XXI ENGEMA
Encontro Internacional sobre Gestão Empresarial e Meio Ambiente

ISSN: 2359-1048
Dezembro 2019

Novas Diretrizes empregadas na privacidade e proteção de dados dos cidadãos aplicados em modelos de inovação baseados na conectividade da Computação Corporativa, Big Data e Governança Cibernética

BEN-HUR MONTEIRO BARIZON
CEFET - CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA - RJ

JOSE CLAUDIO DA GAMA DIAS COSTA
UNIVERSIDADE FEDERAL FLUMINENSE (UFF)

Introdução

Com a evolução tecnológica que vivenciamos hoje, sobretudo das tecnologias de computação e o grande desenvolvimento das TICs(tecnologias de informação e comunicação) temos disponível uma gama enorme de produtos (bens e serviços), com diversos graus de qualidade, disponibilizados a quase todas as pessoas, em quase todo lugar e em qualquer momento, o que propicia condições que elevam o nível de qualidade de vida do cidadão e em geral da sociedade. Mas, ao mesmo tempo em que nos beneficiamos individualmente e coletivamente desses avanços tecnológicos ficamos cada vez mais expostos em nossa privacidade.

Com o intuito de se ofertar bens e serviços cada vez mais personalizados, as empresas privadas de todos os níveis e áreas de atuação, e também as instituições governamentais, coletam nossos dados pessoais, com os quais utilizam suas estratégias comerciais e industriais no intuito de direcionar seu foco naquele cliente a fim de individualizar produtos, bem como autenticar indivíduos e permitir acessos a redes de serviços digitais em nuvem, tais como plataformas de comércio eletrônico, plataformas de serviços públicos ofertados ao cidadão, redes sociais, etc.

O outro lado da moeda é exposição pessoal e a violação privada do indivíduo caso seus dados sejam acessados e usados de modo inadequado. Nesse sentido torna-se primordial a proteção dos dados pessoais aproveitando o avanço da tecnologia, o que vem fazendo com que governos se debrucem sobre as questões envolvendo a elaboração de políticas públicas (leis) que permitam o desenvolvimento tecnológico e econômico ao mesmo tempo em que protege os dados pessoais de seus cidadãos. A computação em nuvem, o Big Data e a governança tornam-se, assim, marcos da evolução tecnológica atual e da proteção de dados digitais pessoais.

A Computação em Nuvem (CN) é um das mais interessantes e produtivas formas de comunicação no sentido de utilizar novos modelos de armazenamento de informações onde pode-se utilizar o conceito de computação de maneira global e gerenciar os processos com perspectivas de economia, praticidade e eficácia, tornando a ideia de armazenamento de dados com um caráter de prestação de serviços funcional, de maneira que os recursos de computação envolvidos, principalmente na forma de processamento e armazenamento, podem ser consumidos e pagos pelo usuário de uma maneira que se torne mais adequada a sua própria conveniência, similar aos serviços básicos como fornecimento de energia elétrica, gás e telefonia.

O objetivo da computação em nuvem, segundo estudo produzido por Ramalho e Prado (2013) é oferecer serviços e produtos que possam ser disponibilizados, em tese, a qualquer pessoa e em qualquer lugar, somente precisando ter um acesso a internet e senha para conexão.

Pode-se utilizar desde acesso a programas básicos usados em computadores pessoais, materiais didáticos armazenados em ferramentas tipo Dropbox, até armazenamento de informações de grandes empresas em sistemas denominados Data Warehouse que trabalham como modelos de comércio eletrônico pela internet (e-commerce) como Amazon, Alibaba, Google, IBM, Microsoft, entre outras corporações de grande importância no mundo globalizado atual.

Para facilitar esses acessos aos servidores de computação em nuvem, utilizamos em alguns casos sua implementação por meio de redes de transmissão de dados baseadas na tecnologia de quarta geração de celulares (4G) num modelo denominado LTE (Long Term Evolution) que já está em operação no Brasil desde 2012, podendo executar tanto transmissão de dados, quanto transmissão de voz por meio de pacotes de dados com compressão denominados (VoIP), onde algumas operadoras de telecomunicações chamam este modelo de VoLTE (Voz sobre LTE).

Neste modelo de comunicação baseado na 4G-LTE temos diversas vertentes que são aplicadas dependendo da necessidade e da garantia de qualidade de acesso aos servidores de computação em nuvem. A principal vertente é a 4G/LTE (Long-Term-Evolution), que foi uma evolução da rede 3G (GSM/WCDMA), mas também existem outras como a LTE-Advanced, chamada de 4G+ ou a LTE – Advanced-Pro, chamada de 4,5G+. Essas vertentes apresentam melhorias perante o 4G/LTE como agregação de portadora, tecnologia MIMO e modulação 256QAM.

Para melhorar o acesso aos servidores e *Data warehouse*, principalmente para usuários e empresas que estão dentro de áreas metropolitanas e também em lugares mais distantes, as prestadoras de serviços de telecomunicações buscaram utilizar faixas de frequências no espectro de 700MHz, que antes ficava restrito às transmissões das TVs analógicas que começaram a ser desligadas pelas cidades no Brasil desde 2015, migrando para outra faixa na transmissão digital, onde poderiam operar sem os problemas de reflexão e distorção que atrapalhavam as transmissões analógicas.

A frequência de 700 MHz traz maior penetração de sinal, o que melhora a recepção em ambientes internos, além de possibilitar melhor uso da tecnologia VoLTE para fazer chamadas telefônicas. Por enquanto a maior parte da rede 4G no Brasil ainda está na faixa de 2,5GHz, que exige uma maior quantidade de antenas para sua propagação.

Para viabilizar estas características de ampliação das redes e transmissão de dados, segundo estudo da ANATEL e do site TELECO, em julho de 2018 a tecnologia 4G/LTE já dispunha de 120 mil terminais ativos, o que correspondia a mais de 50% do total.

No mundo globalizado que vivemos em constante mutação, a computação em nuvem adquire importância vital para todas as empresas que precisam movimentar seus ativos financeiros e competir para conquistar velhos e novos clientes.

Segundo estudo da consultoria Economática (2018), no mês de agosto deste ano a Apple superou 1 trilhão de dólares em valor de mercado, ficando à frente de Amazon, com U$ 877,4 Bi, Alphabet (Google), com U$ 854,7 Bi e Microsoft, com U$ 811,1 Bi. Todas estas empresas conseguiram superar em valor de mercado a soma de todas as 360 empresas brasileiras listadas na BOVESPA, o que indica a grande importância que a computação em nuvem configurou-se no mercado mundial e no mercado de E-commerce.

A grande mudança foi a valorização de todas as companhias que focam seu portfólio de produtos nas vendas virtuais no chamado E-commerce, e com isto conseguem ganhar espaço no mundo inteiro, muito mais do que as empresas que somente fazem seu planejamento estratégico em lojas com produtos vendidos fisicamente.

O grande paradigma para que este modelo de vendas virtuais possa ser aplicado em escala global é a necessidade das empresas em buscarem incessantemente os dados do usuário para conseguir oferecer as melhores ofertas instantaneamente e neste caso um dos grandes entraves e que este modelo pode causar problemas em relação a privacidade dos dados dos usuários. Este tema tem causado grandes controvérsias e muitos estudos no sentido de tentar proteger ao máximo o cidadão de empresas inescrupulosas que aparecem todos os dias no comércio eletrônico.

Para tentar regulamentar os métodos de acesso aos dados dos usuários foi criada uma lei nº 13.709 de 14 de agosto de 2018, denominada LPDP – Lei de Proteção dos dados pessoais que tenta buscar um diálogo entre preservação e o respeito dos direitos de liberdade e privacidade em contraponto com a evolução de uma sociedade que “respira” sistemas de informação desde o nascedouro de seus cidadãos e necessita de desenvolvimento econômico, tecnologia e principalmente criação de novos modelos e ferramentas que buscam constantemente a inovação.

Um dos grandes ofensores que são explorados neste modelo de exposição constante dos dados dos cidadãos é efetuar um controle bem delineado, mesmo com suporte da LDPD, na disseminação indiscriminada dos dados pessoais por toda uma cadeia de logística, culminando na transmissão destes

dados para empresas de todos os tipos que receberiam informações brutas sem a devida apuração e checagem de seu real valor.

Uma das aplicações envolvidas neste estudo, por exemplo, podem ser redes de financiamento imobiliário em conjunto com indústrias farmacêuticas, que podem acabar baseando sua análise de forma pontual, até no caso de liberação de um financiamento, iriam consultar um cadastro para saber a real consistência se o cidadão poderia ter renda para pagar alguma dívida contraída, além de que a disponibilidade indiscriminada dos dados pessoais poderia causar problemas na compra de algum remédio de grande vulto, na qual poderia ter a intensão de rejeitar algum financiamento na interpretação que a pessoa poderia estar com uma doença grave e com risco de vida. A empresa acabaria negando o empréstimo ou iria gerar um crescimento na taxa de juros, no entendimento errado que o cidadão não teria condições de arcar com a dívida contraída.

Não somente na área privada, o acesso às informações do cidadão sem alguma forma criteriosa pode gerar grades problemas pessoais, na área pública também ocorrem restrições de grande vulto. O grande diferencial na área pública em relação à LPDP é no sentido de seguir determinadas diretrizes em relação ao tratamento de dados pessoais no âmbito da administração Pública visando unicamente o processo de compartilhamento de dados necessários à execução de políticas públicas em diversas áreas como Fiscal (Tributação onde é necessário o compartilhamento para fins de arrecadação de impostos), Saúde (SUS – compartilhamento dos dados para os contribuintes e beneficiários que tem cadastros no SUS), entre outras áreas.

Este modelo em alguns momentos pode ter caráter ambíguo, pois pelas medidas previstas pela LPDP descreve que o consentimento deve ser fornecido por escrito e de forma destacada das demais cláusulas contratuais, onde busca obrigar as empresas a oferecer informações relevantes a seus consumidores, mas por outro lado pela necessidade eterna de proteção contra sanções penais pelo poder público e segurança jurídica, muitas empresas não oferecem de forma clara estas condições em muitos casos descrevendo regras intermináveis de dificultam o entendimento e a interpretação de determinadas condições, inibindo a capacidade do cliente de entender a real intenção daquilo que é o cerne daquela situação, o que acaba não se mostrando eficaz em produzir um modelo padrão para regulação contratual do tratamento de dados.

Em todo este universo de dados públicos ou privados, cada vez mais existe a necessidade de criação de mecanismos e processos que possam executar de forma efetiva e precisa uma análise deste universo imenso de dados no intuito de melhorar a estrutura e a forma de preservação da privacidade.

Um dos modelos criados para executar uma análise cada vez mais crescente dos dados de forma exponencial se denomina Big Data. Este termo descreve o

grande volume de dados tanto estruturados quanto não estruturados nos quais as empresas têm que lidar diariamente. Essas análises tem uma real importância em relação ao planejamento estratégico que vai ser implementação para que os gestores possam lidar com a quantidade de dados que serão analisados buscando obter uma diretriz mais objetiva no sentido de achar as melhores decisões e principalmente a melhor ação estratégia a ser implementada para criação de valor no negócio da empresa, a fim de se manter competitiva no mercado.

Essas análises devem ter como parâmetros 3 aspectos:

a) Volume, onde as empresas podem coletar dados de variadas fontes como por exemplo transações financeiras, pesquisas nas mídias sociais de seus clientes e, também dentro do modelo M2M (Máquina a Máquina) pela análise de informações dos dados transmitidos por meio de sensores que coletam as informações que trafegam nas redes.

b) Velocidade, onde se tenta buscar as informações de maneira muito rápida com dados praticamente navegando em velocidades de tempo real, onde pode-se utilizar determinadas tecnologia para esta captura como Etiquetas baseadas em RFID, Sensores eletrônico e medições inteligente dos dados.

c) Variedade, onde se busca analisar determinados dados que trafegam em múltiplos formatos, desde sua forma estruturada, onde tem-se uma representação numérica dentro de base de dados tradicionais, como em sua forma não estruturada, onde se busca encontrar e interpretar dados dentro de ferramentas diversas como: e-mail, áudio, vídeo, cotações listadas em bolsa de valores, documentos de texto e também listagens de listagens de transações financeiras.

De posse destas ferramentas consegue-se um mapeamento de informações nas mais diversas situações, como por exemplo, uma análise de compras e hábitos de consumo de determinado cliente e também numa área que provoca danos e grandes prejuízos para as empresas e clientes (segurança bancária e empresarial), onde procura-se diminuir o risco com fraudes que possam trazer problemas para os clientes das organizações, além de sanções penais que possam derivar de qualquer atitude ilícita cometida pelos hackers.

Para garantir que a quantidade imensurável de dados analisados neste mapeamento de informações instituídos na diretriz do Big Data possa efetivamente estar à disposição dos analistas de dados, necessitamos estar conectados a um novo modelo de proteção baseado na segurança cibernética.

Com o crescimento da globalização em caráter mundial tanto na parte econômica quanto nas partes política e tecnológica, as trocas de informações

se tornaram mais dinâmicas e cresceram de forma exponencial, tornando o acesso à informação um bem de uso pelo cidadão comum para melhorar sua qualidade de vida e aumentar seu conhecimento sobre diversos assuntos. Isto acabou potencializando o aparecimento de pessoas e empresas inescrupulosas utilizando-se de complexos algoritmos e programação, criando estratégias maléficas de obtenção de dados pessoais ou corporativos de forma ilícita, gerando novas formas de ataques digitais que também crescem exponencialmente, onde uma das atividades que se tornam mais comuns e tem caráter devastador para todos os cidadãos e empresas é a violação de dados.

Desta forma as empresas e principalmente as agências de governo estão constantemente sofrendo ataques virtuais cibernéticos, o que fez com que se tornasse prioridade dentre as políticas dos governos tentar de alguma maneira buscar rotinas de segurança e prevenção de seus dados e sistemas. Vários estudos confirmam que a grande maioria das instituições governamentais deverá ser alvo de hackers nos próximos 12 meses. Infelizmente um ponto desfavorável é que as agências do governo tem grande ineficiência em considerar e preservar a experiência e usabilidade do usuário final na implantação de tecnologias e políticas de segurança cibernética, em muitos casos pelo desrespeito de seu próprio usuário que não leva em consideração as medidas de segurança cibernética e acaba se tornando "uma porta de entrada" para que a agência se torne vulnerável a algum ataque que gere roubo e perda de dados importantes e sensíveis. Neste sentido as agências do governo têm procurado mecanismos para combater as ameaças à segurança da informação e a alternativa tem sido mudar a abordagem, que combina uma governança de cima para baixo e mecanismos de segurança de baixo para cima. Esses mecanismos estão totalmente integrados com o sistema de **Gestão da Informação Corporativa (EIM) – Enterprise Information Management**, sistema que busca considerar sua análise no usuário final, ou seja, no funcionário.

O sistema EIM é projetado para proteger as informações no local onde são acessadas, ou seja, no ponto de interação e no próprio aplicativo. O sistema adquire mecanismos de proteção como acesso e direitos de permissão, auditoria e intercâmbio de informações seguras. Tecnologias como o gerenciamento de registros e autoclassificação fornecem uma solução que elimina a necessidade dos usuários de ordenar e classificar o conteúdo, permitindo que as agências tenham maior controle e proteção em relação aos seus conteúdos. Ao automatizar a capacidade do sistema de identificar registros e aplicar classificações, as agências garantem que as informações estão seguras em todo o seu ciclo de vida.

As agências governamentais são desafiadas a proteger dados pessoas e respeitar a privacidade, permitindo ao mesmo tempo livre acesso à informação pública. De cima pra baixo, EIM oferece uma abordagem baseada no risco

para a segurança da informação e que garanta que os recursos, programas e processos estejam prontos para ajudar os governos a manter a confidencialidade, integridade e disponibilidade dos conteúdos.

O valor da informação não deve ser considerado fora do contexto de segurança digital. EIM é um componente-chave em meio às políticas e procedimentos de proteção digital, treinamento de funcionários e monitoramento de riscos.

De posse de todos os mecanismos de segurança, mesmo os mais bem elaborados, ainda estaremos sujeitos a ataques de indivíduos inescrupulosos, grandes conhecedores de sistemas e algoritmos denominados Hackers que invadem qualquer tipo de rede por razões conhecidas ou não.

Não existe uma proteção efetiva completa para que se possa proteger totalmente qualquer empresa desses ataques cibernéticos.

Tudo depende da filosofia a ser seguida pela empresa ou governo na elaboração de normas de conduta e ética na preservação dos dados e privacidade do usuário, mas quando alguma pessoa resolve ir para o “lado negro da força” é muito difícil poder controlar este ímpeto e convencê-la a seguir as regras universais de ética e moral de algum país.

Na visão de Hurel e Lobato (2018), especialistas na área de segurança cibernética, os hackers desenvolvem programas tão sofisticados que podem ultrapassar o avanço da segurança, que automaticamente prepara os contra-ataques e dificilmente atua de forma proativa no desenvolvimento de alguma defesa para ataques que ainda não existem.

Hackers criam recursos tão atuais que podem burlar os sistemas de segurança, seja de forma inédita ou por meio de caminhos já conhecidos que sejam pouco monitorados ou não recebam manutenção com frequência. Os profissionais de cibersegurança devem procurar defender seu campo de atuação utilizando métodos antigos ou buscando soluções novas no mercado, mas infelizmente nem sempre terão grande eficácia.

Para evitar surpresa e tentar minimizar e mitigar os problemas de invasão aos sistemas, cada empresa deverá implementar um sistema personalizado para a varredura contra invasões, pois somente seus gestores nesta área saberão com exatidão quais são os seus dados estratégicos que precisam de melhor armazenamento, conhecem o perfil dos usuários e sabem quais são os pontos fortes e fracos de suas redes, dependendo das máquinas nas quais investiram e sistemas que contrataram.

O que se percebe com as metodologias aplicadas é que todas precisam de um bom planejamento de ações para poder conseguir proteger os dados. Uma boa saída para manter as informações seguras é fazer o uso da IoT – Internet das

coisas (*Internet Of Things*, em inglês), além do uso do armazenamento em nuvem e de backups.

De posse de todas estas informações relacionadas à proteção de dados poderia se pensar em algum tipo de medida que pudesse ser tomada para tentar melhorar a proteção principalmente de infraestruturas críticas na área pública.

Uma das práticas principais seria a criação de uma politica de governança Digital similar à que foi constituída pelo governo em 2016 no intuito de administrar a utilização dos recursos de TICs com o objetivo de melhorar a disponibilização de informação e prestação de serviços públicos, incentivando a participação da sociedade no processo de tomada de decisão e aprimoramento dos níveis de responsabilidade, transparência e efetividade do governo, calcada em algumas normas como:

a) Oferta e prioridade de serviços públicos em meio digital disseminado para uma maior quantidade de dispositivos e plataformas de forma pulverizada;

b) Garantir de forma efetiva a segurança e privacidade dos cidadãos pela infraestrutura existente ou uma inovação por meio de novas tecnologias como AI (Inteligência Artificial) e IoT (Internet das coisas);

c) Disponibilização da prestação de serviços públicos de forma prioritária num modelo de “autosserviço”, onde o cidadão pode usar os serviços públicos em meio digital por sua própria interação, sem necessidade de auxílio de algum órgão ou entidade (empresa) que precise ofertar este serviço;

d) Disseminar a disponibilização de dados em formato aberto sem ser proprietário, de forma a ser usado num modelo amplo, acessível e que possa ser utilizado em larga escala no sistema de usuário simples ou entre máquinas (M2M).

Uma evolução histórica e o contexto atual da proteção de dados na Europa e no Brasil

Apesar do tema proteção de dados pessoais parecer bastante novo e atual a União Europeia já se preocupa com ele há bastante tempo, basicamente desde o início da década de 1970. Percorrendo um histórico das legislações específicas editadas desde essa época, REINALDO FILHO traça uma síntese da evolução dessas legislações. Segundo o autor, em 1970, o estado de Hesse, na Alemanha, editou a primeira lei específica sobre o tema. Depois foi a vez da Suécia, em 1973, editar a lei 289, de 11 de maio de 1973, o *Datalegen*. A Alemanha edita, em 1977, uma lei federal de proteção de uso ilícito de dados pessoais. A Dinamarca, por meio de duas leis - lei 243 e lei 244, ambas de 08

de julho de 1978 - regulamenta a proteção de dados e estende tal proteção para as pessoas jurídicas. Em 1978, na França, é editada a lei 78-77. Ainda nessa década, Espanha e Portugal tratam do tema por meio de dispositivos constitucionais; a Espanha estabelece no art. 18, par. 1º de sua constituição uma regra para a proteção da privacidade contra invasões da atividade informática, já Portugal, apresenta, ainda segundo o autor, um texto mais completo, em sua Constituição de 1977 (art. 35), "pois contempla a previsão do direito do cidadão de conhecer os dados que lhe são concernentes, de que esses dados sejam utilizados de acordo com a finalidade para o qual foram recolhidos e, ainda, de retificá-los (em caso de erro) e de atualizá-los" [REINALDO FILHO].

As legislações listadas acima, ainda que representem marcos regulatórios bastante importantes, o fazem de maneira nacional – isolada -, isto é, são legislações específicas de cada país da Europa, e em um momento ainda anterior à consolidação da União Europeia (EU), ou seja, não atuavam de modo integrado, com abrangência multinacional.

Ainda no traçado de uma evolução histórica das legislações pertinentes à proteção de dados pessoais na Europa, vale citar, o que diz REINALDO FILHO (2018) sobre a proteção de dados, ressaltando 5 parágrafos que descrevem a importância deste tema:

a) Os textos de caráter multinacional foram registrados como um fenômeno com a edição de leis nacionais de proteção de dados pessoais por diversos países de forma individual;
b) O OCED (1980) publicou por meio do seu comitê de ministros as "diretrizes sobre proteção da privacidade";
c) O mesmo OCDE publicou na mesma época, o Fluxo Transnacional de Informações pessoais que era um documento que buscava estabelecer princípios básicos sobre proteção de dados e sobre o fluxo das informações entre países que estavam em conformidade com estas leis, mesmo sem existir uma força coercitiva e permitir uma grande variação na implementação interna dos países;
d) Em 1981, foi promulgada pelo Conselho da Europa uma convenção que servia para "Proteção dos indivíduos em relação ao processamento automático de dados pessoais, que somente passou a vigorar em 1985;
e) A convenção do conselho é bastante similar a promulgada pela OCDE, onde estão contidas regras que protegem as informações pessoais em todas as fases do processamento de dados , iniciando a coleta até sua disseminação em larga escala. Existe uma proteção que descreve um processamento de maneira justa, de forma adequada, relevante e não excessiva em relação à finalidade da coleta, com dados exatos, atualizados e armazenados somente no período necessário da análise. O proprietário tem o direito de inquirir o controlador sobre o uso, obter

cópia da demanda, além de poder corrigir os dados falsos ou processados de forma imprópria. Todos os países signatários deverão editar suas leis em conformidade com seus princípios.

Em relação aos textos, Reinaldo Filho (2018) descreve a importância e influência dos mesmos na edição das leis de proteção dos dados que foi aplicada em 30 países que estavam contidos na convenção, além de alguns outros que resolveram aderir, pois desde 1997, os 15 países membros da união europeia já possuíam uma legislação própria em conformidade com a convenção, influenciando muitos outros mesmo aqueles que não eram da OCDE.

O autor ainda descreve que existe uma atividade legiferante (elaboração de leis) dentro dos Estados Nacionais que não é uniforme, por 3 razões principais:

a) Algumas leis nacionais de proteção de ados já existiam antes da convenção;
b) Ela não tinha caráter autoexecutável, o que permitia a implementação por alguns países de formas variadas;
c) Ela não incorporou alguma definições importantes, como um nível adequado de proteção de dados, o que permitiu que os países membros pudessem implementar conceitos e definições próprias dentro de sua legislação nacional.

Em 1995, a União Europeia editou uma Diretiva denominada 95/46/EC referente ao processamento de dados em nível pessoal no intuito de harmonizar o grau de proteção existentes nas leis de cada país e assegurar um fluxo livre de informações pessoais por todos os países membros, onde estabelecia um conjunto de regras que reforçava os direitos conquistados anteriormente além da criação de um novo conjunto de direitos aplicados ao processamento automático de dados em conjunto com a forma manual. Esta norma foi a responsável pela internalização no ordenamento jurídico de cada país membro da EU de direitos acerca de dados e informações pessoais no âmbito da EU, bem como de sua proteção. Para materializar a proteção desses direitos a Diretriz estabeleceu, ainda, que cada país membro da EU tivesse uma agência ou comissário de proteção de dados.

No passar dos anos 1980 e 1990, com a globalização ampliaram-se as possibilidades de negócios entre empresas locais e globais e a troca de informações entre governos e países. A reboque desse processo ocorreu um desenvolvimento exponencial das Tecnologias da Informação e Comunicação (TICs), o que propiciou uma alta capacidade de obter, armazenar e processar informações com a ajuda da informática. Logo as empresas perceberam as

vantagens competitivas que processamento de dados pessoais de seus clientes e consumidores em potencial traria para seus negócios. Nos anos 2000 vimos o crescimento exponencial das práticas de coleta, armazenamento e processamento de todo tipo de dados sobretudo os dados pessoais. Esses, viraram mercadoria e até moeda de troca, sendo negociados – comprados e vendidos – indiscriminadamente quer por meios ilícitos quer por meios lícitos (nenhuma proibição expressa em lei desse comércio), até culminarmos nos escândalos do **caso *Snowden*** e, mais recentemente, no **caso *Cambridge Analytica***.

Podemos dizer que os dois eventos citados se tornaram "cases" de referência quanto ao tema da proteção de dados pessoais e seus assuntos correlatos. Muito em função deles, mas também considerando uma preocupação antiga, já demonstrada na evolução histórica da proteção de dados pessoais, observamos hoje uma grande preocupação por parte das pessoas e de governos em proteger os dados pessoais, além das empresas e instituições de protegem seus dados e informações sensíveis. Nesse sentido, a GDPR europeia, recentemente aprovada pelo parlamento europeu, representa uma evolução da Diretiva 95/46/EC ao buscar equilibrar as relações e os processos que englobam pessoas, empresas e governos quanto a troca e obtenção de informações de caráter pessoal ou privado.

A GPDR em números

Com sua entrada em vigor em 25 de maio de 2018, a General Data Protection Regulation (GDPR), completou seu primeiro aniversário neste mês de maio de 2019. Segundo artigo de César, Aspis e Chaves (2019), citando trabalho realizado pela European Commision e a International Association of Privacy Professionals (IAPP) foram elaboradas as seguintes estatísticas dentro da pesquisa: 67% dos europeus ouviram em algum momento a respeito da GDPR; 57% dos europeus sabem que existe uma autoridade pública responsável pela proteção de dados pessoais; foram realizadas aproximadamente 144.376 reclamações às autoridades de proteção de dados europeias por supostas violações à GDPR; 89.271 notificações de ***data breach (violação de dados)*** foram apresentadas para as autoridades europeias de proteção de dados; 500 mil entidades localizadas na chamada European Economic Area (EEA) registraram Data Protection Officers (DPOs) perante as autoridades europeias; a aplicação da GDPR resultou em um montante de multas no valor de aproximadamente 56 milhões de euros.

No Brasil, pode-se dizer que a proteção de dados pessoais está, atualmente, ancorada, basicamente, em duas leis: a lei 12.965, de 23/04/2014, chamada de Marco Civil da Internet e a lei 13.709, de 14/08/2018, chamada de lei geral de proteção de dados (LGPD). A LGPD dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa

jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, sobre a proteção de dados pessoais enquanto que a lei 12.965 (Marco Civil da Internet) estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Ambas as leis brasileiras foram inspiradas na GDPR da EU e visam garantir maior controle sobre a coleta, utilização, transferência, correção e processamento de dados pessoais. Segundo Koehler e Scalco (2018) , este texto da LGPD consegue estabelecer de uma forma sistematizada, abrangente, dispondo de maior rigidez e organização, quais serão os critérios que serão utilizados para realização de operações que envolvam dados pessoais por o universo de pessoas físicas e jurídicas, tanto de direito público quanto de privado, excluindo-se a utilização de dados por pessoa física para uso particular e não econômico, e que seja utilizado para fins exclusivamente jornalísticos, artísticos, acadêmicos, na forma de investigação policial ou de segurança nacional.

Como principal medida protetiva, a partir da entrada em vigor da LGPD, em fevereiro de 2020, dados pessoais somente poderão ser usados mediante consentimento expresso e formal do titular da informação, que deverá receber informações sobre a finalidade, forma e duração de tratamento de seus dados pessoais. Esse mecanismo de proteção pretende dar mais controle à pessoa proprietária dos dados e mais transparência no uso dos dados pessoais por terceiros. Em decorrência dessas medidas protetivas as empresas deverão reformular internamente seus processos de tratamentos de dados de seus clientes, consumidores ou usuários, estabelecendo políticas de boas práticas e segurança de dados. Como forma de dar mais controle e transparência aos proprietários dos dados, a LGPD exige que aquele que controla dados pessoais de terceiros (pela ótica da empresa) “indique uma pessoa natural, denominado de encarregado, que será o responsável por supervisionar e fiscalizar o cumprimento das regras e servirá como um canal de facilitação da comunicação entre os titulares dos dados e aquele que os trata”. (Koehler e Scalco, 2018)

Tais medidas condicionam as empresas a ajustarem seus "termos e condições gerais de privacidade" de modo a darem indicação clara da forma, motivo e duração da utilização dos dados pessoais de seus clientes, consumidores ou usuários, além de força-las a criarem procedimentos simples para a obtenção das autorizações expressas e formais do uso dos dados de terceiros, bem como mecanismos de alteração e exclusão dos dados por solicitação desses terceiros.

Podemos dizer sem risco de errar que os dados e informações pessoais apresentam-se hoje como peso de ouro nos dois lados da balança que rege as

relações entre empresas e instituições, e clientes e pessoas. Nessa balança, o acesso aos dados pessoais, de modo geral, representam, por um lado, grandes oportunidades de realização de negócios e de prestação de serviços, dando às empresas e instituições informações valiosas de perfis de consumo e demanda de seus clientes ou consumidores, mas, por outro lado expõem a intimidade e violam a privacidade desses mesmos clientes ou consumidores. Se por um lado o acesso aos dados pessoais pode gerar lucros em geral, em uma economia globalizada, por outro, pode gerar prejuízos pessoais irreparáveis, tanto financeiros quanto sociais ou psicológicos. Por isso os governos dos países mais adiantados têm se debruçado sobre o tema, para que não haja excessos de qualquer dos lados, ou seja, para que não se permita o uso indiscriminado dos dados pessoais pela justificativa do lucro, da eficiência e do crescimento econômico, nem que se proíba qualquer uso de qualquer dado pessoal pela justificativa da preservação indiscriminada da privacidade. Parece ser consenso que os governos devem regular essa balança por meio de políticas públicas bem dimensionadas para buscar o ponto ótimo de equilíbrio entre as partes.

Bibliografia

ALVES, F. da Mota. **LGPD ou LPDP: como denominar a lei de proteção de dados brasileira**. Disponível em <http://www.lexmachinae.com>. Acesso em 30 de outubro de 2018.

AMAZON. **Amazon Elastic Compute Cloud (Amazon EC2).** Disponível em: <http://aws.amazon.com/pt/ec2/>. Acesso em: 29/10/2018.

BELLI, L. **Community networks: The Internet by the people, for the people.** Ed. FGV Direito-Rio, 2017.

BRASIL. **Lei de Informática e Tecnologia de Informação e Comunicação** – Lei 13.674 de 12 de junho de 2018. disponível em < www.planalto.gov.br>. acesso em 20/10/2018.

CÉSAR, A.; ASPIS, F. e CHAVES, L. **1 ano da GDPR: o que podemos aprender com os erros e acertos da Europa.** Disponível em : < https://www.conjur.com.br/2019-mai-31/opiniao-podemos-aprender-europa-ano-gdpr.>. Acesso em: 04/08/2019.

COUTINHO, L. **O Futuro da economia e o papel das TICs.** 54º Encontro Tele Síntese, Brasília. 2018.

FERREIRA, J. N. **Acessando a rede: um olhar sobre a formação da agenda para a regulação da internet no Brasil.** FGV EAESP - CMAPG: Dissertações de Mestrado em Administração Pública e Governo. 2014

HUREL, L.; LOBATO, L. **Uma Estratégia para a Governança da Segurança Cibernética no Brasil**. Instituto Igarapé. 2018.

ISACA. **Computação em Nuvem: Benefícios para o Negócio com Perspectivas de Segurança, Governança e Qualidade**. Documento Técnico da ISACA sobre Tecnologias Emergentes, 2009. Disponível em: <http://www.isaca.org/Knowledgecenter/Research/Documents/Cloud_WP_Portuguese_23Feb2011.pdf?id=7b50eb1c-093f-4835-b8c5-c8c9a7ab71d3>. Acesso em 28/10/2018.

KNIGHT, P et all. **Banda Larga no Brasil: Passado, Presente e Futuro**. Ed. Novo Século. 2016

KOEHLER, D. e SCALCO, N. **Proteção de dados: Novas diretrizes**. 2018. Disponível em: < https://www.migalhas.com.br/dePeso/16,MI286630,51045-Protecao+de+dados+Novas+diretrizes>. Acesso em: 04/08/2019.

MCAFEE, A.; BRYNJOLFSSON, E. **Big Data: The Management Revolution**. Harvard Business Review. Outubro 2012.

PINHO, F. **Anonimização de bases de dados empresariais de acordo com a nova Regulamentação Europeia de Proteção de Dados.** Universidade do Porto. 2016

RAMALHO, N.; PRADO, N. **Características dos Serviços de Computação em Nuvem Usados por Organizações Brasileiras** - USP. Disponível em < http://www.usp.br >. acesso em 22/10 /2018.

REINALDO FILHO, D. **A Diretiva Europeia sobre Proteção de Dados Pessoais - uma Análise de seus Aspectos Gerais**. 2018. Disponível em: <http://www.lex.com.br/doutrina_24316822_a_diretiva_europeia_sobre_protecao_de_dados_pessoais__uma_analise_de_seus_aspectos_gerais.aspx>. Acesso em: 04/08/2019.

WANG, L.; LASZEWSKI, G. et all. **Cloud Computing: a Perspective Study**. New Generating Computing. April 2010, Vol. 28, Issue 2.

Economática. 2018. **Valor de Mercado: Amazon é a segunda maior empresa do mundo**. Disponível em <https://insight.economatica.com/por-valor-de-mercado-amazon/> acesso em 20/07/2019.

Teleco. 2018 . **Evolução do mercado de telecomunicações**. Disponível em http://www.teleco.com.br acesso em 10/08/2018.