
CYBERLAW
by CIJIC

CYBERLAW by CIJIC

EDIÇÃO N.º VI – SETEMBRO/OUTUBRO DE 2018

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

EDITOR: NUNO TEIXEIRA CASTRO

SUPORTE EDITORIAL: EUGÉNIO ALVES DA SILVA

PRESIDENTE DO CIJIC: EDUARDO VERA-CRUZ PINTO

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

CYBERLAW by CIJIC

NOTAS DO EDITOR:

No prólogo de mais esta nova edição da revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa, antecipo-me a aduzir dois actos, em breve, solenes, que não deverão passar em claro nas agendas de cada um.

O primeiro desses actos terá lugar no próximo 17 de Outubro na Universidade de Aveiro. Trata-se da Sétima edição da Iniciativa Portuguesa do Fórum da Governação da Internet.

Um sublinhado desde logo para o local do evento. É importante que a academia se sinta interligada com Portugal, no seu todo. Sair de Lisboa, do conforto centralizador da capital, é um pequeno mas mui nobre sinal de que há muito e bom trabalho a ser desenvolvido diariamente na plenitude dos mais de 98 mil quilómetros quadrados que compõem o nosso pequeno país.

No que à edição deste ano do Fórum da Governação da Internet diz respeito, trata-se de um evento organizado pela FCT (Fundação para a Ciência e a Tecnologia I.P), em parceria com a ANACOM (Autoridade Nacional de Comunicações), APDSI (Associação para a Promoção e Desenvolvimento da Sociedade da Informação), API (Associação Portuguesa de Imprensa), Associação DNS.PT, Ciência Viva (Agência Nacional para a Cultura Científica e Tecnológica), CNCS (Centro Nacional de Cibersegurança), IAPMEI (Agência para a Competitividade e Inovação), ISOC-PT

(Capítulo Português da ISOC), Polo TICE.PT, Secretaria Geral da Presidência do Conselho de Ministros, e Sociedade Civil.

Serão objecto de discussão, temas como «Governação e políticas públicas da Internet nos contextos nacional e global»; «Inteligência Artificial e *Big data*»; «Segurança no Ciberespaço: O dilema entre a privacidade do indivíduo e a segurança do Estado»; «Governação, confiança, privacidade e desafios na era do IoT»; «*Fake news, fake views* -Sociedade da (Des)Informação».

As sessões e respectivos painéis apresentam temas e oradores de reconhecida qualidade, e, seguramente, será um 17 de Outubro de 2018 muito e bem preenchido em Aveiro[1].

O outro evento, como seria natural, até pelo investimento feito pelo país na realização deste por mais dez anos em Portugal, é a *Lisboa web summit* 2018.

O programa e agenda[2] da feira, que se realizará no Altice Arena entre 5 e 8 de Novembro, já foram dados a conhecer. O destaque recai na presença de oradores como o Secretário-Geral das Nações Unidas, Sr. António Guterres; o inventor do *www*, Sir Tim Berners-Lee; o CEO do eBay, Mr. Devin Wenig; a Comissária Europeia para a Concorrência, Mrs. Margrethe Vestager; entre outros.

Os temas são vastos. A agenda *idem*. Uma semana desta feira para explorar avidamente.

Em suma, sendo eventos contrastantes na apresentação, na forma e até na finalidade, seria pouco cordial não aproveitar a proximidade destes para esta nota de agenda.

Arrolado o introito, focando-nos apenas no essencial desta nova edição, seguramente que a entrada em vigor, em pleno, do RGPD - *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*; bem como da Lei Geral de Protecção de Dados (LGPD) no Brasil, aprovada no plenário do

1 Informações sobre o programa do evento podem ser consultadas em: https://www.governacaointernet.pt/pdf/forum_programa_2018.pdf.
O evento é de entrada livre mas requer uma inscrição prévia. Mais informações em: https://www.governacaointernet.pt/2018.html
2 Mais informações em: https://websummit.com/schedule

Senado Federal pelo PLC 53/2018, a 10 de Julho; impuseram que o tema da protecção de dados pessoais fizesse, novamente, parte do cardápio da revista.

No plano nacional, a Proposta de Lei 120/XIII, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, continua em suave desenvolvimento[3], mais de dois anos após a publicação do Regulamento europeu, o RGPD.

Não obstante, procurando contrariar o *adagio* da Proposta de Lei 120/XIII, procuramos coligir doutrina e opinião que demonstrem um pouco do *vivace* de pessoas e organizações na adaptação às novas realidades supranacionais. Neste sentido, encontraremos *ways not to read* o RGPD; as principais dificuldades e dúvidas partilhadas por organizações e por pessoas singulares na adaptação à nova realidade jurídica europeia. *Curiosamente*, do outro lado do Atlântico, trazemos, ainda, o impacto da LGPD brasileira nos negócios e nas pessoas, neste novel quadro normativo de agregação temática. É, pela actualidade do tema, tempo, ainda, de reintegrar o conceito de desindexação, *in casu*, da desindexação de conteúdos ofensivos na net, recuperando críticas jurídicas ao relevante caso *Google Spain*.

Saltando da circunspecção dos dados pessoais e da privacidade para outro tema, serão apresentadas reflexões quanto à apreensão de correio eletrónico e registos de comunicação de natureza semelhante. O tema é fervilhante. Na actualidade, a vivência em sociedade cresce *digitalodependente*, convocando discussões doutrinárias profundas. Ainda não será desta que se pacificará, entre os intérpretes e aplicadores do direito, a distinção juridicamente relevante entre correio e correio eletrónico. Mas, as reflexões que aqui se publicam, valem a leitura e o crepitar de questões.

Colocada em perspectiva esta espécie de matrimónio, de conveniência, que o direito e a tecnologia assumiram, a problemática dos drones, inteligência artificial e robótica, também têm aqui palco no plano jurídico.

Direito e Tecnologia são meios essenciais ao desenvolvimento do homem, com implicações, dilacerantes, nas mais variadas formas em como revelamos o ser social que somos. A ética, juridicamente relevante, aliada à segurança - subjacente ao

3 Pode ser consultada a actividade relativa à Proposta de lei em: http://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=42368

conceito *Safe-by-design* (SbD) - estimulam dissecções imediatas desde o plano de concepção, no patamar R&D do desenvolvimento das mais diversas ferramentas, utensílios, *gadgets*, cada vez mais apetrechadas de inteligência artificial e robótica, que vão procurando satisfazer necessidades diversas do *mercado*, isto é, nossas.

Aproveitando a epígrafe, projecto uma questão, que gostava de ver discutida numa próxima edição da revista: será profícuo que ao invés da pirexia em torno da segurança - a qualquer custo - dos dispositivos, tentando antecipar toda a indeterminabilidade da vida humana – com todos os custos inerentes a esta tarefa de adivinhação – o foco poderia vir a incidir sobre a *responsabilidade pela segurança*? Assumindo-se a impossibilidade de segurança absoluta de toda e qualquer ferramenta, será que alvitraremos, no futuro, um modelo de responsabilidades partilhadas como solução?

A insolência típica das muitas questões não poderia terminar sem o regresso a uma ideia em processo de maturação: como conciliar diversas ordens, práticas e tradições jurídicas; actores, partes e contrapartes processuais; pessoas singulares, organizações e Estados, perante tal amálgama de situações quotidianas neste *pot-pourri* que a Internet é e do qual dependemos? Estaremos no vértice da necessidade de um Tribunal Internacional para a Internet? Mais umas penadas sobre a arquitetura de um desejável edifício de harmonização e resolução de pleitos jurídicos a nível mundial.

Resta-me, por fim, agradecer a todos pelo esforço e pelo trabalho, endereçando, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um sentido reconhecimento a cada um dos autores: Muito Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

Boas leituras.

Lisboa, FDUL, 05 de Outubro de 2018

Nuno Teixeira Castro

CYBERLAW

by CIJIC

OPINIÃO

CYBERLAW
by CIJIC

ANÁLISE BREVE DA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA (*LGPD*):

QUE IMPACTO TRAZ AOS NEGÓCIOS E ÀS PESSOAS?

VALÉRIA REANI RODRIGUES GARCIA [*]

[*] Advogada, OAB/SP, Brasil. Especialista em Direito e Privacidade de Dados pela UNL - Universidade Nova Lisboa; em Direito Digital e "*Compliance"* – Faculdade Damásio; e em Direito Empresarial – PUC-Campinas-Pontifica Universidade Católica de Campinas. Coordenadora Pedagógica Científica e Docente dos Cursos de Direito Digital e Inovação da ESA- Escola Superior de Advocacia de Santos, Santo André e Campinas.
Contacto: valeriareani@primoecampos.com.br

INTRODUÇÃO

No dia 10 de julho de 2018, foi aprovado no plenário do Senado Federal o PLC 53/2018, o qual dispõe sobre a proteção de dados pessoais e altera a Lei 12.965/16 (Marco Civil da Internet), consolidando-se assim como a Lei Geral de Proteção de Dados brasileira (LGPD) [†].

A lei cria um novo regramento para o uso de dados pessoais no Brasil, tanto no âmbito *online q*uanto *offline,* nos setores privados e públicos, de forma a reforçar e complementar, a Legislação setorial, que já tratava de privacidade, como a própria Constituição Federal, Código de defesa do Consumidor, Código Civil e Marco Civil da Internet do Brasil, que justamente

[†] Há mais 30 diplomas legais sobre o assunto – aí se inclui a própria Constituição Federal, o Marco Civil da Internet, Código de Defesa do Consumidor, Lei de Acesso à Informação, Lei do Cadastro Positivo, Código Civil. Na Constituição Federal logo em seu art. 1o, III, preceitua que um dos fundamentos do Estado Brasileiro é a dignidade da pessoa humana, para alguns doutrinadores, esse princípio é a guia para a tutela efetiva de todos os direitos fundamentais contidos na Carta Magna de 1988. Mais a frente, no mesmo diploma legal, em seu art. 5o, X, preceitua que "*são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação*", ficando evidente a proteção dos direitos da personalidade, que também ficam claros no art. 21 do Código Civil, ao preceituar que "*A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma*", protegendo a intimidade e a vida privada, possuindo grande ligação com a questão da proteção dos dados pessoais sob a ótica européia, consubstanciada no art. 8, no 1 da Carta dos Direitos Fundamentais da União Européia.
A lei 8.078/90, Código de Defesa do Consumidor, em seu art. 43, trata da questão do acesso por parte do consumidor aos dados pessoais que estejam arquivados – "*O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes*", mostrando uma preocupação do legislador com essa questão, sendo que o referido artigo do CDC possui forte ligação com o art. 5o LXXII, ao prever o remédio constitucional conhecido como *habeas data,* ao preceituar que*: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo*. O remédio constitucional do Habeas Data não se mostrou de grande efetividade e eficácia no ordenamento jurídico pátrio, sendo pouco utilizado, sendo questionado, por alguns doutrinadores sobre a sua real importância como tutela efetiva de proteção de dados pessoais. Mais recentemente ocorreu a entrada em vigor da Lei 12.965/ 14, o Marco Civil da Internet, que poderia ter resolvido, de certa forma, esse vácuo legislativo existente no Brasil, já que o arcabouço jurídico pátrio não possui norma efetiva que tutele a proteção de dados pessoais e seu tratamento, porém limitou-se a tratar de forma tímida em seu art. 11 a questão da proteção dos dados pessoais, deixando, ainda, um campo aberto para regulação. Lei de Acesso à Informação (LAI), Lei nº 12.527/2011, decorrente do art. 5º, XXXIII, art. 37, § 3º, II e o art. 216, § 2º, todos da CF/88, com o direito constitucional da privacidade. O primeiro possibilita o recebimento de informações públicas dos órgãos estatais e propicia maior liberdade de opinião e de expressão. Enquanto o segundo protege e assegura os direitos à privacidade e à intimidade que provêm da própria natureza humana e daí o seu caráter inviolável, intemporal e universal, impedindo a devassa nas informações de cunho estritamente pessoal.

por ser setorial, trazia insegurança jurídica e tornava o país menos competitivo no contexto econômico Global cada vez mais movido a dados.

I. QUAL O OBJETIVO DA LEI GERAL DE PROTEÇÃO DE DADOS?

A lei objetiva garantir ao cidadão:

Direito à privacidade: garantir o direito à privacidade e à proteção de dados pessoais dos cidadãos ao permitir um maior controle sobre seus dados, por meio de práticas transparentes e seguras, visando garantir direitos e liberdades fundamentais.

Regras claras para empresas: estabelecer regras claras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais para empresas.

Promover desenvolvimento: fomentar o desenvolvimento econômico e tecnológico numa sociedade movida a dados.

Direito do consumidor: garantir a livre iniciativa, a livre concorrência e a defesa do consumidor.

Fortalecer confiança: aumentar a confiança da sociedade na coleta e uso dos seus dados pessoais.

Segurança jurídica: aumentar a segurança jurídica como um todo no uso e tratamento de dados pessoais.

II. A IMPORTÂNCIA DE UMA LEI GERAL DE PROTEÇÃO DE DADOS:

Unificar regras: regras únicas e harmônicas sobre o uso de dados pessoais, independente do setor da economia.

Adequar as regras no Brasil: tornar o Brasil apto a processar dados oriundos de países que exigem um nível de proteção de dados adequados, o que pode fomentar, principalmente, os setores de tecnologia da informação.

Portabilidade: indivíduos poderão transferir seus dados de um serviço para outro, aumentando a competitividade no mercado.

III. A LGPD

A LGPD tem aplicação tanto no âmbito público e privado, *online* e *offline*. Ela versa sobre o conceito de dados pessoais;

- lista as bases legais que autorizam o seu uso a exemplo do consentimento, do titular dos dados pessoais, permitindo o uso de dados com base no legítimo interesse do controlador dos dados;
- Trata de princípios gerais, direitos básicos do titular – como acesso, exclusão dos dados e explicação sobre uso – obrigações e limites que devem ser aplicadas a toda entidade que se vale do uso de dados pessoais, seja como insumo do seu modelo de negócio, seja para a atividade de seus colaboradores.

IV. PRINCIPAIS PONTOS DA LEI GERAL DE PROTEÇÃO DE DADOS - LGPD

- Aplicação transversal, multissetorial, a todos os setores da economia, tanto no âmbito público quanto privado, *online* e *offline*. Trocando em mudos, e a poucas exceções, toda e qualquer prática que se valer do uso de dados pessoais estará sujeita à lei.

- Aplicação extraterritorial: em moldes similares à regulamentação europeia, a ***General Data Protection Regulation*** - **GDPR,** a Lei Geral, ou seja, o dever de conformidade superará os limites geográficos do país. Toda empresa estrangeira que, com filial no Brasil, ou oferecer serviços ao mercado nacional e coletar e tratar dados de pessoais naturais localizadas no país estará sujeita à nova lei.

- Traz conceito amplo do que deve ser considerado dado pessoal informação relacionada à pessoa natural/física, identificada ou identificável. Ou seja, qualquer dado, que isoladamente ou agregado a outro possa permitir a identificação de uma pessoa natural, ou sujeitá-la a um determinado comportamento.

- Define **dados pessoais sensíveis**, como aqueles que pela sua própria natureza podem sujeitar o seu titular a práticas discriminatórias, tais como dados sobre a origem racial ou étnica, a convicção religiosa, a opinião política, dado referente à saúde ou à vida sexual; ou permitir a sua identificação de forma inequívoca e persistente, tais como dado genético ou biométrico. Por sua peculiaridade tais dados devem ser tratados de forma diferenciada, segurança adicionais.

- Conceitua dados **anonimizados** que seriam os relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Dados efetivamente anonimizados são essenciais para o funcionamento de tecnologias e na da Internet das Coisas, inteligência artificial, ***machine learning, smart cities***.

- Fala também de dados públicos, tais como os constantes de bases geridas por órgãos públicos, publicações oficiais e cartórios, ou os expressamente tornados públicos pelos seus titulares, como em perfis públicos em redes, ficando o uso desses dados, limitado às finalidades.

V. PROTEÇÃO DOS DADOS PESSOAIS DE CRIANÇAS?

Sim. A Lei estabelece que um termo de privacidade deverá existir toda vez que forem solicitados dados pessoais, seja nas plataformas *online* ou em lojas físicas, clínicas de saúde, entre outros estabelecimentos, objetivando manter a integridade dos pequenos, como nome, endereço, escolaridade, entre outros, que só poderão ser usados pelas empresas após consentimento dos responsáveis dos menores de 12. Maiores de 12 anos poderão consentir, desde que entendam do que se trata aquele termo. Por isso, eles devem ter linguagem clara e acessível.

VI. A LGPD LISTA 10 PRINCÍPIOS/razões que devem ser levados em consideração no tratamento de dados pessoais, tais como:

1) **Finalidade**: propósito legítimo para uso dos dados pessoais;

2) **Adequação**: compatibilidade de tratamento com a finalidade;

3) **Necessidade**: Uso e tratamento dos dados deve ser restrito ao mínimo necessário;

4) **Livre acesso**: garantia de consulta facilitada e gratuita sobre a integralidade de dados, forma e duração do tratamento;

5) **Qualidade dos dado**s: garantia de exatidão, clareza, relevância e atualização dos dados de acordo com a finalidade de seu tratamento:

6) **Transparência:** garantia de informação precisa sobre o tratamento dados;

7) **Segurança:** utilização de medidas técnicas capazes de garantir a Segurança do tratamento;

8) **Prevenção:** adoção de medidas para prevenir a ocorrência de danos, em função do tratamento inadequado;

9) **Não discriminação**: impossibilidade de tratamento para fins discriminatórios, ilícitos e abusivos;

10) **A responsabilização e prestação de contas**, que obriga o responsável pelo tratamento dos dados pessoais a demonstrar de forma cabal e transparente a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais previstas na lei.

VII. QUAIS SÃO OS DIREITOS BÁSICOS DOS TITULARES DE DADOS:

Dentre os direitos listados, destaca-se o de acesso aos dados, retificação, cancelamento ou exclusão, oposição ao tratamento, de informação e explicação sobre o uso dos dados. A grande novidade é o direito à portabilidade dos dados que, similar ao GDPR, pode ser feito entre diferentes empresas de telefonia e bancos, permite ao titular não só requisitar uma cópia da integralidade dos seus dados que facilite a transferência destes para outros serviços, mesmo para concorrentes.

Devido a sua natureza, este novo direito tem sido encarado como um forte elemento de competição entre diferentes empresas que oferecem serviços similares baseados no uso de dados pessoais.

Responsabilidade dos agentes de tratamento: os diferentes agentes envolvidos no tratamento de dados – o controlador e o operador – podem ser solidariamente responsabilizados por incidentes de segurança da informação e/ou o uso indevido e não autorizado dos dados, ou

pela não conformidade com a lei. Ressalte-se que a LGPD, determina a nomeação de um *Data Protection Officer* (DPO), cuja tradução e " encarregado", responsável pelo tratamento de dados pessoais dentro da organização.

VIII. QUAL O IMPACTO NOS NEGÓCIOS E ATIVIDADES?

A LGDP não afeta somente os grandes *players* do setor de tecnologia e serviços *online*, como aqueles oferecidos pelo *Google* e *Facebook*, mas também qualquer organização que realize uma operação de coleta, uso, processamento e armazenamento de dados pessoais.

Exemplos de aplicação da lei:

- Tratamento de dados no âmbito de atividades de bancos, corretoras, seguradoras, clinicas médicas, hospitais, e-commerce, varejo, hotéis, companhias aéreas, agências de viagens, restaurantes, academias, entre muitas outras, podem estar sujeitas a aplicação da lei, ainda que tais atividades ocorram exclusivamente fora do ambiente digital.

- Tratamento de dados pessoais em relações de clientes e fornecedores de produtos e serviços, prestadores e tomadores de serviços, empregados e empregadores, e demais relações nas quais dados pessoais sejam recebidos, enviados e/ou processados.

IX. QUEM ESTÁ SUJEITO A LGPD? QUAIS REGRAS DEVEM SER OBSERVADAS PELAS EMPRESAS DO SETOR PÚBLICO E PRIVADO?

De modo geral, a LGPD estabelece regras detalhadas que regulam qualquer operação de tratamento de dados, realizada por pessoas físicas ou jurídicas, no setor público ou privado e estabelece uma série de obrigações:

- a definição e documentação da base legal que autoriza o tratamento de dados (que podem incluir, mas não se limitam, a definir se o tratamento é realizado com base no consentimento, para fins de cumprimento de obrigação legal, para a execução de contrato, ou com base no interesses legítimo);

- o atendimento aos direitos concedidos aos titulares de dados, como o direito de obter informações sobre o tratamento de dados, realizar o acesso, retificação e eliminação de dados, direito à portabilidade a outro fornecer de produtos e serviços e obter a revisão de decisões automatizadas, dentre outros;
- a nomeação de um ENCARREGADO ou *Data Protection Officer* (DPO), responsável pelo tratamento de dados pessoais dentro da organização;
- a notificação a autoridade competente, em caso de incidente (divulgação e/ou uso não autorizado de dados pessoais);
- a adoção de medidas de (organizacionais e técnicas para) proteção de dados, a partir da criação de qualquer nova tecnologia ou produto (*privacy by design*); e,
- adequação das hipóteses que autorizam a transferência de dados para fora do país, quando aplicável.

X. QUAIS INFORMAÇÕES SÃO CONSIDERADAS COMO DADOS PESSOAIS?

Dados pessoais podem compreender qualquer informação relacionada à uma pessoa natural, identificada ou identificável. Neste sentido, dados de pessoas jurídicas não são cobertos pela LGPD, mas somente informações relacionadas às pessoas físicas. Um segundo aspecto importante é relacionado ao fato de que dados pessoais podem consistir em qualquer informação de pessoas identificadas ou identificáveis. **Dados pessoais de indivíduos identificados são aquelas informações que imediatamente podem identificar uma pessoa, como o nome, número de CPF e RG e informações de documentos pessoais**. Por outro lado, dados pessoais de indivíduos identificáveis são aquelas informações que não podem imediatamente identificar um indivíduo, mas que, ao serem alocadas juntamente com outras, podem passar a identificar e serem relacionadas a um indivíduo.

A LGPD regula o tratamento de dados pessoais em relações de clientes e fornecedores de produtos e serviços, prestadores e tomadores de serviços, empregados e empregadores, e demais relações nas quais dados pessoais sejam recebidos, enviados e/ou processados.

XI. AS ATIVIDADES DE PROCESSAMENTO DE DADOS DENTRO E FORA DO PAÍS ESTÃO SUJEITAS A LEI?

Operações de tratamento de dados realizadas dentro do território brasileiro estão sujeitas a aplicação da LGDP. Além de operações de tratamento realizadas dentro do país, quando o tratamento tiver por objetivo a oferta ou fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território brasileiro, a lei também pode se aplicar, ainda que a organização responsável por essa atividade esteja sediada ou localizada fora do país. Assim, o local onde os dados são tratados não é requisito único ou preponderante para aplicação da lei, sendo também importante identificar a localização do indivíduo cujos dados serão coletados.

XII. QUEM NÃO ESTÁ SUJEITO A LEI?

O uso pessoal para fins particulares e não econômicos, para fins jornalísticos, artísticos ou acadêmicos, não estão dentro do escopo da lei e, portanto, aos requisitos de tratamento de dados. Da mesma forma, o tratamento de dados para fins de segurança pública, defesa nacional, segurança do estado e/ou atividades de investigação e repressão de infrações penais também não estão sujeitos a LGPD, e estão sujeitos a regulação de legislação específica no tema. Dados provenientes e destinados a outros países, que apenas transitem pelo território nacional, sem que aqui seja realizada qualquer operação de tratamento podem eventualmente não estar sujeitos a aplicação da lei.

XIII. QUAL O RISCO DO NÃO CUMPRIMENTO DA LEI?

As penalidades por descumprimento da LGPD incluem advertência, obrigação de divulgação do incidente, eliminação de dados pessoais, bloqueio, suspensão e/ou proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados pessoais, multa, chegando ao valor limite de R$ 50.000.000,00 (cinquenta milhões de reais) por infração.

Por fim, desde o último dia 14 de agosto o Brasil passou a ter não somente uma importante legislação específica que regulamenta o tratamento de dados pessoais, tanto pelo poder público quanto pela iniciativa privada que traz as novas regras criadas como meio de fortalecer a proteção da privacidade dos usuários, como também um grande desafio técnico, jurídico e cultural.

O “vacatio legis” é de 18 (dezoito) meses de sua publicação oficial, isto quer dizer que o interregno para a estruturação empresarial privado e público acontece nos próximos 18 meses, quando entrará em vigor a lei, mais precisamente, em fevereiro de 2020.

CONCLUSÃO

Assim, o Brasil conta com uma robusta legislação em termos de proteção de dados pessoais, o que possivelmente aprimorará o desenvolvimento tecnológico, práticas de negócios, crescimento do mercado digital e ao mesmo tempo proteção aos dados pessoais dos cidadãos em nosso país.

Outrossim, (logo que regularizada essa questão vetada) um cuidado que se deve ter, é com a Autoridade Nacional de Proteção de Dados (ANPD), responsável pela supervisão, fiscalização e a disseminação de boas práticas entre as empresas públicas e privadas, sob pena de ausência de confiança do mercado, priorize um engajamento construtivo com a indústria, no seguinte sentido de que ao invés de inquisição e sanção, dar prioridade ao diálogo, apoio, mutua cooperação, orientação, conscientização e informação; além de estimular relações abertas e construtivas com negócios que lidem com dados pessoais, primando pela boa-fé das empresas e nos seus esforços em cumprir a lei; bem como propiciar a criação de ambientes para inovações responsáveis, como *"Regulatory Sandboxes"*, nos quais novos projetos podem ser testados em atmosferas controladas visando avaliar eventuais e futuras necessidades regulatórias, conforme o caso, mas *a posteriori*.

Salienta-se que as empresas que demonstrem vanguarda na adequação da LGPD, em agir de forma responsável, sejam encorajadas a demonstrar seus programas de privacidade, segurança da informação, códigos de conduta e gerenciamento de risco, visando gerar o reconhecimento do mercado por suas boas práticas, incluindo certificações, entre outros padrões de "*accountability".*

As sanções devem ser a "*ultima ratio*", principalmente e somente quando houver alguma violação dolosa, ou práticas exponencialmente negligentes, condutas reiteradas ou extremamente graves.

Ter um órgão controlador de todo esse processo é ideal e essencial para que ele seja sempre gerenciado conforme a lei. No entanto, enquanto uma nova agência é criada pelo Executivo e enquanto as empresas estão em período de preparação e adaptação às novas mudanças, é possível ir tomando medidas de auditorias dentro das próprias empresas sobre seus dados atuais, além da possibilidade da contratação de um ENCARREGADO – já que, assim, o oficial de dados atribui a responsabilidade de processadores e controladores de informações à uma pessoa.

Embora esse trabalho seja difícil e, muitas vezes, complexo, o desafio das empresas de estar em conformidade com a lei é importante e pode se tornar uma vantagem competitiva mais para a frente. Por isso, é importante olharmos para os passos que devem ser feitos até que ela se concretize, pensando sempre na importância da análise e de uma auditoria que controle a empresa, evitando que esteja fora da regulamentação.

Finalmente, é com muita satisfação que vejo a aprovação da nossa LGPD, trazendo um equilíbrio entre interesses sociais e econômicos; entre o poder público e o privado; entre liberdade, proteção e segurança, buscando tutelar, ao mesmo tempo, a proteção de dados pessoais, a dignidade da pessoa humana, a privacidade, a honra e a imagem das pessoas, assim como a livre iniciativa e o uso econômico dos dados, de forma legítima, séria, responsável, proporcional e razoável.

Referência Bibliográfica

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 - Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm