I CONGRESSO DE TECNOLOGIAS APLICADAS AO DIREITO

TECNOLOGIA, EMPRESA E TRIBUTAÇÃO

T255
Tecnologia, empresa e tributação [Recurso eletrônico on-line] organização I Congresso de Tecnologias Aplicadas ao Direito – Belo Horizonte;

Coordenadores: Pedro Eliezer Maia, Pilar de Souza e Paula Coutinho Elói e Fernando Lage Tolentino – Belo Horizonte, 2017.

Inclui bibliografia
ISBN: 978-85-5505-664-2
Modo de acesso: www.conpedi.org.br em publicações
Tema: O problema do acesso à justiça e a tecnologia no século XXI

1. Direito. 2. Tecnologia. 3. Empresa. 4. Tributação. I. I Congresso de Tecnologias Aplicadas ao Direito (1:2018 : Belo Horizonte, BH).

CDU: 34

I CONGRESSO DE TECNOLOGIAS APLICADAS AO DIREITO

TECNOLOGIA, EMPRESA E TRIBUTAÇÃO

Apresentação

É com imensa satisfação que apresentamos os trabalhos científicos incluídos nesta publicação, que foram apresentados durante o I Congresso de Tecnologias Aplicadas ao Direito nos dias 14 e 15 de junho de 2018. As atividades ocorreram nas dependências da Escola Superior Dom Helder Câmara, em Belo Horizonte-MG, e tiveram inspiração no tema geral "O problema do acesso à justiça e a tecnologia no século XXI".

O evento foi uma realização do Programa RECAJ-UFMG – Solução de Conflitos e Acesso à Justiça da Faculdade de Direito da UFMG em parceria com o Direito Integral da Escola Superior Dom Helder Câmara. Foram apoiadores: o Conselho Nacional de Pesquisa e Pós-graduação em Direito - CONPEDI, EMGE – Escola de Engenharia, a Escola Judicial do Tribunal Regional do Trabalho da 3ª Região, a Federação Nacional dos Pós-graduandos em Direito – FEPODI e o Projeto Startup Dom.

A apresentação dos trabalhos abriu caminho para uma importante discussão, em que os pesquisadores do Direito, oriundos de dez Estados diferentes da Federação, puderam interagir em torno de questões teóricas e práticas, levando-se em consideração a temática central do grupo. Foram debatidos os desafios que as linhas de pesquisa enfrentam no tocante ao estudo do Direito e sua relação com a tecnologia nas mais diversas searas jurídicas.

Na coletânea que agora vem a público, encontram-se os resultados de pesquisas desenvolvidas em diversos Programas de Pós-graduação em Direito, nos níveis de Mestrado e Doutorado, e, principalmente, pesquisas oriundas dos programas de iniciação científica, isto é, trabalhos realizados por graduandos em Direito e seus orientadores. Os trabalhos foram rigorosamente selecionados, por meio de dupla avaliação cega por pares no sistema eletrônico desenvolvido pelo CONPEDI. Desta forma, estão inseridos no universo das 350 (trezentas e cinquenta) pesquisas do evento ora publicadas, que guardam sintonia direta com este Grupo de Trabalho.

Agradecemos a todos os pesquisadores pela sua inestimável colaboração e desejamos uma ótima e proveitosa leitura!

O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS E A ATUAÇÃO DAS EMPRESAS BRASILEIRAS

THE GENERAL DATA PROTECTION REGULATION AND THE BRAZILIAN COMPANIES PERFORMANCE

Juliana Falci Sousa Rocha Cunha

Resumo

O desenvolvimento tecnológica promove mudanças na sociedade, na legislação e nas empresas. Neste contexto, verificamos que a violação de dados pessoais tem sido cada vez maior, exigindo alterações legislativas, como a promovida pela União Europeia através do Regulamento (UE) 2016/679 (Regulamento Geral de Proteção de Dados). Desta feita, é essencial que as empresas estejam atentas aos novos desafios e atuem de acordo com as legislações pertinentes. Especialmente com relação ao referido Regulamento, notamos que empresas estrangeiras são afetadas, como as brasileiras, sendo necessárias adaptações, como o desenvolvimento de pessoal, a atualização documento e o acompanhamento regular de conformidade.

Palavras-chave: Proteção de dados, União europeia, Brasil, Legislação, Empresa

Abstract/Resumen/Résumé

The technological development encourages changes in the society, in the legislation and in the companies. For example, personal data breach has been increasing, making necessary legislation changes, such as the one promoted by the European Union through Regulation (EU) 2016/679 (General Data Protection Regulation). Thus, the companies should be alerted to new challenges and act according to the relevant legislation. With the European Regulation some foreign companies are affected, such as Brazilian ones, and adjustments are necessary, like personnel development, document updating and compliance regular monitoring.

Keywords/Palabras-claves/Mots-clés: Data protection, European union, Brazil, Legislation, Company

1. Introdução

Os dados pessoais são as informações relacionadas à pessoa natural identificada ou que possa ser identificada direta ou indiretamente. Exemplos de dados pessoais são o nome, as fotos, os e-mails, os números de identificação (Carteira de Identidade, CPF etc), os dados bancários, as informações médicas e os dados de localização.

As novas tecnologias como a Inteligência Artificial, o Big Data e a Internet das Coisas impactam diretamente a sociedade. Contudo, muitas pessoas não têm consciência de que as suas informações disponibilizadas na rede mundial de computadores (por exemplo, em sites de comércio eletrônico e redes sociais) e tratadas por terceiros podem tanto alterar o desempenho do mercado em geral quanto causar danos aos titulares dos dados.

Assim sendo, frente ao crescente e constante desenvolvimento da tecnologia e à necessidade de maior proteção de dados[1], desde 25 de maio de 2018[2] é aplicável o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, conhecido como Regulamento Geral de Proteção de Dados – RGPD, relativo à proteção de dados pessoais e à sua livre circulação. A referida regulamentação revogada a Diretiva 95/46/CE de 24 de outubro de 1995[3] (item 1 do art. 94) e objetiva não somente harmonizar as leis existentes nos Estados-Membros, mas também aumentar as restrições sobre as empresas que tratam os dados pessoais, além de possibilitar aos cidadãos mais controle sobre os mesmos. Desta forma, espera-se um ganho significativo em termos de segurança e privacidade dos dados pessoais.

O RGPD é um avanço no que se refere à proteção de dados e acarreta um maior investimento das empresas em planejamento, processos, tecnologia e capital humano. Deste modo, as empresas devem estar preparadas para atuar conforme o Regulamento e continuamente acompanhar toda a organização no que se refere à tutela da proteção de dados.

O objetivo deste breve artigo é abordar questões relevantes do RGPD no que se refere às empresas, focando na sua aplicação extraterritorial, em especial no Brasil. Assim sendo, para a elaboração do trabalho a metodologia utilizada foi a pesquisa bibliográfica e documental quanto ao procedimento e exploratória quanto

---

Artigo submetido ao I Congresso de Tecnologias Aplicadas ao Direito, promovido pela Universidade Federal de Minas Gerais e

[1] Segundo PEYROU (2015, p. 213-214), "La protection des données à caractère personnel apparaît comme une préoccupation récente, née avec le développements de l'Internet et les infinies possibilités de stockage offertes par des machines sur lesquelles semble s'exercer de moins en moins de contrôle qu'elles soient dans un insaisissable "nuage", voire dissimulées, comme "l'affaire Snowden" l'a révélé. (…)"

[2] Um mês antes da entrada em vigor da legislação em comento, a CYBERSECURITY INSIDERS (2018) divulgou o relatório "2018 GDPR Compliance Report", o qual apresenta o resultado de um estudo sobre a perspectiva das empresas com relação ao impacto do novo Regulamento e como se planejar para atuar de acordo com a nova lei. Do resultado de tal destacamos: a) "A whopping 60% of organizations are at risk of missing the GDPR deadline. Only 7% of surveyed organizations say they are in full compliance with GDPR requirements today, and 33% state they are well on their way to compliance deadline."; b) "The primary compliance challenges are lack of expert staff (43%), closely followed by lack of budget (40%), and a limited understanding of GDPR regulations (31%). A majority of 56% expect their organization's data governance budget to increase to deal with GDPR challenges."

[3] Sob a égide da antiga legislação europeia os Estados-Membros deveriam realizar a transposição da Diretiva para o ordem jurídica interna. Portugal, por exemplo, decretou a Lei 67/98, de 26 de outubro de 1998.

Já o RGPD possui a vantagem de ser automaticamente aplicável em todos os Estados-Membros, não sendo necessário que ele seja transposto em legislação interna. Contudo, os referidos países podem legislar quanto à tópicos específicos.

ao objetivo, incluindo artigos científicos, doutrina, relatórios públicos, legislação e conversas informais com profissionais que trabalham em empresas diretamente com o tema proposto.

2. Brasil: legislação e autoridade de proteção de dados

Especialmente com relação à proteção de dados no âmbito da América do Sul e Central, verificamos que o tema precisa de maior desenvolvimento por parte da legislação e da jurisprudência de alguns Estados. Contudo, devido à influência da União Europeia é importante destacar que alguns países já haviam adotado o direito à proteção de dados pessoais em suas legislações nacionais antes da aplicabilidade do RGPD, tais como, Chile[4], Argentina[5], Uruguai[6], Colômbia[7] e México[8]. Especialmente com relação à Argentina e ao Uruguai, a Comissão Europeia reconhece-os como Estados que asseguram um nível adequando de proteção de dados.

Já o Brasil não possui legislação específica que trata da proteção de dados, apesar de se encontrarem em andamento na Câmara dos Deputados, o Projeto de Lei 4.060/2012 (ao qual foi apensado o Projeto de Lei 5.276/2016[9], ao qual anteriormente havia sido apensado o Projeto de Lei 6.291/2016) e no Senado Federal o Projeto de Lei 330/2013, que tramita em conjunto com os Projetos de Lei 131/2014 e 181/2014.

---

[4] No Chile, existe a Lei 19.628, de 28 de agosto de 1999 que trata da proteção da vida privada e dos dados pessoais. Contudo, muitas pessoas consideravam a referida legislação inadequada, tendo protegido excessivamente os interesses daqueles que processavam dados pessoais. Esta legislação foi proposta em 5 de janeiro de 1993, tendo como fundamento a legislação comparada (como, Espanha e França). Após tantos anos, notou-se a necessidade de atualização da legislação sobre o tema, tendo sido propostos alguns Projetos de Lei, os quais ainda não foram aprovados. Finalmente, em 2017 o Poder Executivo enviou ao Senado um Projeto de Lei visando elevar a proteção de dados à níveis internacionais em matéria de tratamento de dados, além de adequá-la à economia digital, o qual encontra-se em tramitação.

[5] Na Argentina o artigo 43 da Constituição apresenta disposição relativa à proteção de dados pessoais. Além disso, existe uma legislação específica que trata sobre o tema, qual seja, a Lei 25.326, de 4 outubro de 2000. Com relação à União Europeia é importante destacar que conforme a Decisão 2003/490/EC de 30 de junho de 2003 da Comissão, a Argentina é considerada um país que possui nível "adequado" de proteção dados pessoais (de acordo com a legislação vigente na data da referida Decisão, qual seja a Diretiva 95/46/EC), sendo que o Grupo de Trabalho ARTIGO 29 (2002) já havia se posicionado no mesmo sentido no Parecer 4/2002, de 03 de outubro de 2002.

[6] No Uruguai existe legislação de proteção de dados, qual seja, a Lei 18.133 de 11 de agosto de 2008 (o art. 1 reconhece o direito à proteção de dados como direito humano, nos termos do art. 72 da Constituição da República), norma que foi regulamentada pelo Decreto 414/009 de 31 de agosto de 2009. Com relação à União Europeia é importante destacar que conforme a Decisão de Execução 2012/484/EU de 21 de agosto de 2012 da Comissão, o Uruguai é considerado um país que possui nível "adequado" de proteção dados pessoais (de acordo com a legislação vigente na data da referida Decisão, qual seja a Diretiva 95/46/EC), sendo que o Grupo de Trabalho ARTIGO 29 (2010) já havia se posicionado no mesmo sentido no Parecer 6/2010, de 12 de outubro de 2010. Ademais, cabe destacar que o Uruguai dispõe de Autoridade de Proteção de Dados, a qual é denominada "Unidad Reguladora y de Control de Datos Personales".

[7] Na Colômbia o artigo 15 da Constituição aborda os direitos fundamentais, como o direito à intimidade e à proteção de dados. A Lei 1.266, de 31 de dezembro de 2008 dispõe sobre a coleta, uso e transferência de dados pessoais, em especial relacionados às empresas das áreas financeira, de crédito, comercial e de serviços. Além disso, existe a Lei 1.581, de 17 de outubro de 2012, que apresenta disposições gerais sobre a proteção de dados pessoais e o Decreto 1.377, de 27 de junho de 2013 que regulamenta parcialmente a Lei 1.581/2012 tratando, por exemplo, da coleta de dados pessoais, da autorização para tratamento de dados pessoais sensíveis, de políticas de tratamento de informação e transferências internacionais de dados pessoais.

[8] No México o direito à proteção de dados é protegido como direito fundamental pela Constituição, em especial pelo §2º do art. 16. Além disto, também existe lei federal que trata do tema ("Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados", de 13 de dezembro de 2016), bem como que se refere aos dados em posse de terceiros ("Lei Federal de Protección de Datos Personales en Posesión de Particulares", de 5 de julho de 2010). Esta lei (dados pessoais em posse de particulares) objetiva garantir a privacidade e o direito à autodeterminação informativa das pessoais privadas, admitidas exceções conforme o art. 2. Ademais, tal legislação apresenta os Princípios de Proteção de Dados Pessoais e dispõe sobre os requisitos que as empresas devem cumprir no que tange ao processamento de dados.

[9] De acordo com BARBOSA e VILHENA (2016), o texto do referido Projeto de Lei foi elaborado pelo Ministério da Justiça no ano de 2011, tendo sido submetido à consulta pública cujas sugestões foram incorporadas ao texto.

Muitos especialistas estimam que a lei brasileira sobre o tema somente será aprovada a partir de 2019 devido às próximas eleições, apesar dos debates sobre o tema já terem ocorrido nas Casas Legislativas. Contudo, tal legislação é de grande relevância para o país, posto que diversos Estados já a possuem e têm exigido do Brasil maior segurança e proteção de dados, o que pode impactar significativamente na atividade empresarial nacional e na atração de investimentos externos.

Neste contexto, alguns estudiosos do tema discutem a possibilidade de adoção de uma Medida Provisória, visando garantir uma ambiente nacional mais seguro em termos de proteção de dados, visto que a Comissão Europeia não considera o Brasil como um país com um nível adequado de proteção de dados, o que foi agravado com a adoção do RGPD.

Entretanto, é importante lembrar que o Brasil possui leis que, direta ou indiretamente, trazem disposições relacionadas à proteção de dados, como a Constituição Federal[10], o Marco Civil da Internet (Lei 12.965 de 23 de abril de 2014)[11] e o Código de Defesa do Consumidor (Lei 8.078 de 11 de setembro de 1990)[12]. Contudo, tais legislações não têm se mostrado suficientes frente às novas legislações internacionais e ao crescente desenvolvimento tecnológico.[13]

O Brasil também não dispõe de uma autoridade responsável por centralizar questões relacionadas ao tema. Desta forma, alguns órgãos têm buscado tratar da questão, como a Secretaria Nacional do Consumidor – SENACON (que faz parte do Ministério da Justiça), o Ministério Público Federal, os Ministérios Públicos Estaduais, os Programas de Proteção e Defesa do Consumidor – PROCONs (vinculados aos Ministérios Públicos Estaduais) e entidades de defesa do consumidor. Contudo, verificamos que os esforços muitas vezes são duplicados, além de existirem diversas lacunas e omissões, o que poderia ser suprido pela adoção de uma Autoridade Nacional de Proteção de Dados.[14]

Desta forma, é importante que o Poder Legislativo atue ativamente no sentido de discutir e aprovar uma legislação de proteção de dados e é essencial que as empresas brasileiras que ainda não se atentaram para a relevância do tema se informem e estejam preparadas para atuar de acordo com a recente legislação

---

[10] No que tange à Constituição Federal destacamos os incisos X ("são violáveis a intimidade e a vida privada (…)" e XII ("é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas (…)") do art. 5.

[11] Especialmente com relação ao Marco Civil da Internet é importante observarmos o inciso III do art. 3 (proteção dos dados pessoais como princípio do suo da Internet no país), os incisos II, VII, VIII e IX do art. 7 e o art. 8.

Já quanto às regras relacionadas à proteção de dados apontamos: a) consentimento: incisos VII e IX do art. 7 e inciso I do art. 16; b) transparência: incisos VI, VIII e XI do art. 7 (também deve-se considerar o inciso I do art. 16 do Código de Defesa do Consumidor - CDC); c) proteção contra a discriminação: inciso III do art. 4 (além do inciso II do art. 6 do CDC); d) comunicação em casos de vazamento: inciso XIII do art. 7 (que deve ser interpretado conjuntamente com o §1º do art. 10 do CDC); e) respeito ao contexto da coleta: inciso VIII do art. 7.

É importante recordar que o Decreto 8.771/16 de 11 de Março de 2016 regulamentou a dita legislação e apresenta alguns conceitos relevantes à mesma, tais como, dado pessoal e tratamento de dados, como se verifica nos incisos I e II do art. 14.

[12] No caso do Código de Defesa do Consumidor destacamos o art. 43 que se refere às informações e dados pessoais e de consumo existentes em cadastros, fichas e registros aos quais o consumidor terá direito a acessar.

[13] Verificamos que a jurisprudência também tem utilizado outras legislações quando se trata do tema em análise, tais como, a Lei Geral de Telecomunicações (Lei 9.472 de 16 de julho de 1997), a Lei do Cadastro Positivo (Lei 12.414 de 9 de junho de 2011) e a Lei de Acesso à Informação (Lei 12.527 de 18 de novembro de 2011).

[14] Foi criada a Comissão de Proteção de Dados Pessoais, de iniciativa do Procurador-Geral de Justiça do Distrito Federal e Territórios que a instituiu no âmbito do Ministério Público do Distrito Federal e Territórios – MPDFT, a qual é dedicada exclusivamente ao tema proteção de dados pessoais e privacidade, conforme disposto na Portaria Normativa 512 de 20 de novembro de 2017 da Procuradoria-Geral de Justiça do MPDFT. Segundo tal Portaria, algumas das atribuições conferidas à referida Comissão são: " (...) I – promover e incentivar a proteção dos dados pessoais, nos termos da legislação; II – sugerir diretrizes para uma Política Nacional de Proteção dos Dados Pessoais e Privacidade; III – promover entre a população, empresas e órgãos públicos o conhecimento das normas e das políticas públicas sobre proteção de dados, bem como medidas de segurança;; (...)".

europeia, sob pena de ficarem isoladas do mercado global que está cada vez mais cauteloso no que se refere à tal tema.[15]

3. O Regulamento Geral de Proteção de Dados[16] e o Brasil

O RGPD tem aplicação extraterritorial, ou seja, fora do território da União Europeia. Sendo assim, ao estabelecimento do responsável pelo tratamento (ou o subcontratante) que se situa fora da UE está sujeito ao RGPD sempre que os titulares dos dados se encontrem na União Europeia e o tratamento esteja relacionado com oferta de produtos/serviços aos residentes na UE ou controle de comportamento de residentes na União Europeia.

Caso a nova legislação não seja observada, a empresa poderá ser penalizada com multas pesadas (até 4% do faturamento anual da empresa ou € 20 milhões – art. 83), o que pode impactar significativamente nas atividades empresariais e até mesmo eventualmente levar ao encerramento de suas atividades.

Com isto, algumas empresas brasileiras têm procurado orientação junto à consultorias jurídicas especializadas para se adequarem à nova realidade, visando minimizar os riscos de violação do RGPD. Entretanto, são poucas as empresas brasileiras que adotaram medidas efetivas visando se adequar à nova legislação europeia, especialmente no que se refere as pequenas e médias empresas.

Algumas das mudanças previstas no RGPD e que podem impactar diretamente as empresas brasileiras são: a) obrigatoriedade de notificação no prazo máximo de 72 horas à autoridade de controle e ao titular dos dados pessoais em caso de violação que possa resultar em elevado risco para os direitos e liberdades da pessoa natural (Considerando 85 e n. 1 do art. 33); b) direito do titular dos dados pessoais de obter do responsável pelo tratamento o apagamento dos seus dados pessoais em circunstâncias determinadas, como quando eles forem ilicitamente tratados (com exceção dos dados pessoais relacionados as obrigações legais e fiscais) (art. 17); c) conservação de registro de todas as atividades de tratamento de dados pessoais (como os dados coletados e a finalidade de uso) (n. 1 do art. 30); d) obtenção do consentimento do titular para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas (letra a do n. 1 do art.6); e) realização de avaliação de impacto das operações de tratamento, visando anular ou mitigar riscos de violação de dados pessoais, por exemplo, no caso do tratamento ser susceptível de resultar num elevado risco para os direitos e liberdades dos titulares dos dados pessoais (art. 35); f) adoção do "Privacy by Design": desde a

[15] A iniciativa brasileira de proteção de dados pessoais é uma preocupação não somente da esfera federal, mas também de alguns estados e municípios. Por exemplo, na Câmara Municipal de São Paulo foi proposto em 21 de Novembro de 2017 o Projeto de Lei 807/2017 de autoria de alguns vereadores, entre eles, Patrícia Bezerra (PSDB), José Police Neto (PSD e Eduardo Matarazzo Suplicy (PT), o qual tratada da "(...) política municipal de proteção de dados pessoais e da privacidade no âmbito da Administração Pública direta e indireta no Município de São Paulo (...)". A iniciativa de tal Projeto de Lei é de organizações da sociedade civil (por exemplo, Coletivo Intervozes e Rede Nossa São Paulo) e da Rede Latino-Americana de Estudos sobre Vigilância Tecnologia e Sociedade – LAVITS (que anteriormente havia desenvolvido uma proposta base).

[16] No que se refere ao Direito da Internet, incluído o tema de proteção de dados, o ideal seria a implantação de uma legislação de escopo mundial, contudo, não estamos caminhamos neste sentido, mas sim no de criação de leis nacionais (e até mesmo estatais) e quiçá regionais. Entretanto, existem iniciativas relevantes por parte das Organizações das Nações Unidas – ONU e da União Europeia no sentido de proteção de direitos humanos, incluído no ambiente virtual, como é o caso da Declaração Universal dos Direitos Humanos da ONU e do já referido Regulamento Geral de Proteção de Dados da União Europeia.

concepção os produtos, serviços, processos e sistemas devem cumprir os princípios de proteção de dados (Considerando 78); g) obrigatoriedade de designação de Encarregado de Proteção de Dados ("Data Protection Officer") em situações determinadas, como no caso de entidades que controlam regularmente dados pessoais em grande escala (art. 37).

4. Compliance das empresas brasileiras[17] com relação à proteção de dados[18]

No atual ambiente de negócios notamos a crescente necessidade de proteger e melhor gerenciar os dados pessoais. Com isso, o compliance[19], a gestão de risco[20] e a governança[21] têm cada vez mais sua importância acrescida no tema em questão.

Mesmo não havendo legislação específica de proteção de dados no Brasil, nada impede que sejam adotadas práticas de auto-regulação[22], como regras setoriais, Códigos de Conduta (art. 40 e letra m do §1º do art. 57 do RGPD)[23], "Binding Corporate Rules" (n. 20 do art. 4 e art. 47)[24], cláusulas contratuais (n. 8 do art. 28, letra d do n. 2 do art. 46 e letra j do §1º do art. 57 do RGPD) e Certificação (art. 42 e letra n do §1º do art. 57 do RGPD)[25].

De qualquer forma, para que as empresas brasileiras atuem de acordo com o RGPD é importante que elas realizem, por exemplo: a) mapeamento do ambiente da dados[26] da organização, envolvendo o grau de

[17] As empresas sujeitas ao novo Regulamento europeu são aquelas que manipulam e tratam dados pessoais envolvendo consumidores, empregados e acionistas cidadãos da União Europeia ou de outras nacionalidades, mas que residem na região ou que os dados estejam armazenados na UE ou que possua fluxo internacional de dados com empresas que realize negócios na região.

[18] No novo contexto de regulação da proteção de dados observa-se a necessidade de desenvolvimento de mão de obra especializada para atuação em empresas brasileiras e estrangeiras. Tal fato pode ser confirmado por diversas pesquisas realizadas à nível mundial, dentre elas a realizada pela CYBERSECURITY INSIDERS (2018), que divulgou no relatório "2018 GDPR Compliance Report" que 43% das empresas afirmam que faltam empregados especialistas com as habilidades necessárias para atuarem diretamente com proteção de dados.

[19] O compliance na área de proteção de dados auxilia a empresa a manter a sua atividade e consequentemente a recolha e tratamento dos dados pessoais dentro do previsto na legislação, nas normas internas e em contratos.

[20] É o conjunto de estratégias que visam identificar, avaliar, prevenir, mensurar, tratar e monitorar as respostas aos riscos de um projeto, ativo, setor, departamento, organização etc. Risco, por sua vez, é a possibilidade de um evento negativo influenciar na realização de um ou mais objetivos.

[21] A Governança de Dados e Informações, permite, por exemplo, que os dados e as informações estejam disponíveis aos empregados, parceiros, fornecedores, acionistas, "stakeholders" etc que realmente deles necessitam, possibilitando a sua gestão mais eficiente, a redução de acessos indevidos, o tratamento mais assertivo e a correta divulgação de dados e informações.

[22] Auto-regulação para CRAIG (2013, p. 219) é "the process by which an identifiable group of people or industry governs or directs their own activities by their own rules."

[23] Para ASBROECK e DEBUSSCHE (2017, p. 91) os Códigos de Conduta são "(…) une sorte de mécanisme de "semi-autorégulation" et peuvent être proposés par des associations ou des organes représentatifs dans le contexte d'activités de traitement de données. Ces codes pourraient fournir des indications utiles dans des domaines essentiels, tels la "pseudonymisation" ou la mise en oeuvre appropriée des nouveaux principes de "privacy-by-design" et de "privacy-by-default" (…)."

[24] De acordo com a DIREÇÃO GERAL DE JUSTIÇA E CONSUMIDOR DA COMISSÃO EUROPEIA (2018, p. 2) "binding corporate rules" (ou regras vinculativas aplicáveis às empresas) são "legally binding data protection rules approved by the competent data protection authority which apply within a corporate group".

[25] Para ASBROECK e DEBUSSCHE (2017, p. 91), com relação à Europa, "(…) les certifications, labels et marques sont quant à eux des mécanismes volontaires visant à démontrer le respect des règles de protection des données ou à indiquer que des importateurs de données situés en dehors de l'espace économique européen ("EEE") ont mis en oeuvre des garanties adéquates à des fins de transfert de données. (…)"

[26] Tal mapeamento deve envolver as bases de dados estruturadas ou não, quem os detém (área e responsável), os tratamentos das bases de dados e quem os realiza, o fluxo dos dados (em especial aqueles que apresentam maior risco), quem compartilha os dados, os sistemas que processam os dados, onde ele está localizado/armazenado e os documentos legais relacionados à coleta de dados e/ou consentimento.
Para realizar tal mapeamento podem ser realizadas entrevistas, coleta de documentos e até mesmo questionários junto às áreas de Negócios (Comercial, Marketing e Financeiro), Informática (como, TI e Segurança da Informação), Jurídico, Compliance e Operacional.

conformidade e riscos de descumprimento com as regulamentações de proteção de dados; b) capacitação (inicial, bem como de sensibilização rotineira) dos profissionais da empresa; c) implantação do Plano de Ação, baseado no referido mapeamento; d) atualização da documentação empresarial (Termos de Uso, Políticas de Privacidade, Política de Segurança da Informação, Códigos Internos – ex. Código de Ética e Contratos) e procedimentos; e) acompanhamento regular do cumprimento de tais normas visando a conformidade e a melhoria contínua.[27]

Finalmente, é importante destacar que as empresas brasileiras não estabelecidas na União Europeia que realizam o tratamento de dados pessoais de titulares residentes na UE deverão manter um representante em tal localidade (n. 2 do art. 3; designado por escrito, nos termos do n. 1 do art. 27 do RGPD), o qual será considerado como interlocutor entre a empresa contratante e a Autoridade de Controle, os titulares dos dados e demais pessoas pertinentes, no que tange a questões relacionadas ao tratamento de dados pessoais (n. 4 do art. 27 do RGPD).

5. Conclusão

Na sociedade atual verificamos a digitalização de dados/informações com a consequente armazenagem em base de dados por diferentes entes privados e públicos, os quais realizam tratamento de dados. Desta forma, verificamos que cada vez mais os dados pessoais têm se tornado mais valiosos para o mercado[28]. Frente à este contexto, a União Europeia aprimorou a sua legislação de proteção de dados, tendo outros países adotado leis específicas, o que entretanto não foi feito no Brasil. Frente à isto, é essencial que este país rediscuta os mecanismos jurídicos da tutela relacionados à proteção de dados.

Além disso, as empresas devem estar atentas no que se refere à proteção de dados frente aos novos desafios que se impõe, por exemplo, através do RGPD. Esta legislação, por exemplo, provocou um avanço significativo no tratamento de dados, mas requer mudança de postura por parte das organizações, sob pena de serem inviabilizados muitos negócios.

Mesmo que o Brasil não tenha legislação específica sobre o tema, as empresas devem estar atentas às disposições relativas em legislações esparsas, por exemplo, da Constituição Federal, do Código de Defesa do Consumidor e do Marco Civil da Internet. Ademais, é essencial que o Poder Legislativo dê andamento aos Projetos de Lei sobre proteção de dados que tramitam no Congresso Nacional, visando assim manter o país competitivo em termos internacionais, possibilitando a atração de novos clientes, o fornecimento produtos e serviços para o exterior e captação de investimentos internacionais.

A partir deste mapeamento é possível elaborar um Diagnóstico de Riscos e um Plano de Ação para mitigá-los, o qual deve envolver o "Privacy Impact Assessment" e análise de "gaps".

[27] Segundo ASBROECK e DEBUSSCHE (2017, p. 90-91), para que as empresas, inclusive as brasileiras, estejam preparadas para o cumprimento do RGPD é necessário que elas regularmente, por exemplo: "(…) (i) évaluer leur conformité actuelle à la législation en matière de vie privée; (ii) identifier les lacunes ("gap analysis") entre la conformité avec le système actuel et ce qui doit changer afin d'assurer la conformité au RGPD; (iii) prioriser les mesures correctives qui s'imposent; et (iv) mettre en oeuvre des mesures correctives fondées sur une hiérarchisation des risques."

[28] Para alguns estudiosos do tema os dados pessoais são o "novo petróleo".

Referência bibliográfica

ARTICLE 29 – Grupo de Trabalho de Proteção de Dados Pessoais. Opinion 4/2002 on the level of protection of personal data in Argentina, de 3 de outubro de 2002.

_____. Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay, de 12 de outubro de 2010.

ASBROECK, Benoit Van; DEBUSSCHE, Julien. Les obligations de "compliance" des enterprises. In: DOCQUIR, Benjamin (coordinateur). *Vers un droit européen de la protection des données?*. Bruxelles: Larcier, 2017, p. 90-133.

BARBOSA, Cláudio R.; VILHENA, Pedro. *Data protection in Brazil*: overview. Practical Law: Global Guide 2016/2017 (data protection).

BRASIL (Câmara dos Deputados). Projeto de Lei 4.060/2012, de 13 de junho de 2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências.

_____. Projeto de Lei 5.276/2016, de 13 de maio de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural.

_____. Projeto de Lei 6.291/2016, de 11 de Outubro de 2016. Altera o Marco Civil da Internet, no sentido de proibir o compartilhamento de dados pessoais dos assinantes de aplicações de internet.

BRASIL (Procuradoria-Geral de Justiça do Ministério Público do Distrito Federal e Territórios). Portaria Normativa 512, de 20 de novembro de 2017.

BRASIL (Senado Federal). Projeto de Lei 330/2013, de 13 de Agosto de 2013. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências.

_____. Projeto de Lei 131/2014, de 16 de abril de 2014. Dispõe sobre o fornecimento de dados de cidadãos ou empresas brasileiros a organismos estrangeiros.

_____. Projeto de Lei 181/2014, de 20 de Maio de 2014. Estabelece princípios, garantias, direitos e obrigações referentes à proteção de dados pessoais.

COMISSÃO EUROPEIA (Direção Geral de Justiça e Consumidor da Comissão Europeia). Notice to Stakeholders – Withdrawal of the United Kingdom from the Union and EU Rules in the field of data protection, de 9 de janeiro de 2018.

CYBERSECURITY INSIDERS. 2018 – GDPR Compliance Report, Abril de 2018.

PEYROU, Sylvie. La protection des données à caractère personnel: un droit désormais constitutionnalisé et garanti par la C.J.U.E. In: TINIÈRE, Romain; VIAL, Claire (direction). *La protection des droits fondamentaux dans l'Union européenne*: Entre évolution et permanence. Bruxelles: Lancier, 2015.

SÃO PAULO (Câmara Municipal). Projeto de Lei 807/2017. Dispõe sobre a Política Municipal de proteção de dados pessoais e da privacidade no âmbito da Administração Pública direta e indireta no Município de São Paulo e dá outras providências.

UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

_____. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

UNIÃO EUROPEIA (Comissão). Decisão 2003/490/EC, de 30 de junho de 2003, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais na Argentina.

_____. Decisão de Execução da Comissão de 21 de agosto de 2012. Decisão 2012/484/EU nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados.