: **a GDPR se aplica a coleta de dados pessoais de pessoas naturais que se encontram na União Europeia, independente da sua nacionalidade, cidadania, domicílio ou residência.**

Adicionalmente, em suma, será verificado com este estudo, que, caso uma empresa brasileira, de uma forma ou de outra, colete, processe ou receba dados pessoais de pessoais naturais localizadas na União Europeia, independente da sua nacionalidade, incluindo dados de consumidores, colaboradores, dados financeiros, ou ofereça serviços para algum dos 28 países do bloco europeu, poderá estar sujeita a jurisdição prescrita pela norma, dando ensejo ao dever de conformidade com esta (*compliance*), o que poderá ter um impacto nas suas operações e custos de transação.

Ademais, além das multas previstas na GDPR, mesmo que a empresa brasileira não se encaixe, diretamente, nos elementos e/ou pontos de contato que ensejam a aplicação da nova regulamentação, caso esta preste serviços de tratamento de dados para empresas, como coleta, armazenamento, enriquecimento, *profiling*, seja ela contratada ou subcontratada por empresas que estão sujeitas à GDPR, estas somente podem contratar com empresas que também estejam em conformidade. Esta nova obrigação legal pode, eventualmente, ser causa para rescisão justificada de contratos, sem direito a

multas contratuais e cláusulas penais, caso tal premissa não esteja prevista nos acordos.

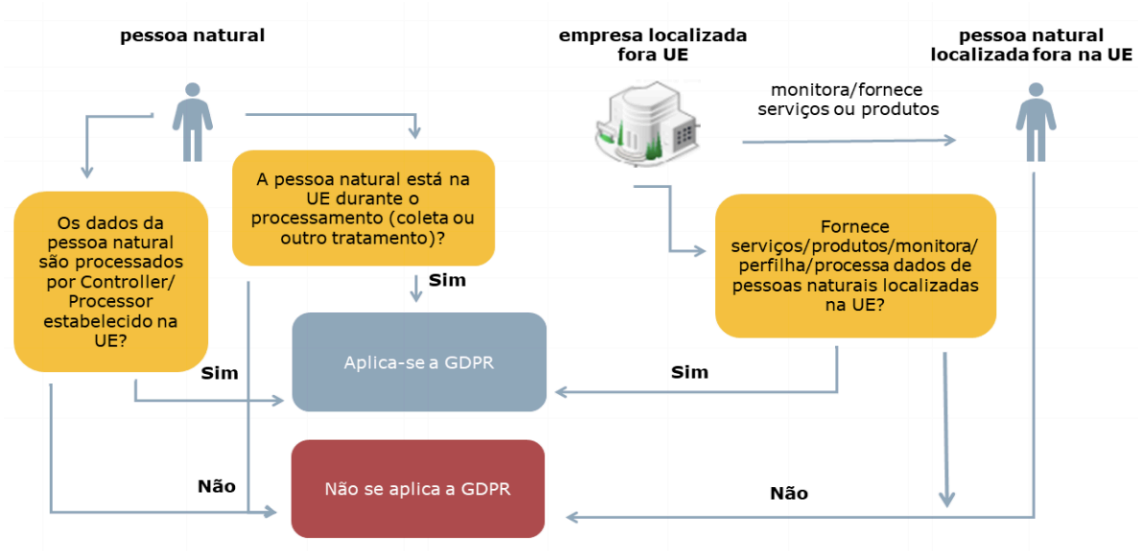
/ SUMÁRIO EXECUTIVO – APLICAÇÃO EXTRATERRITORIAL

- / aplicação extraterritorial que alcança empresas brasileiras com filiais na União Europeia ou que ofertem serviços ao mercado europeu
- / Aplica-se: empresa com filial ou representação na União Europeia ("EU")
- / Aplica-se: empresa, mesmo sem presença física na EU, mas que oferece serviços ao mercado europeu
- / Aplica-se: empresa, mesmo sem presença física na EU, que coleta dados de pessoas naturais localizadas na EU, independente da nacionalidade.
- / Aplica-se: empresa, mesmo sem presença física na EU, que monitora pessoas naturais localizadas na EU, independente da nacionalidade.
- / Aplica-se: empresa, mesmo sem presença física na EU, que terceiriza o processamento de dados para empresas localizadas na EU

Fornecedores (data processors): obrigação de conformidade -> causa para rescisão de contratos

Multas de até €20 milhões ou 4% do faturamento global

/ GRÁFICO – APLICAÇÃO EXTRATERRITORIAL



/ O QUE É A GENERAL DATA PROTECTION REGULATION – GDPR

A Regulação Geral de Proteção de Dados (*General Data Protection Regulation* – GDPR) (Regulação (EU) 2016/679[1]) ("Regulação") é uma Regulação adotada pela União Europeia em abril de 2016 para substituir a Diretiva

[1] http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

95/46/EC ("Diretiva"), conhecida como Diretiva Europeia de Proteção de Dados Pessoais. O objetivo principal da regulação foi atualizar, modernizar e harmonizar as arcabouço legal de proteção de dados pessoais na União Europeia ("EU"), conferindo aos indivíduos um controle maior sobre seus dados, ao mesmo tempo que fomenta o desenvolvimento econômico, tecnológico e a inovação. A Regulação[2] recebeu uma *vacatio legis* de 24 meses e entrará em vigor em 25 de maio de 2018, efetivamente substituindo a antiga Diretiva. A Regulação terá um efeito global, uma vez que ela se aplica a entidades que processam dados pessoais, mesmo quando o tratamento se dá fora da limitação geográfica da União Europeia, desde que sejam oferecidos bens ou serviços a titulares de dados que se encontram em algum país do bloco europeu ou caso monitore o comportamento de titulares de dados localizados na União Europeia.

/ CONCEITO DE DADO PESSOAL E TRATAMENTO DE DADOS

O escopo de aplicação de normas que versam sobre proteção de dados pessoais está intrinsicamente ligado ao o que pode ser considerado dado pessoal. A Regulação adota, em seu Art. 4, um conceito expansionista[3], que vai além do dado que efetivamente identifica uma pessoa natural, para incluir, também, o conceito de identificável, desde que os passos que levem a identificação por meio de combinação/agregação/cruzamento não sejam desproporcionais. Desta forma, para a Regulação, dado pessoal é:

> *"qualquer informação relacionada a uma pessoa natural identificada ou identificável. Uma pessoa natural identificável é alguém que pode ser identificada, direta ou indiretamente, principalmente por meio de referência a um identificador único como nome, número de identificação, dado locacional, identificador eletrônico ou um ou mais fatores específicos a identidade física, psicológica, genética, mental, econômica, cultural ou social da pessoa natural"*[4]

A Regulação adota, também, para fins de *profiling*, um conceito consequencialista[5] de dados que pode, eventualmente, determinar que dados

[2] Regulação, diferente das Diretivas, tem aplicação imediata em todos os membros da União Europeia, sendo desnecessária a sua internalização por meio de uma norma nacional. Desta forma, as regras estabelecidas na Regulação, com algumas exceções, são uniformes para todos os 28 países membros.
[3] BIONI, Bruno. Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. Grupo de Estudos em Políticas Públicas em Acesso à Informação da USP – GPOPAI.
[4] Art. 4 (1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; (tradução literal)
[5] Op. Cit. 3.

que não estejam estritamente dentro do conceito de dado pessoal previsto no Art. 4 possam estar cobertos para fins de aplicação da norma, como dados anonimizados ou pseudoanonimizados[6].

Ainda, para determinar quais práticas estão sujeitas às regras estabelecidas pela Regulação, necessário ter em mente o que esta conceitua como processamento, que de acordo com seu texto significa:

> *"Qualquer operação ou conjunto de operações as quais são realizadas em um dado pessoal ou em conjuntos de dados pessoais, por meios automatizados ou não, tais como catalogação, gravação, organização, estruturação, armazenamento, adaptação ou alteração, coleta, consulta, uso, revelação por meio de transmissão, disseminação ou qualquer forma que torne disponível, alinhamento, combinação, restrição, apagamento ou destruição"[7].*

Em suma, desde que esteja sob sua jurisdição, a Regulação sujeita qualquer prática de processamento de dados pessoais às suas regras, limites, obrigações e confere aos titulares dos dados uma série de direitos, muitos deles não previstos na Diretiva de 1995.

/ TRANSFERÊNCIA INTERNACIONAL DE DADOS

A Regulação permite a transferência de dados pessoais para países terceiros, fora do bloco europeu, por meio de uma série de condições, desde que este seja considerado pela Comissão Europeia um país com um nível "adequado" de proteção de dados pessoais, o que não é o caso do Brasil[8]. O art. 45[9] estabelece as condições para transferências internacionais baseadas em decisões de adequação, que consideram o país com um nível adequado de proteção. O considerando 104[10] especifica que decisões de adequação são

[6] Opinion 05/2014 on Opinion 05/2014 on Anonymisation Techniques of the Article 29 Working Party. Disponível em: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[7] Art. 4 (2): 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

[8] Na América do Sul, apenas Argentina e Uruguai receberam o selo de nível de adequação.

[9] Art. 45 (1): "A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorization".

[10] Considerando 10 -: Criteria for an adequacy decision: In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country

conferidas a países com níveis de proteção similar ao garantido na União Europeia.

Entretanto, na ausência de uma decisão da Comissão considerando o país adequado, transferências também são permitidas para países fora da União Europeia em algumas circunstâncias[11], tais como o uso de cláusulas contratuais padrão - cláusulas genéricas previamente aprovadas pela Comissão Europeia antes de serem introduzidas nos contratos que versam sobre transferências internacionais -, ou "*Binding Corporate Rules*" ("BCR")[12], aprovadas pelas autoridades nacionais de proteção de dados pessoais para casos particulares, como para uma empresa ou um conglomerado econômico específico[13]. Em ambas as situações, o processo é considerado severamente burocrático, principalmente pelo fato de retirar a simples autonomia das partes para estabelecer os padrões de proteção, uma vez que a intervenção estatal no que será decidido é obrigatória.

---

should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress."

[11] Art. 46 (1)(2): In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules in accordance with Article 47;
- standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
- standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
- an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

[12] Art. 47 (1): "The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

- are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;
- expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and fulfil the requirements laid down in paragraph 2.

[13] Considerando 110 - Binding corporate rules: A group of undertakings, or a group of enterprises engaged in a joint economic activity, should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same group of undertakings, or group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

Ademais, a Regulação inova ao introduzir, no seu art. 42[14], a possibilidade de autorizar transferência para países terceiros por meio de selos, certificações, desde que instrumentos jurídicos vinculativos e aplicáveis sejam acordados com o responsável pelo processamento de dados visando garantir proteções apropriadas.

/ TRANSFERÊNCIAS INTERNACIONAIS BASEADAS EM INSTRUMENTOS JURÍDICOS

A Regulação também enumera outros instrumentos que autorizam a transferência internacional de dados[15], desde que o processamento dos dados pessoais já seja baseado em uma hipótese legítima de tratamento, como consentimento expresso ou dever legal. Quais são:

- O titular dos dados expressamente consentiu com a transferência internacional dos seus dados, depois de ter sido informado dos possíveis riscos de tal transferência devido à ausência de uma decisão de adequação e proteções apropriadas[16].

Importante enaltecer que com relação à transferência internacional de dados, a Regulação requer "consentimento expresso" no lugar de "consentimento inequívoco". De acordo com a Regulação, o consentimento inequívoco permite que o titular dos dados informar o seu desejo em autorizar o processamento dos seus dados por meio de uma declaração ou uma ação afirmativa, como um comportamento[17]. O consentimento expresso requer que o titular dos dados "responda ativamente a uma pergunta, oralmente ou por escrito", como definido pelo *Article 29 Working Party*[18].

---

[14] Art. 42 (1)(2): Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects".

[15] Art. 49 (1).

[16] Art. 49(1)(a): "the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards";

[17] Article 4(11)

[18] Opinion 15/2011 on the definition of consent of the Article 29 Working Party: "respond actively to the question, orally or in writing". Disponível em: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

De acordo com o Art. 13[19] da Regulação, responsáveis pelo processamento devem fornecer determinadas informações para os titulares dos dados quando da obtenção do consentimento expresso, o que inclui:

- Que o responsável pretende transferir os seus dados pessoais para um terceiro país fora da União Europeia;
- Que essa transferência se dará para um país que obteve uma decisão de adequação de um nível de proteção de dados pessoais; ou
- Referência às proteções adequadas ou apropriadas para garantir seus direitos e como obtê-las.
- Essas informações devem ser fornecidas numa forma concisa, transparente, inteligível e de fácil acesso, por meio de uma linguagem simples e clara, de acordo com o Art. 12[20].

Outras possibilidades de transferência internacional são quando:

- A transferência é necessária para a execução de um contrato entre o responsável pelo tratamento e o titular dos dados, ou para a implementação de medidas pré-contratuais requisitadas pelo titular dos dados[21];
- A transferência é necessária para a conclusão ou execução de um contrato concluído no interesse do titular dos dados, mas celebrado

[19] Art. 13(1): Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the data protection officer, where applicable;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
- the recipients or categories of recipients of the personal data, if any;
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

[20] Art. 12 (1): "The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means".

[21] Art. 49(1)(b): "the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request";

entre o responsável pelo processamento dos dados e uma terceira pessoa, natural ou jurídica[22];

- A transferência é necessária por razões de interesse público subjacente[23].

Uma grande inovação da Regulação foi introduzir a possibilidade de transferências internacionais para países terceiros ou organizações baseadas nos legítimos interesses do responsável pelo processamento dos dados no caso de inexistência das hipóteses acima, incluindo decisões de adequação, cláusulas padrão ou BCRs. Esse tipo de transferência é possível desde que esta:

> *"não seja repetitiva, se limite somente a um número limitado de titulares de dados, e seja necessária para os importantes interesses legítimos do responsável pelo processamento de dados, e não se sobreponha aos interesses, direitos e liberdades do titular dos dados, e o responsável pelo processamento tenha endereçado todas as circunstâncias relacionadas à transferência dos dados para fornecer proteção adequadas aos dados pessoais"[24].*

A hipótese de transferência internacional baseada em interesses legítimos é similar à hipótese autorizativa de processamento de dados para outros fins, após o efetivo teste de proporcionalidade[25], mas limitada à um pequeno grupo de titulares, e somente para poucas ocasiões.

/ EFICÁCIA EXTRATERRITORIAL

Quanto a eficácia extraterritorial da Regulamentação, antes de qualquer análise pormenorizada, é necessário afirmar que ela não leva, em nenhum momento, para fins de determinação de jurisdição ou de onde e quando a norma será aplicada, a nacionalidade das pessoais naturais titulares dos dados pessoais. **Em outras palavras, a GDPR não se aplica, somente, a**

[22] Art. 49(1)(c): "the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person";
[23] Art. 49 (1)(d): "the transfer is necessary for important reasons of public interest;
[24] Art. 49(1)(parágrafo único): "not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data."
[25] Considerando 47: "The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller".

cidadãos europeus. A nacionalidade não é um elemento que deve ser levado em consideração.

Para corroborar esse entendimento, recentemente o Conselho Europeu publicou[26] uma correção ao texto do Art. 3(2) do Regulamento, pois a tradução deste do inglês (língua original) para outras línguas levou a algumas dúvidas interpretativas que davam margem a entender que a GDPR se aplicaria apenas a dados de pessoais residentes na EU (ainda assim não havia menção à nacionalidade ou cidadania). O conceito "who are" (em inglês) foi erroneamente traduzido para "residente" (português), que é um conceito jurídico, mas o legislador queria se referir a pessoas naturais que "se encontram" em território pertencente a algum dos 28 países membros da EU. Segue comparativo:

Texto original	Texto corrigido
Onde se lê: "2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares **residentes** no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com:"	**Leia-se:** "2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares **que se encontrem** no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com:".

Desta forma, **a GDPR se aplica a coleta de dados pessoais de pessoas naturais que se encontram na União Europeia, independente da sua nacionalidade, cidadania, domicílio ou residência.**

Dando continuidade, os pontos de contato abaixo são balizas elementares para se verificar se a GDPR de aplica à empresa, independente destas se localizaram fisicamente na União Europeia. Segue um breve resumo destes:

- Aplicação extraterritorial alcança empresas brasileiras com filiais na União Europeia ou que ofertem serviços ao mercado europeu;
- Aplica-se: empresa com filial ou representação na União Europeia ("EU");
- Aplica-se: empresa, mesmo sem presença física na EU, mas que oferece serviços ao mercado europeu;

[26] Publicação do Conselho Europeu com as correções em diversas línguas, inclusive Português: http://data.consilium.europa.eu/doc/document/ST-8088-2018-INIT/en/pdf

- Aplica-se: empresa, mesmo sem presença física na EU, que coleta dados de pessoas naturais localizadas na EU, independente da nacionalidade;
- Aplica-se: empresa, mesmo sem presença física na EU, que monitora pessoas naturais localizadas na EU, independente da nacionalidade;
- Aplica-se: empresa, mesmo sem presença física na EU, que terceiriza o processamento de dados para empresas localizadas na EU.

A Regulação inova em relação à Diretiva e aumenta drasticamente os limites da sua jurisdição para incluir, também, responsáveis pelo tratamento que se encontram geograficamente fora da União Europeia. Desta forma, a Regulação deve ser aplicada quando:

- O responsável pelo processamento está geograficamente localizado em membro da União Europeia e tem um estabelecimento principal, independentemente deste ser a matriz ou uma filial, ou da forma jurídica. **A nacionalidade dos titulares dos dados é irrelevante.** Neste caso, o Responsável estará sujeito apenas a supervisão da uma autoridade de proteção de dados pessoais do local do estabelecimento principal[27].

- Se o Responsável pelo processamento de dados está geograficamente localizado fora da União Europeia e oferece serviços ou produtos para residentes na União Europeia ou monitora o comportamento de residentes na União Europeia[28]. Neste cenário, o responsável não só estará sob a jurisdição da Regulação, mas também estará sujeito à supervisão de todas as autoridades de proteção de dados pessoais dos países para os quais oferece os seus serviços ou produtos ou monitora o comportamento de seus residentes.

Todavia, a Regulação não deixa claro o que seria oferecer serviços ou produtos, ou monitorar o comportamento, apenas que deve existir a intenção em oferecer os serviços para aquele(s) país(es) membro(s). Para determinar a intenção, a linguagem utilizada e a moeda de transação podem ser levadas em consideração. Com relação ao monitoramento, este independe de uma relação comercial ou pagamento, e pode ir além de *online tracking*, mas os tipos de práticas e tecnologias ainda serão alvo de discussão[29].

[27] Art. 3(1): "This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not".

[28] Art. 3(2): "This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
- the monitoring of their behaviour as far as their behaviour takes place within the Union.

[29] Considerando 24 - Applicable to processors not established in the Union if data subjects within the Union are profiled: "The processing of personal data of data subjects who are in the Union by a controller or processor not

Outro ponto que Regulação não deixa claro para determinar a sua jurisdição é o conceito de titulares de dados que se encontram na União Europeia, independente da nacionalidade, uma vez que esta não define se seriam apenas pessoas que residem nos países membros ou também àquelas que ali estão presentes, mas não residem efetivamente. A melhor doutrina tem entendido que a mera localização física, mesmo que temporária, de uma pessoa natural, independente da sua nacionalidade, em qualquer um dos 28 países da União Europeia, ou locais do mundo que estejam sob sua jurisdição, daria ensejo a aplicação extraterritorial[30].

Como apontado acima, responsáveis pelo processamento de dados que se encontram foram da União Europeia não podem se valer do conceito de *one-stop-shop*, qual seja, responder a autoridade de proteção de dados de apenas um país, mesmo que processe dados em referência a outros países membros. Neste cenário, o Responsável estará sujeito às autoridades de todos os países e deve indicar um representante perante as autoridades de cada um, o que pode aumentar os custos operacionais.

As autoridades nacionais podem tomar medidas contra os representantes localizados em seus territórios, não contra os responsáveis pelo processamento se estes se encontram em países terceiros. Mas estas podem ordenar, por exemplo, que operadores de infraestrutura de comunicação, como empresas de telefonia, bloqueiem o acesso aos serviços oferecidos pelo responsável. Em ambas situações existe um risco de dano reputacional muito grande, o que pode influenciar a decisão em cooperar com as autoridades.

/ ENFORCEMENT – APLICAÇÃO DE MULTAS E RESCISÃO CONTRATUAL

Se devido aos pontos de contato acima descritos a empresa estiver sob a égide da Regulação, tendo, portanto, que estar em conformidade, caso decida por não se adequar, as penalidades podem variar entre 20 milhões de Euros

established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes".

[30] MADGES, Robert. GDPR's global scope: the long story. Disponível em: https://medium.com/mydata/does-the-gdpr-apply-in-the-us-c670702faf7f

ou 4% do faturamento global da empresa ou do grupo econômico, o que for maior[31].

Todavia, caso a empresa não esteja efetivamente localizada na União Europeia, não tenha indicado nenhum representante perante as autoridades[32], ou nomeado um Data Protection Officer (DPO)[33], qualquer Autoridade de Proteção de Dados nacional de qualquer um dos 28 países membros da União Europeia pode ter dificuldades para realizar o *enforcement* das suas penalidades, sendo, eventualmente, necessário se valer de instrumentos de cooperação internacional para tanto, o que pode ser, por vezes, extremamente lento e burocrático.

Todavia, a Regulamentação determina expressamente que o Responsável só pode contratar com Operadores que estejam em conformidade com a GDPR[34]. Desta forma, o Responsável pode, eventualmente, devido a nova obrigação legal em vigor a partir do dia 25 de maio de 2018, ter que rescindir seus contratos de processamento ou terceirização de qualquer tipo de tratamento de dados pessoais, como armazenamento, enriquecimento, matching, consulta, *profiling*, com empresas que não estejam em conformidade com a GDPR, inclusive se estas estiverem no Brasil. Esta causa de rescisão pode, até mesmo, ser considerada justificada, sem qualquer direito a multa ou indenização, caso esse cenário não esteja previsto no contrato, por ser

---

[31] Art. 83(5). Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
(b) the data subjects' rights pursuant to Articles 12 to 22;
(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
(d) any obligations pursuant to Member State law adopted under Chapter IX;
(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

Art. 83 (6). Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

[32] Art. 27(1). Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

[33] Art. 37(1) The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.

[34] Art. 28(1) : Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

medida de lei a qual o Responsável está obrigado. Desta forma, os Operadores que estiverem em conformidade terão um oceano azul[35], pois os Responsáveis somente poderão contratar com eles, limitando a atividade de toda uma miríade de concorrentes. Em outras palavras, estar em conformidade com a GDPR pode ser considerada um diferencial competitivo.

/ CONCLUSÃO

Com base no exposto acima, **qualquer empresa brasileira poderá estar sujeita à jurisdição prescrita pela Regulação caso colete dados pessoais de pessoas naturais, físicas, localizadas na União Europeia, ou ofereça seus serviços e produtos diretamente para o mercado de membros da União Europeia, e caso trate dados de pessoas naturais localizadas no bloco econômico**. Caso seja este o caso, recomendamos um estudo mais profundo sobre as regras, limites e obrigações impostas pela norma, em face do dever de conformidade.

Ademais, o Brasil não é considerado pela Comissão Europeia como um país com um nível adequado de proteção de dados. Desta forma, a transferência de dados pessoais de titulares localizados na União Europeia, de forma direta ou indireta, somente poderá acontecer com base em uma das hipóteses autorizativas. Por questões operacionais e burocráticas, recomenda-se o uso cláusulas contratuais em que o titular localizado em um dos estados membros expressamente autoriza, de acordo com as regras informativas acima descritas, a transferência dos seus dados pessoais para o Brasil ou país onde a empresa vier a processar tais dados, como, por exemplo, por meio de serviços de *outsourcing* e *cloud computing.*

[35] É um conceito de negócios, apresentado em um livro de mesmo nome, que diz que a melhor forma de superar a concorrência é parar de tentar superá-la. Ou seja, buscar mercados ainda não explorados, chamados pelos autores do conceito de "oceano azul". KIM, W. Chan. A Estratégia do Oceano Azul.