VIOLAÇÃO DE DADOS PESSOAIS E O PRINCÍPIO DA EFICIÊNCIA: UM DIÁLOGO ENTRE O PÚBLICO E O PRIVADO

VIOLACIÓN DE DATOS PERSONALES Y EL PRINCIPIO DE LA EFICIENCIA: UN DIÁLOGO ENTRE EL PÚBLICO Y LO PRIVADO

Vitor Hugo das Dores Freitas[*]

RESUMO
Os dados pessoais de milhares de cidadãos estão sendo violados causando profundos impactos aos usuários e à sociedade. O artigo tem por objeto analisar esta questão, conhecida como "vazamento de dados", e verificar se existem instrumentos legais e políticos – de indução, punição e proteção – para que o Estado promova, preventivamente, a funcionalização do direito dos cidadãos. A hipótese é de que não existem tais instrumentos preventivos despontando omissão do Estado e comprometimento de sua eficiência. A pesquisa utilizou-se do método hipotético-dedutivo, procedimentos bibliográficos, documentais e dados estatísticos para o estudo do tema de modo a oferecer reflexão sobre a necessidade de adoção de políticas públicas de prevenção à proteção dos dados pessoais.
Palavras-chave: Internet; Segurança da informação; Violação de dados; Privacidade.

RESUMEN
Los datos personales de millares de ciudadanos están siendo violados causando profundos impactos para ellos y para la sociedad. El artículo tiene por objeto analizar esta cuestión, conocida como "fuga de datos", y verificar si hay instrumentos legales y políticos - de inducción, penalización y protección – para que el Estado fomente, preventivamente, la funcionalidad del Derecho de los ciudadanos. La hipótesis es que no existen tales instrumentos preventivos señalando la omisión del Estado y comprometimiento de su eficiencia. La investigación utilizo el método hipotético-deductivo, procedimientos bibliográficos, documentales y datos estadísticos para el estudio del tema de modo a ofrecer reflexión sobre la necesidad de adopción de políticas públicas de prevención a la protección de los datos personales.
Palabras clave: Internet; Seguridad de la información; Violación de los datos; Privacidad.

Considerações Introdutórias

A violação de dados pessoais e sua exposição na Internet e outras midias, ação esta também conhecida como "vazamento de dados", merece reflexão mais acurada pela sociedade e pelo Estado.

[*] Advogado. Especialista em Direito da Informática pela Escola Superior de Advocacia – ESA; Mestrando em Direito pela Universidade Nove de Julho; Presidente das Comissões de Ciência e Tecnologia da OABSP e de Direito na Sociedade da Informação e Crimes Eletrônicos da OAB Pinheiros; Vogal suplente pela OABSP no segmento Terceiro Setor do Comitê Gestor da Internet no Brasil (CGI.com); Diretor do escritório brasileiro da Sociedade da Internet – ISOC BR; Palestrante do Departamento de Cultura e Eventos da OABSP na área de Direito da Informática, Processo Eletrônico, Certificação e Assinatura Digital; Presidente do Conselho de Usuários do Grupo América Móvil (Embratel, Net, Claro) da Região Sudeste. E-mail: vhf@uol.com.br

Além de se constituír em atentado ao direito fundamental da privacidade, a violação de dados pessoais pode servir de moeda ao crime organizado, à espionagem corporativa e à manipulação da sociedade e do mercado.

A partir da compreensão da revolução tecnológica e seus efeitos, do que vem a ser dados, dados pessoais, banco de dados, o conceito de violação de dados e os direitos envolvidos, este artigo tem por objeto analisar a seguinte questão: quais os instrumentos legais e políticos que o Estado dispõe para promover, preventivamente, a funcionalização do direito fundamental do cidadão quanto à sua privacidade?

Não há como desconhecer o fato de que existem problemas para o Estado na concretização dos direitos fundamentais do cidadão; todavia, impõe-se o enfrentamento da questão visando promover diálogo entre o público e o privado de forma que as partes interessadas possam dimensionar não só a responsabilidade do Estado quando se omite na realização de políticas públicas voltadas à defesa dos direitos fundamentais do cidadão como permitir criar massa crítica para que a sociedade possa buscar solução eficiente e eficaz contra problema que tende a se agravar.

Tendo isto em mente o estudo utilizou-se de várias estatísticas disponíveis que permitiram a interpretação dos dados em sua total realidade de forma a avaliar se a violação de dados vem ou não aumentando e se este fato está atingindo, sistemicamente, a sociedade como um todo. Após o estudo, autoridades e sociedade estarão aptas a discorrem, em condições de igualdade e mais profundamente, sobre a questão.

O estudo está dividido em partes que, com certeza, permitirão auferir os resultados obtidos conduzindo o leitor para uma solução adequada à questão formulada.

Há que se ponderar que existiam redes de computadores antes do advento da Internet que se comunicavam por meio de cartões perfurados e, posteriormente, por cabos *ethernet*. Estas redes ainda funcionam e são conhecidas como intranets, de uso interno e restrito. Em razão disso o artigo acompanha entendimento de que a expressão Internet com "I" maiúsculo se refere à "[...] rede global de computadores conectados entre si [...]" diferenciando-a da expressão com "i" minúsculo destinada para designar "[...] redes de computadores privadas interligadas sem qualquer relação com a Internet global [...]"[1]; novamente acompanhando posicionamento doutrinário de Marcel Leonardi e José Afonso da Silva[2] a expressão "privacidade" utilizada no artigo engloba tanto "intimidade" quanto "vida privada" referindo-

[1] LEONARDI, Marcel. *Tutela e Privacidade na Internet*. São Paulo: Saraiva, 2012, p. 23.
[2] Idem, op. cit., p. 83

se, assim, ao direito ou seu objeto; por fim, o artigo considera violação de dados pessoais todos os atos praticados de forma acidental ou intencional.

O longo caminho da informação

A tecnologia é inerente ao homem. Individualmente ou socializado, o ser humano sempre se utilizou da tecnologia para alçar novos patamares ou reformular o meio ambiente adaptando-o às suas necessidades.

Ao se entender tecnologia como "...qualquer mecanismo que possibilite ao homem executar suas tarefas fazendo uso de algo exterior ao seu corpo, ou seja, tudo aquilo que se caracteriza como extensão do organismo humano..."[3] então a revolução tecnológica sempre existiu – o que ocorreu é que só a percebemos como tal quando deixou de ser um contrapeso para passar a controlar o homem gerando desequilíbrio na relação de interdependência.

Evidentemente que a evolução humana e a evolução tecnológica nem sempre caminharam no mesmo passo: afinal há 200 mil anos a comunicação era realizada de forma oral; posteriormente agregou-se a visual (petróglifos) e finalmente a escrita (hieróglifos) e desta até os dias atuais a tecnologia evoluiu a passos largos impactando o meio-ambiente e todas as áreas conhecidas pelo homem, inclusive o direito "A tecnologia muda o homem e muda o direito, não exatamente no mesmo compasso, provocando muitas vezes surpresa e perplexidade aos feitores e mantenedores do direito"[4] evocando a teoria autopoiética de Humberto Maturana[5]:

> A tecnologia é uma operação em conformidade com as coerências estruturais de diferentes domínios de ações nas quais uma pessoa pode participar como ser humano. Enquanto tal, a tecnologia pode ser vivida como um instrumento para ação intencional efetiva, ou como um valor que justifica ou orienta o modo de viver no qual tudo é subordinado ao prazer vivido ao se lidar com ela. Quando é vivida desse último modo, a tecnologia se torna um vício cuja presença os nela viciados desejam justificar com argumentos racionais fundados na realidade histórica de sua imensa expansão nos tempos modernos. Se vivida como um instrumento para ação efetiva, a tecnologia leva ã [sic] expansão progressiva de nossas habilidades operacionais em todos os domínios nos quais há conhecimento e compreensão de suas coerências estruturais.

---

[3] PERLES, João Batista. *Comunicação: conceitos, fundamentos e história*. Biblioteca on-line de ciências da comunicação. Portugal, [s.d]. p. 4. Disponível em <http://www.bocc.ubi.pt/pag/perles-joao-comunicacao-conceitos-fundamentos-historia.pdf>. Acesso em: 19 abr. 2014.

[4] LIMA, Paulo Marco Ferreira. *Crimes de Computador e Segurança Computacional*. 2ª ed., São Paulo: Atlas, 2011, p. XIII.

[5] MATURANA R., Humberto. *Cognição, Ciência e Vida cotidiana*. Organização e tradução: Cristina Magro, Victor Paredes. - Belo Horizonte: Ed. UFMG, 2001, p. 187.

Tudo indica, assim, que hodiernamente o homem acabou se transformando em um dependente tecnológico o que se reflete, por exemplo, no uso de redes sociais, ou seja:

> "Do ponto de vista clínico, considera-se Dependência de Tecnologia (do inglês 'technological addiction') quando o indivíduo não consegue controlar o próprio uso da internet/jogos/smartphones, ocasionando sofrimento intenso e/ou prejuízo significativo em diversas áreas da vida." [6]

Como mera curiosidade, deve ser observado que a abstinência do uso das tecnologias da informação e comunicação causa os mesmos sintomas da abstinência do uso de drogas, álcool e jogos de azar por se tratar de transtorno comportamental[7].

Inicialmente armazenada em pedras, pergaminhos e rolinhos de argila a informação, atualmente, é arquivada em meios digitais; em razão do avanço da tecnologia e da nanotecnologia os dados ainda poderão ser armazenados, no primeiro caso, em bancos de dados próprios ou em nuvem (privada, pública ou mista) e, no segundo, em discos de terceira, quarta e quinta dimensão (holografia) não significando isso o exaurimento dos meios de registro ou de armazenamento de informações; ao contrário, esse conceito poderá incorporar no futuro qualquer material, orgânico ou não, físico ou virtual - desde que os sistemas de transmissão de dados assim o suportem. Com efeito, um eficiente meio de registro de informações datado de milhões de anos é o ***ácido desoxirribonucleico***, conhecido pela sigla inglesa *DNA*, no qual cientistas de Harvard demonstraram ser possível o armazenamento de dados[8]. Dentre outras vantagens nesse método de registro e guarda de informações destacam-se duas: a estabilidade de ocultar a informação em temperatura ambiente e a possibilidade de alguém acessar as informações depois da morte do "agente". Uma das desvantagens é a velocidade de leitura e gravação dos dados.

Com relação aos meios de transmissão de dados, o telégrafo permitiu:

> [...] a inauguração de novos serviços (transmissão de ordens de pagamento, compra e venda de ações, redes de transporte, etc). Para se ter uma ideia da revolução causada pelo descobrimento do telégrafo nos Estados Unidos da América no ano de 1880, mais de 32 milhões de mensagens foram trocadas através daquele meio criando, assim, novas indústrias, riquezas, cultura e inovação.[9]

---

[6] DEPENDÊNCIA DE TECNOLOGIA. *Definições: o que é dependência de tecnologia?* [s.l.] [s.d]. Disponível em < http://dependenciadetecnologia.org/dependencia-de-tecnologia/definicoes/>. Acesso em: 10 jun. 2014.

[7] HOUGH, Andrew. *Student 'addiction' to technology 'similar to drug cravings', study finds*. UK, 08 abril de 2011. The Telegraph. Disponível em < http://www.telegraph.co.uk/technology/news/8436831/Student-addiction-to-technology-similar-to-drug-cravings-study-finds.html>. Acesso em: 10 jun. 2014.

[8] LEO, R. Alan. Harvard Medical Schol. *Writing the Book in DNA*. August 16, 2012. Disponível em < http://hms.harvard.edu/news/writing-book-dna-8-16-12>. Acesso em: 10 jun. 2014.

[9] FREITAS, Vitor Hugo das dores. *O e-mail profissional enquanto correspondência:* a legislação brasileira, a doutrina e jurisprudência sobre a matéria. Escola Superior de Advocacia da Ordem dos Advogados do Brasil, Seção de São Paulo. São Paulo: 2012, p. 29.

Com a invenção do computador e das redes de computadores a revolução causada pelo telégrafo não só se solidificou como permitiu, anos mais tarde, o surgimento de outra inovação tecnológica: a Internet que, identicamente, causou nova revolução dando ensejo à criação do espaço virtual onde floresce ciberculturas, a cibersocialização[10] e, consequentemente, a realização de novos serviços e atividades. Pedro R. Doria[11], que prefere utilizar o termo *cyberspace*, conceitua espaço virtual como "...o ambiente da Internet. Se voltarmos à noção de cidade, dizemos que o cyberspace é o espaço onde os habitantes da cidade vivem. Mas, se preferirmos a noção de banco de dados, definimos como o ambiente em que esses bancos de dados estão.".

A sociedade da informação assenta a sua base na cultura da informação podendo ser conceituada como "... uma nova forma de organização social, política e econômica que recorre ao intensivo uso da tecnologia da informação para coleta, produção, processamento, transmissão e armazenamento de informações"[12] exercendo forte influência em todos os setores da sociedade[13].

Assim, se em 1880 o telégrafo movimentou mais de 32 milhões de mensagens, em 2016 a Internet deverá movimentar mais de um sextilhão de *bytes*, ou seja, alcançará 1,3 *zettabyte* (1.180.591.620.717.411.303.424 de *bytes* ou 2^{21} *bytes*) bem maior que o tráfego de dados de 2011, este com 369 *exabyte* (1.152.921.504.606.846.976 de *bytes* ou 2^{18} *bytes*), conforme noticiado nas mídias eletrônicas[14], valendo lembrar que *bytes* representam nos computadores caracteres alfanuméricos. Com relação aos dados móveis, o Relatório Cisco VNI (*Visual Networking Index*) sobre o Tráfego Global de Dados Móveis 2013-2018 relata que o tráfego global da Internet móvel será multiplicado por 11 nos próximos quatros anos, alcançando 190 *exabytes* em 2018 equivalendo este valor a 190 vezes a soma de todo o

---

[10] OABSP. *Internet, ciberespaço, cibercultura e cibersocialização.* Comissão de Ciência e Tecnologia. Certificados e Assinatura Digital. São Paulo: 2013. Disponível em <http://www2.oabsp.org.br/asp/certificadodigital/internet.html>. Acesso em: 10 jun. 2014.

[11] DORIA, Pedro R., 1995 *apud* AQUINO, Leonardo Gomes de. *Direito & Internet: Uma Questão de Congruência*. Conteúdo Jurídico. Brasilia-DF: 24 abr. 2009. Disponível em: <http://www.conteudojuridico.com.br/?artigos&ver=2.22546>. Acesso em: 10 jun. 2014.

[12] VIEIRA, Tatiana Malta. *O Direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação*. Porto Alegre: Sergio Antonio Fabris Ed., 2007, p. 176-177

[13] BARBOSA, Alexandre F. (Coord.). Tradução:Karen Brito Sexton. *Pesquisa sobre o uso das tecnologias de informação e comunicação no Brasil : TIC Educação 2010*. Disponível em < http://op.ceptro.br/cgi-bin/cetic/tic-educacao-2010.pdf>. Acesso em: 10 jun. 2014.

[14] *Tráfego de dados na Internet ultrapassará o "zettabyte" em 2016*. Portal Terra, [s.l.], 30 de maio de 2012. Disponível em <http://tecnologia.terra.com.br/internet/trafego-de-dados-na-internet-ultrapassara-o-quotzettabytequot-em-2016,024bfe32cdbda310VgnCLD200000bbcceb0aRCRD.html>. Acesso em: 10 jun. 2014.

tráfego IP (fio e móvel) gerado no ano de 2000, a 42 milhões de imagens e a 4 biliões [sic] de clips de vídeo[15].

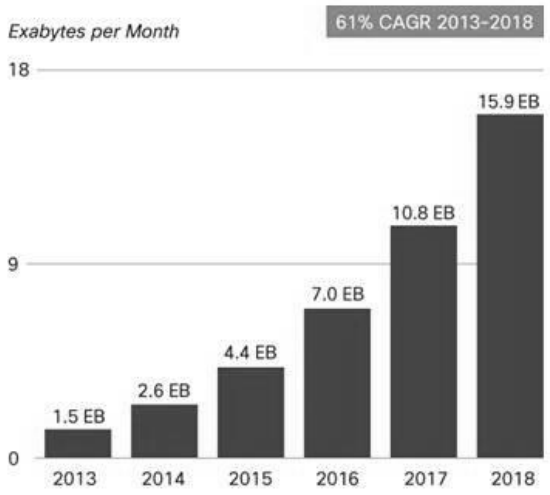

Figura 1 – Projeção do tráfego de dados móveis global. Fonte: Cisco VNI Mobile 2014

Recentemente a *International Telecommunication Union* -ITU, agência especializada das Nações Unidas para as tecnologias de informação e comunicação, divulgou comunicado[16] relatando, dentre outras estatísticas, que até o final do ano de 2014 a Internet terá aproximadamente 3 bilhões de usuários dos quais 2/3 serão provenientes de países em desenvolvimento; que o número de assinaturas de banda larga móvel deverá atingir a cifra de 2,3 bilhões de usuários globalmente; que haverá queda de 100 milhões de assinantes na telefonia fixa em relação ao ano de 2009; ocorrerá aumento de assinantes de celulares para quase 7 bilhões de usuários, dos quais 3,6 bilhões na região Ásia-Pacífico; que a banda larga fixa terá atingido 10% a nível mundial com desaceleração do crescimento nos países em desenvolvimento; haverá aumento das assinaturas de banda larga móvel em 32% globalmente; que 44% das famílias em todo o mundo terão acesso à Internet dos quais 31% se referem aos países em desenvolvimento e 78% nos países desenvolvidos, e assim por diante.

Trata-se de vasto volume de dados em trânsito na Internet que acabam desaguando em vários bancos de dados que, de seu turno, devem ser protegidos para que dados pessoais não sejam violados.

---

[15] CISCO. Arquivo de notícias 2014. *Tráfego global de dados móveis crescerá 11 vezes entre 2013 e 2018 segundo o Relatório Cisco VNI*. [s.l.:s.d.]. Disponível em <http://www.cisco.com/web/PT/press/articles/2014/20140205.html>. Acesso em: 10 jun. 2014. Íntegra do relatório disponível em <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html>. Acesso em: 10 jun. 2014.

[16] ITU. Newsroom. Press Release. *ITU releases 2014 ICT figures. Mobile-broadband penetration approaching 32 per cent Three billion Internet users by end of this year*. Disponível em < http://www.itu.int/net/pressoffice/press_releases/2014/23.aspx#.U9WDnbFiNBm >. Acesso em: 10 jun. 2014.

Dados pessoais, tratamento de dados, banco de dados e o valor da informação

Os dados pessoais e o tratamento de dados pessoais podem ser assim definidos

> a) «Dados pessoais», qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social; b) «Tratamento de dados pessoais» («tratamento»), qualquer operação ou conjunto de operações efectuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição; [17]

Devidamente armazenados, tratados, indexados e relacionados entre si em bancos de dados, públicos ou privados, eles acabam ampliando horizontes porque geram informações que permitem a criação de perfis, relatórios complexos, tendências, etc. implicando, de um lado, na rápida tomada de decisões para novos negócios, estratégias militares, comportamentos sociais, tendências políticas, dentre tantos, e, de outro, que governos e empresas, públicas e privadas, se tornem ágeis e dinâmicas modificando estruturas hierarquizadas e piramidais para oferecerem nas relações de consumo, por exemplo, pacotes de produtos e serviços integrados ao cidadão com base em seus desejos e preferências pessoais incorporando, no processo, suas próprias moedas digitais como a *Bitcoin* e *Litecoin*. Por fim, e não menos importante, as informações pessoais podem se transformar em fonte de informações para organizações criminosas; de poder e controle para governos ou mesmo de espionagem corporativa entre conglomerados empresariais.

Desponta certo, assim, que a posse de dados pessoais se reveste de matéria prima para a economia digital.

O valor agregado das informações e dados pessoais é indiscutível valendo lembrar o relato de Nicholas Negroponte sobre visita que fez a uma empresa onde lhe perguntaram, no registro de entrada, se portava um *laptop*; ao informar que sim, solicitaram então que fornecesse o modelo, o número de série e o valor aparelho. Quanto a este último item Nicholas informou que o aparelho custava "Alguma coisa entre 1 e 2 milhões de dólares" e muito embora o aparelho fosse estimado em torno de 2 mil dólares, a "...questão é que, embora os átomos não valessem tudo aquilo, os bits tinham um valor inestimável"[18]. A perda ou roubo de um smartphone, por exemplo, pode nada representar ao usuário – mas as fotos,

[17] UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa. Disponível em <http://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046>. Acesso em: 10 jun. 2014.

[18] NEGROPONTE, Nicholas. *Vida digital.* Tradução: Sérgio Teralloli; supervisão técnica Ricardo Rangel. São Paulo: Companhia das letras, 1995, p. 17

dados pessoais, agenda e outras informações nele armazenadas possuem valor inestimável e, não raras vezes, representam informações insubstituíveis.

Pesquisa realizada pela empresa *Symantec* sobre Custo e Gestão da Informação realizada no ano de 2012 na América Latina[19], nela incluído o Brasil, constatou que empresas estão armazenando enormes quantidades de informações em repositórios como *data centers*, *desktops*, *laptops*, *smartphones*, *tablets*, sistemas de *backup* e arquivos mortos; segundo os entrevistados, o valor da informação corresponde a 50% (cinquenta por cento) do valor de mercado das organizações. Por fim, e não menos interessante, a perda irremediável das informações armazenadas se reveste de catástrofe vez que representa a perda de 55% de clientes; 50% de danos à marca; 40% de redução na receita e 32% em multas.

Como o tráfego de dados tende a crescer na Internet, é certo que seus repositórios acompanharão a mesma tendência implicando, consequentemente, em alto custo em investimentos para sua gestão, ou seja, para a segurança da informação. Em novo relatório do ano de 2013 a mesma empresa chegou a divulgar que o custo das violações de dados implica em uma média global de US$ 136 por registro, ou cerca de R$290 (observando-se que a conversão do dólar foi baseada na taxa de R$2,13 de junho de 2013, segundo a fonte consultada), e que setores altamente regulados como o financeiro, saúde e farmacêutica tiveram custos de violações 70% maiores do que outros segmentos sendo que no Brasil "...o custo total médio de um incidente de violação foi de R$ 2,64 milhões. O custo máximo do vazamento de dados entre as 31 empresas sediadas no Brasil foi de R$ 9,74 milhões e o custo mínimo foi de R$230 mil..."[20].

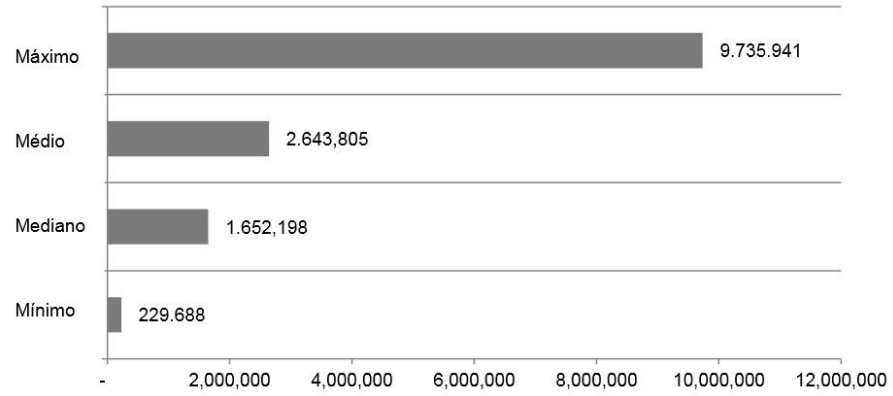

Figura 2. Medidas de custo de vazamento de dados de 31 empresas brasileiras. Fonte: Relatório 2013 da Symantec sobre o Custo do Vazamento de Dados – Brasil. Relatório do Ponemon Institute.

[19] SYMANTEC. *Pesquisa sobre Custo e Gestão da Informação: resultados da América Latina.* [s.l.], [s.d.], 2012. Disponível em < http://www.symantec.com/content/pt/br/enterprise/images/theme/state-of-information/2012-SOI-PDF-LAM-PORT-v2.pdf>. Acesso em: 10 jun. 2014.

[20] SYMANTEC. *Estudo da Symantec e Ponemon Institute Revela que Negligência Humana e Erros de Sistema são Responsáveis por Dois Terços dos Vazamentos de Dados*. São Paulo, 05 de junho de 2013. Disponível em <http://www.symantec.com/pt/br/about/news/release/article.jsp?prid=20130605_01>. Acesso em: 10 jun. 2014.

De esclarecedor no relatório apontado a informação de que o custo médio da violação varia em todo o mundo e cujas diferenças podem ser atribuídas:

> [...] aos tipos de ameaças sofridas pelas organizações bem como às leis de proteção de dados nos respectivos países. Alguns países como Alemanha, Austrália, Reino Unido e Estados Unidos possuem mais leis de proteção ao consumidor e normas para reforçar a privacidade e a segurança dos dados eletrônicos. No Brasil, o custo médio por violação chega a R$ 116 por registro, enquanto países como Estados Unidos e Alemanha se mantém no marco dos vazamentos mais dispendiosos (cerca de *R$400 e *R$424 por registro, respectivamente). Esses dois países também tiveram o mais alto custo por vazamento de dados (Estados Unidos com US$5,4 milhões ou cerca de *R$11,5 milhões e a Alemanha com US$4,8 milhões ou cerca de *R$10,2 milhões).[21]

Exatamente por se revestir a informação de recurso valiosíssimo da economia digital é que empresas devem investir em sua proteção; todavia, como esse investimento possui alto custo pode ocorrer que nem todas promovam o investimento necessário ou, em caso de sua promoção, o façam de forma parcial ou insatisfatória deixando de lado, ou mascarando, a segurança da informação pessoal, a ética e a responsabilidade empresarial que deveriam pautar seus negócios; ademais, conforme pesquisa efetuada pela empresa *PriceWaterhouse*[22], em que pese aumento de 51% de investimentos em segurança da informação no ano de 2014 em comparação com o ano de 2013, as empresas, em sua maioria, utilizam-se de modelos antigos para combater as novas ameaças, perdendo-se na escolha de definições de melhores práticas de segurança e com dificuldades em identificar e priorizar os dados que necessitam de proteção aumentando o número de incidentes com relação à perda de dados em 16% em relação a 2012.

Finalmente o Relatório de Ameaças à Segurança na Internet de 2014[23] da *Symantec* informa que o ano de 2013 foi "O ano das Mega Violações" com um aumento de 62% em relação ao ano anterior divulgando, dentre outras, as seguintes estatísticas: aumento de 91% em campanhas de ataques direcionados e mais de 552 milhões de identidades expostas por meio de violações colocando as informações pessoais de consumidores em risco.

---

[21] Idem, op. cit.

[22] PRICEWATERHOUSE. *Pesquisa Global de Segurança da Informação 2014 da PwC*. Disponível em < http://www.pwc.com.br/pt_BR/br/publicacoes/servicos/assets/consultoria-negocios/pesq-seg-info-2014.pdf>. Acesso em: 10 jun. 2014.

[23] SYMANTEC. *Relatório de Ameaças à Segurança na Internet de 2014, Volume 19*. Disponível em < http://www.symantec.com/pt/br/security_response/publications/threatreport.jsp>. Acesso em: 10 jun. 2014.

Figura 3 - Total de Violações e Total de Identidades Expostas. Relatório de Ameaças à Segurança na Internet de 2014, Volume 19. Fonte: Symantec

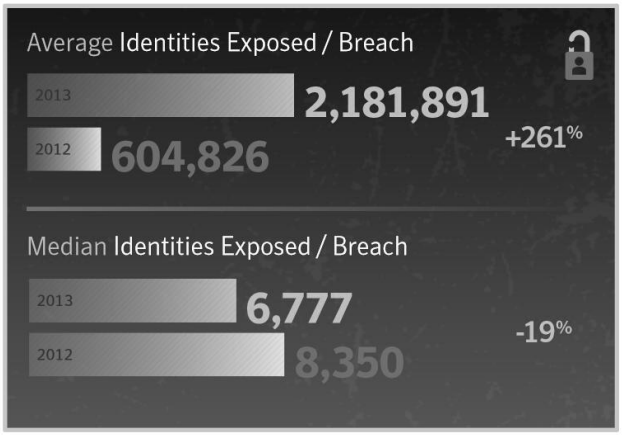

Figura 4 - Média de Identidades Expostas/Violadas. Relatório de Ameaças à Segurança na Internet de 2014, Volume 19. Fonte: Symantec

Violação de dados e sua exposição

Em informática a expressão "incidente" é utilizada para descrever

> qualquer acção ou conjunto de acções desenvolvidas contra um computador ou rede de computadores e que resulta, ou pode resultar, na perda da confidencialidade, integridade ou desempenho de uma rede de comunicação de dados ou sistema computacional, designadamente, o acesso não autorizado, a alteração ou remoção de informação, a interferência ou a negação de serviço em sistema informático.[24]

No Brasil o tratamento de incidentes é efetuado por vários Centros de Segurança e Resposta a Incidentes (CSIRT's); dentre eles destacam-se os Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR

[24] PORTUGAL. CERT.PT – Serviço de Resposta a Incidentes de Segurança Informática. Disponível em < http://www.cert.pt/index.php/servicos/tratamento-de-incidentes>. Acesso em: 19 abr. 2014.

Gov), órgão subordinado ao Departamento de Segurança de Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República (GSIPR) e que tem por objetivo definir os padrões sobre os procedimentos relacionados ao processo de notificação de incidentes de segurança em redes de computadores da Administração Pública Federal (APF), e o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (CERT.br), mantido pelo Comitê Gestor da Internet no Brasil (CGI.br), este último que define incidente como qualquer:

> [...] evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores. São exemplos de incidentes de segurança: tentativas de ganhar acesso não autorizado a sistemas ou dados; ataques de negação de serviço; uso ou acesso não autorizado a um sistema; modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema; desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso.[25]

Esses incidentes, que podem ser intencionais ou acidentais, demonstram as fragilidades de computadores e redes de computadores; como o número de incidentes é vasto[26] eles são organizados em categorias para fins de análise, relatórios e providências. O CERT.br, por exemplo, os classifica em *worm* (vermes); *DoS* (negação de serviços); invasão, *web*, *scan* (varreduras em computadores de forma a identificar alvos para ataque), fraude e outros.

Figura 5- Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2013 - Fonte: CERT.br

[25] CERT.BR – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em < http://www.cert.br/docs/certbr-faq.html#6>. Acesso em: 10 jun. 2014.

[26] VERIZON. *Data Breach Investigations Report Verizon 2014*. [s.l.]. Disponível em < http://www.verizonenterprise.com/DBIR/2014/>. Acesso em: 10 jun. 2014.

A violação de dados – também conhecida como vazamento de dados, vazamento de informações, perda de dados ou derrame de dados – é um incidente de segurança onde dados contendo todo tipo de informações confidenciais é visto, roubado ou utilizado por terceiros não autorizados. Como já afirmado a violação de dados poderá ocorrer de forma acidental ou intencional, interna ou externamente às empresas, e deverá ser apurado por meio de ferramentas, processos e treinamentos; constatando-se, na apuração, que houve violação ou vazamento intencional, o incidente será tratado como fraude.

O Relatório *Security Index* da UNISYS, que fornece estatísticas em oito áreas de segurança (dentre elas Segurança Nacional, Financeira, Internet e Pessoal) concedeu ao Brasil, no ano de 2013, o Índice de Segurança 173 (um pouco abaixo do ano de 2012, quando o índice foi 176) significando "...que os brasileiros estão seriamente preocupados." [27]

Segundo o sumário do relatório daquela empresa 75% dos brasileiros estão seriamente preocupados com a obtenção, por terceiros, de detalhes de seus cartões de crédito ou débito; 54% estão seriamente preocupados com a segurança do computador em relação a vírus ou *spam*; 48% estão seriamente preocupados com a segurança de compras ou operações bancárias online e 87% estão "muito preocupados" com a violação de dados envolvendo pelo menos um dos cinco setores sendo que a vulnerabilidade por parte das organizações de saúde é a maior preocupação (93%), conforme se verifica do mapa *Brazil Security Index - Overall Security Index Score*, 2013/2012, com barra de gráficos para os apontadores *National*, *Financial*, *Internet* e *Personal*:

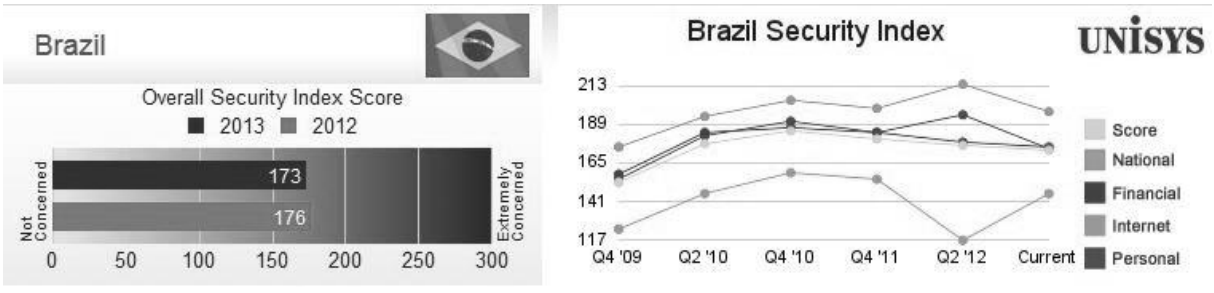

Figura 6- *Brazil Security Index* – Fonte: Unisys Corporation

[27] UNISYS CORPORATION. *Unisys Security Index TM: BRAZIL*. April, 2013. Disponível em <http://www.unisyssecurityindex.com/usi/brazil>. Acesso em: 10 jun. 2014.

Consequentemente, as informações pessoais de usuários e consumidores são alvos desejados pelos criminosos uma vez que servem como ponto de partida para o acesso a outras atividades, serviços e informações do usuário lesado como o acesso ao sistema bancário, o roubo de perfis, espionagem, sequestros, etc.

Segundo a *Verizon*[28]:

> A maioria dos ataques é perpetrada por agentes externos, ao contrário de colaboradores e parceiros. Grupos criminosos com motivação financeira ainda são o tipo dominante de autor em ataques externos - embora a espionagem apareca cada vez mais frequentemente em nosso conjunto de dados. Apesar de toda a ênfase no "hacktivismo" na imprensa, os ataques orientados por ideologia permanecem uma porcentagem muito pequena.

Muitos desses incidentes não são relatados ao público; e, quando relatados, os comunicados se fazem de forma tardia, quando os danos se fizeram sentir em toda a sua plenitude não restando ao usuário ou consumidor senão poucas alternativas dentre as quais a de postarem suas reclamações em sítios eletrônicos especializados; o de providenciarem ações judiciais de forma individual ou coletiva; aguardarem ações e providências dos órgãos governamentais ou; ainda, e o que é pior, ficarem inertes.

Dois exemplos de violação de dados ocorridos no âmbito internacional podem ser esclarecedores ao presente artigo: a empresa *Adobe Systems***,** segundo notícias[29], teve 152 milhões de usuários expostos após uma violação de dados ocorrida em 2013; a empresa não negou os fatos uma vez que afirmou que a invasão chegara a 38 milhões de contas. Entre os dados furtados encontram-se endereços de e-mail, senhas encriptadas e dicas de senhas armazenadas sem qualquer proteção nos perfis dos usuários. Em que pese ter afirmado que 25 milhões de registros contém endereços de e-mail inválidos e que 18 milhões de registros se encontram com senhas sem efeito, o fato é que a violação de dados efetivamente ocorreu. Já na empresa *Target***,** a gigante do varejo norte-americano, a violação atingiu 70 milhões de dados de clientes e 40 milhões de informações bancárias fazendo com que o lucro da empresa recuasse em 46% em sua base anual[30]; segundo outra agência noticiosa "...uma investigação

---

[28] VERIZON. *Data Breach Investigations Report Verizon 2014*, p. 3: "Most attacks are perpetrated by external actors, as opposed to employees and partners. Financially motivated criminal gangs are still the dominant type of perpetrator in external attacks — although espionage appears increasingly often in our data set. Despite all the emphasis on "hacktivism" in the press, ideology-driven attacks remain a very small percentage of the total". Tradução livre. Disponível em < http://www.verizonenterprise.com/DBIR/2014/>. Acesso em: 10 jun. 2014.

[29] O GLOBO.COM. *Vazamento de 152 milhões de contas de usuário da Adobe pode ter sido o maior da história*. Disponível em < http://oglobo.globo.com/sociedade/tecnologia/vazamento-de-152-milhoes-de-contas-de-usuario-da-adobe-pode-ter-sido-maior-da-historia-10725973>. Acesso em: 10 jun. 2014.

[30] ECO.FINANÇAS. *Target: Empresa demite CEO após vazamento de dados*. [s.l], 05 de maio de 2014. Disponível em < http://www.ecofinancas.com/noticias/target-empresa-demite-ceo-vazamento-dados>. Acesso em: 10 jun. 2014.

[na Target] concluiu que a única medida de proteção aplicada pela companhia foi uma cópia gratuita do antivírus Malware-bytes"[31].

O Brasil também está vivenciando violações de dados de grandes proporções, valendo citar três casos de repercussão nacional: ***o primeiro*** se refere ao sítio eletrônico Ingresso.com. Segundo notícias[32], os clientes deste sítio eletrônico tiveram seus dados pessoais (CPF, RG, data de nascimento, sexo, endereço e filiação) violados e divulgados dentro de um e-mail contendo falsa promoção relativa ao jogo do Brasil na Copa do Mundo 2014; em razão deste fato os usuários enviaram reclamações ao Procon, em sítios eletrônicos de defesa do consumidor[33] e na rede social *Facebook*. Consultada, a empresa responsável alegou que "...os dados não partiram de seus sistemas e que o caso está sendo tratado pelas autoridades competentes" enquanto que o Procon, de seu turno, afirmou que estaria abrindo uma investigação a respeito do assunto; ***o segundo*** está ligado às recentes manifestações populares que abalaram o Brasil: em setembro de 2013 dados pessoais (CPF, RG, e-mail, telefone, conta bancária e endereço) de 50 mil policiais do Estado do Rio de Janeiro e que incluíram os dados do comandante-geral da corporação, Coronel Luís Castro, foram expostos na rede social Facebook[34]. A autoria do vazamento de dados foi assumida pelo grupo "*Anoncyber & Cyb3rgh0sts*" que informou que o ato foi uma resposta à violência policial durante as manifestações ocorridas no Estado do Rio de Janeiro – porém que a "...intenção não era prejudicar"[35], e; finalmente, ***o terceiro e último*** trata do que alguns estão denominando de "estelionato mercadológico": no ano de 2013 o Ministério Público Federal descobriu que a empresa Oi S/A, desde 2012, vinha violando dados pessoais (nomes, telefones, informações bancárias e cadastros de pessoas físicas) de seus 6 milhões de clientes em todo o Brasil a outras empresas as quais, passando-se pela Oi, constrangiam consumidores a contratar seus serviços. Segundo o Ministério Público Federal este comportamento é um

---

[31] CANALTECH CORPORATE. Redação. *Relembre os maiores vazamentos de informação de 2013*. [s.l.], 26 de março de 2014. Disponível em < http://corporate.canaltech.com.br/materia/seguranca/Relembre-os-maiores-vazamentos-de-informacao-de-2013/>. Acesso em: 10 jun. 2014.

[32] ROCHA, Camilo. *E-mail exibe dados de clientes do site Ingresso.com*. O Estado de São Paulo. Caderno Economia, B14, 14 de mar. 2014. Disponível em < http://estadao.br.msn.com/link/e-mail-exibe-dados-de-clientes-do-site-ingressocom>. Acesso em: 10 jun. 2014

[33] RECLAMEAQUI. *Vazamento de dados pessoais pela Internet – E-mail de promoção de ingressos para a Copa 2014*. Disponível em <http://www.reclameaqui.com.br/8664929/ingresso-com/vazamento-de-dados-pessoais-pela-intenet-e-mail-de-promocao>. Acesso em: 10 jun. 2014.

[34] HERINGER, Carolina e FILHO, Herculano Barreto. *Vazamento de dados de policiais militares será investigado pela DRCI*. Extra Globo.com. Rio de Janeiro, 16 de set. 2013. Disponível em: <http://extra.globo.com/casos-de-policia/vazamento-de-dados-de-policiais-militares-sera-investigado-pela-drci-9972348.html>. Acesso em: 10 jun. 2014.

[35] O GLOBO.COM *Hackers que vazaram dados de PMs serão investigados.* Rio de Janeiro, 15 de set. 2013. Disponível em: < http://oglobo.globo.com/rio/hackers-que-vazaram-dados-de-pms-serao-investigados-9969301>. Acesso em: 10 jun. 2014.

"...verdadeiro estelionato mercadológico para ludibriar o consumidor e impor-lhe a contratação de um serviço de que na verdade ele não precisa..." para concluir, mais adiante, que nesta "máfia da informação privilegiada, é certo que a Oi S.A desempenha a função primordial na empreitada: o vazamento de dados pessoais de seus clientes a empresas provedoras de conteúdo quando tinha o dever de zelar pela integridade e sigilo dos mesmos". A empresa envolvida defendeu-se alegando que "...é vítima de um ardiloso esquema de venda de dados de seus clientes e que está tomando todas as providências ao seu alcance para dar fim a tais práticas"[36]. Como resultado, a Justiça determinou que a empresa cessasse imediatamente qualquer forma de compartilhamento de informações pessoais e de dados cadastrais[37].

O que há de comum nos casos apresentados é que os incidentes de violação de dados, sejam eles intencionais ou não, causaram sérios e profundos danos, de imediato e ao mesmo tempo, aos direitos de milhares de cidadãos demonstrando que estes são vulneráveis diante de sistema informatizado de empresas que deveriam zelar pela manutenção e integridade dos dados pessoais de seus clientes. Outro ponto em comum é que apesar da existência de relatórios informando que as empresas estão investindo em segurança da informação, este investimento parece representar apenas poucas empresas e não a grande maioria. Por fim, e não menos importante, é que grandes ou pequenas as empresas afetadas se colocam no papel de vítimas antes mesmo da apuração dos motivos da violação de dados – mesmo sabendo que os incidentes de violação podem ter sido causados por falhas humanas, de empregados ou terceirizados responsáveis pela segurança dos bancos de dados de clientes. Ademais, a reparação dos direitos dos usuários ou consumidores lesados implica em processos judiciais lentos e tumultuosos e com resultados não desejados e nem plenamente satisfatórios.

Ainda, outra questão pode se apresentar de extrema complexidade: para o técnico as violações de dados podem ser consideradas falhas banais, de sistemas ou humanas, pois o que causa alvaroço não é a violação dos dados em si e sim o volume dos dados vazados[38]. Assim, como deverão ser analisados, juridicamente, estes erros humanos? Do ponto de vista

---

[36] BRASIL. Ministério Público Federal. *Procuradoria da República em Mato Grosso do Sul. MPF/MS descobre "estelionato mercadológico" e vazamento de dados sigilosos de clientes da Oi em todo o país devem ser interrompidos*. Disponível em < http://www.prms.mpf.mp.br/servicos/sala-de-imprensa/noticias/2013/08/mpf-ms-descobre-201cestelionato-mercadologico201d-e-vazamento-de-dados-sigilosos-de-clientes-da-oi-em-todo-o-pais-devem-ser-interrompidos>. Acesso em: 10 jun. 2014.

[37] FREITAS, Andrea. *Justiça manda Oi suspender vazamento de dados de clientes*. Globo.com. Rio de Janeiro, 9 de agosto de 2013. Disponível em: < http://oglobo.globo.com/economia/defesa-do-consumidor/justica-manda-oi-suspender-vazamento-de-dados-de-clientes-9442393>. Acesso em: 10 jun. 2014.

[38] CARNUT, Marco. *A banalidade dos vazamentos de dados pessoais*. Tempest.blog. [s.l.]. Disponível em <http://blog.tempest.com.br/marco-carnut/banalidade-vazamentos-dados-pessoais.html>. Acesso em: 10 jun. 2014.

econômico, social e legal tais violações se constituem em sério transtorno demonstrando ineficiência Estatal vez que expõe a privacidade e dignidade da pessoa humana; afinal, esses conceitos são direitos fundamentais que devem ser protegidos de forma preventiva, eficiente e eficáz.

Diante de tal situação desponta a problemática: que instrumentos legais e políticos - de indução, punição e proteção – que o Estado possui para promover, **preventivamente**, a funcionalização do direitos do cidadão em caso de violação de seus dados pessoais?

Danos Colaterais: o ferimento aos direitos fundamentais da privacidade e da dignidade humana

Zygmunt Bauman[39] conseguiu dar nova conotação à expressão "danos colaterais" ao trazê-la do vocabulário das forças armadas e incorporá-la na sociedade líquido-moderno. Segundo o autor danos colaterais significam os desfavorecidos naquela sociedade que tem um olho no lucro e outro no consumo.

De forma idêntica, a violação de dados, como demonstrado nos exemplos citados, se constitui em dano colateral porque representa a liquefação de direito fundamental da privacidade, da dignidade humana e o de decidir quais informações devem ser preservadas e quais as que podem ser publicadas. No caso do já mencionado incidente envolvendo a violação e exposição de dados pessoais de mais de 50 mil policiais do Estado do Rio de Janeiro, resta evidente que a vida de cada um daqueles policiais se encontra em risco, assim como de seus familiares. Atuar de forma tardia, e não de forma preventiva, de nada adiantará para quem, em razão daquela e outras violações de dados, vier a perder um pai, irmão, familiar, parte ou todo um patrimônio.

Em razão disso importa rever e frisar a importância da privacidade e da dignidade humana, enquanto direitos fundamentais, como danos colaterais decorrentes da violação de dados pessoais.

Conceituar a privacidade não é tarefa fácil. Parafraseando expressão de Rosa Nery "a palavra guarda, em si, uma *ambiguïté admirable*"[40] podendo representar conforme a cultura e o sistema político e legal de cada povo, tanto na doutrina internacional quanto na pátria, um significado ou outro dependendo dos interesses envolvidos "...sob os ditames da privacidade,

---

[39] BAUMAN, Zygmunt. *Danos colaterais: desigualdades sociais numa era global.* Tradução Carlos Alberto Medeiros. Rio de Janeiro:Zahar, 2013

[40] NERY, Rosa Maria de Andrade. *Introdução ao pensamento jurídico e à teoria geral o direito privado*. São Paulo: Editora Revista dos Tribunais, 2008, p. 13

protegem-se outros interesses, como *personal autonomy, emotional release, self-evaluation* e *limited and protected communicatios*"[41] com cujo ponto Danilo Doneda acresce:

> A profusão de termos utilizados pela doutrina brasileira para representá-la, propriamente ou não, é considerável; além de 'privacidade' propriamente dito, podem ser lembrados os termos: vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada, e outros menos utilizados, como 'privatividade' e privaticidade', por exemplo. O fato da doutrina estrangeira apontar igualmente para uma multiplicidade de alternativas certamente contribui, induzindo juristas brasileiros a experimentar diversas destas. [42]

Ilton Filho explica esse paradoxo, na sociedade pós-moralista e hipermoderna, por meio da análise do público e do privado levada a cabo por Hannah Arendt do período antigo até o contemporâneo, concluindo que tal fato possui raiz histórica: "A história da tutela jurídica da personalidade humana e da intimidade começa com as revoluções americanas e francesa, momento em que os indivíduos exigem a concretização dos direitos naturais, agora designados como direitos humanos"[43] salientando, no entanto, que foi apenas no final do século XIX, com a publicação do artigo *The right to privacy,* que o direito à vida privada e a intimidade começa a ter uma delimitação razoavelmente precisa e passa a ser tutelado juridicamente[44]. Danilo Doneda[45] vai mais além, afirmando que é a partir deste momento que a linha evolutiva da doutrina do direito à privacidade tem início.

Resta evidente, assim, que enquanto a sociedade confiou em sistemas onde a pessoa humana não era a preocupação central não havia porque falar em privacidade – posição essa que começou a se modificar a partir do momento em que surgiram os primeiros conceitos da importância da dignidade da pessoa humana na sociedade civil.

De fato, Silveira e Rocasolano lecionam que "Na Antiguidade, os conceitos de liberdade, cidadania, personalidade e democracia – se existiam – possuíam um sentido diferente do que têm hoje, e os direitos a eles inerentes eram desconhecidos pela maior parte da humanidade"[46]. Ainda segundo aqueles autores a história dos direitos humanos é dividida em três períodos nos quais:

> [...] é possível observar o nascimento das sucessivas *gerações* de direitos humanos, que evoluíram conforme a sociedade se transformava. São elas: (1) os direitos de

[41] WESTIN, Alan. *apud* VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação*. Porto Alegre: Sergio Antonio Fabris Ed., 2007.
[42] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 101.
[43] FILHO, Ilton Norberto Robl. *Direito, Intimidade e Vida Privada: Paradoxos Jurídicos e Sociais na Sociedade Pós-Moralista e Hipermoderna*. Curitiba: Juruá, 2010, p. 124.
[44] Idem, op.cit., p. 148
[45] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 8
[46] SILVEIRA, Vladmir Oliveira da. ROCASOLANO. Maria Mendez. *Direitos Humanos: conceitos, significados e funções*. São Paulo: Saraiva, 2010, p. 112.

> *Primeira Geração*, que aclamam as liberdades civis e os direitos políticos, e são também chamados "Direitos de Liberdade", de autonomia ou de participação; (2) os direitos de *Segunda Geração*, denominados "Direitos de Igualdade" ou prestacionais, compreendendo os direitos sociais, econômicos e culturais; e (3) os "Direitos dos Povos", que marcam a Terceira Geração de direitos humanos, e que correspondem aos ditos direitos difusos ou da solidariedade (fraternidade).[47]

Como os direitos de primeira geração são também chamados de Direitos de Liberdade deve-se então compreender que "Privacidade e liberdade se amalgamam como duas forças de uma mesma moeda, uma vez que tão-somente o manto da proteção da privacidade proporciona a um indivíduo o direito ao exercício da liberdade"[48].

Aos direitos da primeira geração foram acrescidos novos direitos sendo correto afirmar que ao lado daquelas conquistas novos valores morais e culturais também foram acrescidos como condição natural do desenvolvimento da individualidade dificultando, consequentemente, a conceituação de privacidade.

Nesta trilha, Ilton Filho salienta que enquanto no sistema anglo-saxão foi adotado o *common law*, onde a fonte do direito é a jurisprudência, no direito continental europeu foi adotado outro sistema tendo como marco a Revolução Francesa; já na Alemanha a proteção à personalidade humana teve como pressuposto as peculiaridades de suas condições políticas onde a discussão versa sobre a existência de um direito natural específico: o direito geral da personalidade[49] - e em ambos sistemas a conceituação de privacidade é complexa como Marcel Leonardi, com clareza ímpar, deixa evidente vez que envolvido, como dito alhures, diferenças culturais de cada povo:

> [...] o problema não se reduz a uma dicotomia entre o modelo da Civil Law e o da Common Law: ainda que existam diferenças substanciais entre o modelo de privacidade romano-germânico (que adota como principal fundamento a dignidade) e o modelo de privacidade (que adota como principal fundamento a liberdade), não se pode perder de vista que, mesmo entre os sistemas de Common Law do Reino Unido e dos Estados Unidos, há diferenças significativas entre o âmbito de proteção do direito à privacidade. Além disso, ainda que o direito europeu caminhe, por meio de diversas diretivas relacionadas à privacidade, para uma uniformização relativa – ao menos no que tange aos padrões mínimos de proteção – há importantes diferenças culturais entre os países-membros da União Européia, as quais influenciam, por óbvio, a transposição desses padrões mínimos no direito interno de cada nação. [50]

---

[47] Idem, op. cit. p. 112.

[48] VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação*. Porto Alegre: Sergio Antonio Fabris Ed., 2007, p. 27.

[49] FILHO, Ilton Norberto Robl. *Direito, Intimidade e Vida Privada: Paradoxos Jurídicos e Sociais na Sociedade Pós-Moralista e Hipermoderna*. Curitiba: Juruá, 2010, p. 154-165.

[50] LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2012, p. 49-50

Hodiernamente as novas tecnologias da informação e comunicação (TIC's) produziram – e ainda irão produzir – profundas mudanças sociais e culturais como bem ponderado por Ruy de Queiroz[51]:

> A verdade é que, para o jovem ou adolescente contemporâneo, as novas mídias propiciam um novo ponto de encontro para suas práticas íntimas, ponto esse que permite que a intimidade se torne ao mesmo tempo mais pública e mais privada. O jovem pode se encontrar, flertar, namorar, tudo isso fora do alcance da vigilância de pais e adultos, ao mesmo tempo em que tudo se passa à vista de seus amigos online [...] Entretanto, um estudo recente do Berkman Center for Internet and Society, Harvard ("Youth, Privacy and Reputation - Literature Review", por Alice E. Marwick, Diego Murgia-Diaz e John G. Palfrey Jr., Abr 2010), baseado numa detalhada análise da literatura sobre o tópico, conclui que o jovem tem sim uma grande preocupação com sua privacidade, sobretudo com relação a pais e professores terem acesso a suas informações pessoais. Segundo os autores, o jovem de hoje já é intensamente vigiado em casa, na escola e em público por uma gama de tecnologias de monitoração, mas que tanto as crianças quanto os adolescentes desejam manter íntegros e protegidos seus próprios espaços de socialização, exploração e experimentação, longe dos olhos dos adultos. A disponibilização online de conteúdo pessoal faz parte do processo de auto-expressão, de conexão com os pares, de socialização e crescimento da popularidade, e da própria ligação com amigos e membros de grupos de pares.

E a realidade suplantará a ficção produzindo outras gerações de direitos, ou novos direitos, como bem observado por Norberto Bobbio[52]:

> Ao lado dos direitos sociais, que foram chamados de direitos de segunda geração, emergiram hoje os chamados direitos de terceira geração, que constituem uma categoria, para dizer a verdade, ainda excessivamente heterogênea e vaga, o que nos impede de compreender do que efetivamente se trata. O mais importante deles é o reivindicado pelos movimentos ecológicos: o direito de viver num ambiente não poluído. Mas já se apresentam novas exigências que só poderiam chamar-se de direitos de quarta geração, referentes aos efeitos cada vez mais traumáticos da pesquisa biológica, que permitirá manipulações do patrimônio genético de cada indivíduo. Quais são os limites dessa possível (e cada vez mais certa no futuro) manipulação?

O que resultará, evidentemente, no aumento da complexidade jurídica do conceito de privacidade que tenderá a ficar cada vez mais difuso seja porque "ninguém parece ter uma ideia clara do que ele é"[53] ou porque "possui um sentido emotivo e ao mesmo tempo tão vago que, ainda que utilizada pelo ordenamento, não está ela definida, daí os problemas que se colocam na análise do assunto"[54] o que poderá gerar decisões judiciais conflitantes:

---

[51] QUEIROZ, Ruy de. *A evolução do conceito de privacidade*. Instituto Brasileiro de Direito da Informática. Disponível em http://www.ibdi.org.br/site/artigos.php?id=230. Acesso em: 10 jun. 2014.

[52] BOBBIO, Norberto. *A era dos direitos*. Tradução Carlos Nelson Coutinho; apresentação de Celso Lafer. Nova ed. Rio de Janeiro:Elsevier, 2004, 7ª reimpressão, p. 9.

[53] THOMSON, Judith Jarvis. Apud LEONARDI, Marcel. *Tutela e Privacidade na Internet*. São Paulo: Saraiva, 2012. p. 48

54 GASPARIAN, Tais. Apud LEONARDI, Marcel. *Tutela e Privacidade na Internet*. São Paulo: Saraiva, 2012. p. 48

> [...] como não se tem um indicativo constitucional ou legal da extensão desse direito, pode haver um tratamento diferenciado pelas cortes judiciárias, variando largamente de acordo com o contexto social e político em que se discutam questões ligadas à privacidade; como as circunstâncias em que esse tema terá implicado podem variar largamente, fica difícil prever o resultado das lides em cada caso concreto, sendo, ao contrário, fácil prognosticar uma tendência ao desencontro de decisões judiciais, um obstáculo frente à harmonização jurisprudencial.[55]

Não obstante as diferenças culturais Marcel Leonardi informa que mesmo as tentativas de conceituação da privacidade na forma unitária, que segue o método pelo gênero próximo e diferença específica, acabam falhando porque ou se produz conceitos excessivamente restritivos ou excessivamente abrangentes destacando-se, dentre estes, o direito de ser deixado só, o de resguardo contra interferências alheias, o de segredo ou sigilo e o de controle sobre informações e dados pessoais[56].

Consequentemente, considerando que o conceito de privacidade possui ampla multiplicidade de interesses envolvidos que compartilham "...semelhanças de família entre si, que se sobrepõem e se entrecruzam mutuamente..."[57] e que "...parece haver um consenso doutrinário e jurisprudencial a respeito da necessidade de sua tutela do modo mais amplo possível, ante a caracterização da privacidade como um direito de personalidade e como um direito fundamental, cuja base é o princípio da dignidade da pessoa humana, consagrada pela Constituição Federal de 1988..."[58] conclui-se pelo acerto de Danilo Doneda[59] ao afirmar que "A privacidade assume, então, um caráter relacional, que deve determinar o nível de relação da própria personalidade com as outras pessoas e com o mundo exterior – pela qual a pessoa determina sua inserção e exposição".

Assim, adotando-se a mesma definição que Stefano Rodotà dá à privacidade como sendo "o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada" na qual "...a informação (mais precisamente as informações pessoais) coloca-se como elemento objetivo..."[60] conclui-se, forçosamente, que as violações de dados pessoais e sua exposição colocam por terra todas as conquistas travadas durante séculos na busca da privacidade e da dignidade humana impondo-se, portanto, sua mais ampla defesa de forma proativa.

---

55 FILHO, Demócrito Ramos Reinaldo. Apud LEONARDI, Marcel. *Tutela e Privacidade na Internet.* São Paulo: Saraiva, 2012. p. 47-48

56 LEONARDI, Marcel. *Tutela e Privacidade na Internet.* São Paulo: Saraiva, 2012. p. 49-78

57 Idem, op. cit. p. 89.

58 Idem, op. cit. p. 90.

59 DONEDA, Danilo. *Da Privacidade à proteção de dados pessoais*. Renovar. Rio de Janeiro, São Paulo, Recife, 2006, p. 146

60 Idem, op. cit. p. 147

O direito e o princípio da eficácia

Os Centros de Segurança e Resposta a Incidentes (CSIRT's) existentes no Brasil, neles incluído o CTIR Gov, destinam-se basicamente às notificações dos incidentes, às análises correspondentes, ao suporte, recuperação e resposta aos incidentes, distribuição de alertas, recomendações e elaboração de estatísticas, além de oferecer treinamentos, conscientização e análise de tendências de ataques. Seja como for esses centros não se revestem de órgãos reguladores com poderes suficientes e específicos que possam obrigar as empresas nacionais e as sediadas no Brasil a seguirem, obrigatoriamente, determinadas normas legais e de procedimentos como, por exemplo, a comunicação obrigatória à sociedade ou ao órgão específico das notificações de violações de dados ocorridas em seus sistemas, no prazo de cinco (5) dias após a ocorrência do incidente, por se tratar de fato relevante para a sociedade, aos usuários e aos consumidores; o de determinar a obrigatoriedade de informar ao público ou a órgão competente as medidas adotadas no caso da violação de dados; a obrigatoriedade de utilização de softwares e programas de última geração para a prevenção contra a violação de dados; a criação de um cadastro positivo das empresas que aderirem ao programa de prevenção de dados e sua divulgação aos usuários e consumidores de modo a incrementar os negócios; autorização e registro de empresas terceirizadas que cuidam e tratam dos bancos de dados e assim por diante.

Também falta àqueles centros o poder de receber e processar, administrativa ou legalmente, as reclamações de usuários que se sentirem violados nos seus direitos de proteção aos dados pessoais; o poder de fiscalizar e realizar investigações; enfim, todos aqueles poderes que, preventivamente, possam minimizar a violação dos dados pessoais.

Ao contrário do desejável, no Brasil a proteção de dados pessoais dá-se de forma tardia, ou seja, quando o dano já foi perpetrado conforme se verifica da análise da vasta legislação existente e compilada no **Quadro da legislação relacionada à segurança da informação e comunicações**, existente no sitio eletrônico do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República[61]. Este fato fica evidente no Recurso Ordinário em Mandado de Segurança julgado pela 5ª Turma do Superior Tribunal de Justiça que, ao analisar pedido de exclusão de dados relativos a inquérito policial arquivado, assim entendeu:

---

[61] BRASIL. *Quadro da legislação relacionada à segurança da informação e comunicações*. Atualizado em 13/09/2013. Disponível em < http://dsic.planalto.gov.br/documentos/quadro_legislacao.htm>. Acesso em: 10 jun. 2014.

> RECURSO ORDINÁRIO EM MANDADO DE SEGURANÇA. PROCESSUAL PENAL. REGISTROS DE INSTITUTO DE IDENTIFICAÇÃO CRIMINAL. PEDIDO DE EXCLUSÃO DE DADOS RELATIVOS A INQUÉRITO POLICIAL ARQUIVADO. SIGILO GARANTIDO PELAS INSTÂNCIAS ORDINÁRIAS. ACESSO FACULTADO SOMENTE AO PODER JUDICIÁRIO. AUSÊNCIA DE DIREITO LÍQUIDO E CERTO. RECURSO DESPROVIDO.
> ...
> 5. Eventual vazamento indevido das informações sigilosas reclama pela apuração dos responsáveis e pela aplicação das penalidades cíveis, administrativas e criminais cabíveis, sendo impossível acolher a tese de que, diante das novas ferramentas tecnológicas e das notórias violações aos dados confidenciais observadas na experiência, os dispositivos legais aplicáveis tornaram-se obsoletos, a recomendar uma postura ativa do judiciário.[62]

Dois aspectos de interesse chamam a atenção na ementa: de um lado, o reconhecimento da não existência de uma legislação específica, preventiva e proativa em favor da proteção dos dados pessoais e, de outro, a necessidade de instauração de novo processo para apurar eventuais responsabilidades depois do fato ocorrido – engessando o Poder Judiciário e criando obstáculos à sua eficiência, eficácia, efetividade e sustentabilidade.

Para Irene Patrícia Nohara[63] "...só a eficácia é um conceito de apuração mais singela, pois tanto a eficiência como a efetividade devem acoplar em seus sentidos dimensões de proporcionalidade em função dos fins que queiram alcançar..."; assim, segundo a autora para que a sustentabilidade possa ser realizada é necessário que se tenha, concomitantemente, os princípios da eficiência, eficácia e efetividade – o que, no caso da ementa retro citada não ocorreu demonstrando que os mencionados conceitos não integraram a decisão.

Outra questão de interesse é o de saber se a proteção quanto à violação de dados pessoais está garantida só porque a lei assim o diz ou porque, no caso de sua violação, existem instrumentos capazes de buscarem a reparação dos danos.

O inciso III do artigo 3º da Lei 12.965, de 23 de abril de 2014, que estabelece os princípios, garantias e deveres para o uso da Internet no Brasil, conhecida anteriormente como Marco Civil da Internet, dispõe que:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> ...
> III - proteção dos dados pessoais, na forma da lei;

Considerando que a referida lei trata de princípios, o dispositivo legal retro transcrito peca ao remeter o cidadão à legislação existente ***após o fato danoso*** para a apuração e

62 BRASIL. STJ - RMS 42972 / SP - Recurso Ordinário em Mandado de Segurança - 2013/0184882-8. Relatora Min. Laurita Vaz, 5ª T. Data do julgamento: 22/04/2014. Data da publicação: 30/04/2014. DJe. Disponível em <https://ww2.stj.jus.br>. Acesso em: 10 jun. 2014.

63 NOHARA, Irene Patricia. *Reforma Administrativa e Burocracia: impacto da eficiência na configuração do direito administrativo brasileiro*. São Paulo: Atlas, 2012, p. 196

reparação dos danos causados como, aliás, foi expressa a ementa já colacionada, enquanto que o ideal seria uma atuação ***preventiva*** à ocorrência do fato danoso.

A ideia de prevenção, que fique bem claro, não tem por objetivo evitar a violação de dados – o que sempre acabará ocorrendo tendo em vista a evolução da tecnologia e dos erros humanos – e sim o de minimizar os incidentes de violação de dados por meio de adoção de política específica de segurança pública da informação e proteção de dados pessoais, seja por meio de promulgação de lei específica ou por meio de órgão regulador de forma a se atingir todos os princípios constitucionais e aqueles elencados nas diversas leis existentes.

Em entrevista divulgada pelo Portal IDG Now sobre a Lei 12.965, de 23 de abril de 2014, Danilo Doneda[64] esclareceu que os conceitos de privacidade e de proteção de dados são distintos uma vez que enquanto o primeiro é subjetivo, impedindo uma resposta clara, o segundo é objetivo visando proteger a pessoa e exigindo regras claras e específicas para esta proteção. Ainda segundo a entrevista, aquele jurista informou sobre a necessidade da existência de uma legislação específica que deva funcionar como uma legislação geral de proteção de dados pessoais "...em uma mensagem clara de que as empresas e os próprios governos têm que arcar com a responsabilidade de proteção de algo que é muito importante para o cidadão..." para concluir, mais adiante, que "...não é um problema somente de direito do consumidor [...] é necessário estender a garantias a [sic] de proteção de dados pessoais para o cidadão em todas as relações onde seus dados estejam expostos, sejam relações perante o serviço público, segmentos econômicos ou entes não econômicos...".

ELER e SAMPAIO, em artigo publicado no Conpedi de 2013, deixaram assente que:

> A proteção de dados constitui, atualmente, um dos aspectos mais significativos da liberdade individual. Tendo isso em vista, objetiva o artigo fornecer instrumentos valorativos para que o tratamento de dados pessoais considere o novo conceito integral de pessoa, que se manifesta pela sua identidade social e individual; pelo seu corpo físico e eletrônico [...] Contudo, ao lado do acesso aos dados pelas mais variadas tecnologias, sem mitigar a liberdade, toma-se necessário permitir o controle por parte do cidadão, chegando-se, assim, ao equilíbrio desejável que privilegia a dignidade da pessoa humana.[65]

Tal manifestação demonstra cabalmente a necessidade de nova visão sobre a proteção de dados pessoais, conforme leciona Paulo Lima:

---

[64] *O Marco Civil e a proteção de seus dados pessoais – o que muda?* IDGNow! Circuitodeluca. [s.l], 29 de abril de 2014. Disponível em < http://idgnow.com.br/blog/circuito/2014/04/29/o-marco-civil-e-a-protecao-dos-seus-dados-pessoais-o-que-muda/>. Acesso em: 10 jun. 2014.

[65] ELER, Kalline Carvalho Gonçalves; SAMPAIO, Kelly Cristine Baião. *A Garantia da Privacidade na Sociedade Tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana*. In: ROVER, Aires José; FILHO, Adalberto Simão e PINHEIRO, Rosalice Fidalgo (Coord.). Direito e Novas Tecnologias. São Paulo: Funjab, 2013, p. 188. Disponível em < http://www.publicadireito.com.br/publicacao/uninove/livro.php?gt=122>. Acesso em: 10 jun. 2014.

> É claro que essa nova 'Era da Informação' não traz somente vantagens; a segurança das informações armazenadas nos sistemas computadorizados ganha gigantesca importância quando no mundo todo as instituições financeiras passam a fazer toda espécie de transações monetárias com o uso de computadores[1.] Assim, ocorreu aumento significativo dos delitos relacionados com o processamento de dados nas Américas, Europa Ocidental, Austália, Japão, e mesmo em países do antigo bloco socialista. Tais crimes não apresentam perigo tão somente para as empresas privadas, mas também para toda a economia de um país e sua sociedade.[66]

Um exemplo de órgão voltado para a proteção de dados pessoais é o *Office of the Privacy Commissioner* do Canadá, órgão oficial do Parlamento que, com independência e imparcialidade, tem por objetivo garantir os direitos de privacidade dos canadenses e cujos poderes incluem, dentre outros, a investigação de denúncias, realização de auditorias, andamento de ações judiciais, elaboração de relatórios públicos sobre as práticas de manuseio de informações pessoais por organizações públicas e privadas e promoção da consciência pública sobre a compreensão de questões relativas à privacidade.

Dos inúmeros relatórios e publicações do Comissariado destaca-se a seção *OPC Guindance Documents*[67] onde podem ser encontrados manuais sobre proteção de dados pessoais que devem ser observados tanto por pessoas físicas quanto jurídicas. Um dos manuais é o Guia para Empresas e Organizações, atualizado para março de 2014, que foi desenvolvido para ajudar organizações a cumprirem suas responsabilidades de acordo com o Ato de Proteção de Informações Pessoais e Documentos Eletrônicos (PIPEDA) e no qual consta que as pessoas gostam de fazer negócios com organizações que demonstram respeito pelos seus direitos de privacidade lembrando, assim, a ética e responsabilidade social que devem pautar as relações empresariais o que permite competitividade e oportunidade de novos negócios. Os cidadãos canadenses podem efetuar reclamações diretamente pela Internet ao Comissariado se entenderem que seus dados pessoais foram violados[68].

Conclusão

De acordo com os relatórios e estatísticas apresentadas comprovou-se que as violações de dados estão ocorrendo de forma crescente em todo o globo, inclusive no Brasil -

---

[66] LIMA, Paulo Marco Ferreira. *Crimes de Computador e Segurança Computacional*. 2ª ed., São Paulo: Atlas, 2011, p. XII

[67] INTERNACIONAL. Office of The Privacy Commissioner Of Canada. Reports and Publications. *A Guide for Businesses and Organizations: Privacy Toolkit: Canada's Personal Information Protection and Electronic Documents Act*. April 16, 2014. Disponível em <http://www.priv.gc.ca/information/pub/gd_index_e.asp>. Acesso em: 19 abr. 2014

[68] INTERNACIONAL. Office of The Privacy Commissioner Of Canada. *To file a complaint under the* Privacy Act. Disponível em < http://www.priv.gc.ca/complaint-plainte/pa_e.asp>. Acesso em: 19 abr. 2014. *To file a complaint under the* Personal Information Protection and Electronic Documents Act *(PIPEDA)*. Disponível em < http://www.priv.gc.ca/complaint-plainte/pipeda_e.asp>. Acesso em: 19 abr. 2014

onde cidadãos estão preocupados com a exposição de seus dados pessoais. Também restou demonstrado que o valor da informação corresponde a 50% (cinquenta por cento) do valor de mercado das organizações e que a perda irremediável das mesmas representa a perda de 55% de clientes; 50% de danos à marca; 40% de redução na receita e 32% em multas – todavia, as violações continuam ocorrendo demonstrando que os investimentos em segurança da informação com relação aos dados pessoais não são satisfatórios ou que poucas empresas é que realizam, efetivamente, tais investimentos.

Quanto ao cidadão restou comprovado sua vulnerabilidade social em relação à proteção de dados pessoais e a omissão do Estado na defesa e proteção desse direito.

Também restou demonstrado não existir no Brasil legislação específica para tanto e nem órgão regulador que possa exercer uma política de segurança pública da informação para a proteção de dados pessoais de forma preventiva; ao contrário, que caberá ao cidadão buscar seus direitos na Justiça após a efetivação dos danos havendo inversão, assim, nos conceitos de eficiência, eficácia, efetividade e sustentabilidade da Administração Pública.

Em conclusão, se de um lado restou evidente a potencialidade ofensiva da violação de dados pessoais do cidadão, de outro, restou comprovado a relevância social, econômica, política e jurídica do Estado em atuar com mais eficiência e eficácia na defesa preventiva dos direitos fundamentais do cidadão quanto à proteção de seus dados pessoais.

Referências

BARBOSA, Alexandre F. (Coord.). Tradução:Karen Brito Sexton. *Pesquisa sobre o uso das Tecnologias de Informação e Comunicação no Brasil: TIC Educação 2010*. São Paulo: Comitê Gestor da Internet no Brasil, 2011. Disponível em < http://op.ceptro.br/cgi-bin/cetic/tic-educacao-2010.pdf>.

_____ *Pesquisa sobre o uso das tecnologias de informação e comunicação no Brasil: TIC Educação 2012*. São Paulo: Comitê Gestor da Internet no Brasil, 2013. Disponível em < http://www.cetic.br/publicacoes/2012/tic-educacao-2012.pdf>.

BARRETO, Aldo de Albuquerque. *A eficiência técnica e econômica e a viabilidade de produtos e serviços de informação.* Ciência da Informação - Vol 25, número 3, 1996 – Artigos. Disponível em < http://revista.ibict.br/ciinf/index.php/ciinf/article/viewFile/466/425>.

BAUMAN, Zygmunt. *Danos colaterais: desigualdades sociais numa era global.* Tradução Carlos Alberto Medeiros. Rio de Janeiro:Zahar, 2013

BITCOIN - Disponível em <https://bitcoin.org/pt_BR/>.

BOBBIO, Norberto. *A era dos direitos*. Tradução Carlos Nelson Coutinho; apresentação de Celso Lafer. Nova ed. Rio de Janeiro: Elsevier, 2004, 7ª reimpressão.

CANALTECH CORPORATE. *Investimento em segurança da informação subiu 51% em 2013*. [s.l.], 13 de dez. de 2013. Disponível em < http://corporate.canaltech.com.br/noticia/seguranca/Investimento-em-seguranca-da-informacao-subiu-51-em-2013/ >.

_____. *A onda dos "mega" vazamentos de dados*. Disponível em < http://canaltech.com.br/coluna/seguranca/A-onda-dos-mega-vazamentos-de-dados/#ixzz32uA0HkyN>.

_____. *Relembre os maiores vazamentos de informação de 2013*. Disponível em < http://corporate.canaltech.com.br/materia/seguranca/Relembre-os-maiores-vazamentos-de-informacao-de-2013/>.

CARNUT, Marco. *A banalidade dos vazamentos de dados pessoais*. Disponível em <http://blog.tempest.com.br/marco-carnut/banalidade-vazamentos-dados-pessoais.html>.

CISCO. *Tráfego global de dados móveis crescerá 11 vezes entre 2013 e 2018 segundo o Relatório Cisco VNI*. Arquivo de Notícias 2014. Cisco. [s.l.], [s.d.]. Disponível em <http://www.cisco.com/web/PT/press/articles/2014/20140205.html>.

CERT.BR – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em < http://www.cert.br>.

CERT.PT – Portugal. Serviço de Resposta a Incidentes de Segurança Informática. Disponível em < http://www.cert.pt/index.php/servicos/tratamento-de-incidentes>.

CONDEIXA, Fábio. *A espionagem no Direito brasileiro*. Jus Navigandi, Teresina, ano 17, n. 3371, 23 set. 2012. Disponível em: <http://jus.com.br/artigos/22668>.

CTIR Gov - Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR Gov). Disponível em < http://www.ctir.gov.br/sobre-CTIR-gov.html>.

CVM. *Instrução cvm nº 358*, de 03 de JANEIRO de 2002. Disponível em < http://www.cnb.org.br/CNBV/instrucoes/ins358-2002.htm>.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 101.

DORIA, Pedro R., 1995 *apud* AQUINO, Leonardo Gomes de. *Direito & Internet: Uma Questão de Congruência*. Conteúdo Jurídico. Brasilia-DF: 24 abr. 2009. Disponível em: <http://www.conteudojuridico.com.br/?artigos&ver=2.22546>.

ECOFINANÇAS. *Target: Empresa demite CEO após vazamento de dados*. Disponível em < http://www.ecofinancas.com/noticias/target-empresa-demite-ceo-vazamento-dados>.

ELER, Kalline Carvalho Gonçalves; SAMPAIO, Kelly Cristine Baião. *A Garantia da Privacidade na Sociedade Tecnológica: um imperativo à concretização do princípio da*

dignidade da pessoa humana. In: ROVER, Aires José; FILHO, Adalberto Simão e PINHEIRO, Rosalice Fidalgo (Coord.). Direito e Novas Tecnologias. São Paulo: Funjab, 2013. Disponível em < http://www.publicadireito.com.br/publicacao/uninove/livro.php?gt=122>.

FILHO, Ilton Norberto Robl. *Direito, Intimidade e Vida Privada: Paradoxos Jurídicos e Sociais na Sociedade Pós-Moralista e Hipermoderna*. Curitiba: Juruá, 2010, p. 124.

FREITAS, Andrea. *Justiça manda Oi suspender vazamento de dados de clientes*. Disponível em: < http://oglobo.globo.com/economia/defesa-do-consumidor/justica-manda-oi-suspender-vazamento-de-dados-de-clientes-9442393>.

FREITAS, Vitor Hugo das dores. *O e-mail profissional enquanto correspondência: a legislação brasileira, a doutrina e jurisprudência sobre a matéria*. Escola Superior de Advocacia da Ordem dos Advogados do Brasil, Seção de São Paulo. São Paulo: 2012.

GONÇALVES, Marcos Rogério; Gouveia, Sônia Mara; Petinari, Valdinéa Sonia. *A Informação como produto de alto valor no mundo dos negócios*. CRB-8Digital, São Paulo, v. 1, n. 1, p. 43-54, jul. 2008. Disponível em < http://revista.crb8.org.br/index.php/crb8digital/article/viewFile/42/43> .

HERINGER, Carolina e FILHO, Herculano Barreto. *Vazamento de dados de policiais militares será investigado pela DRCI*. Extra Globo.com. Disponível em: <http://extra.globo.com/casos-de-policia/vazamento-de-dados-de-policiais-militares-sera-investigado-pela-drci-9972348.html>.

HOUGH, Andrew. *Student 'addiction' to technology 'similar to drug cravings', study finds*. UK. The Telegraph. Disponível via web em < http://www.telegraph.co.uk/technology/news/8436831/Student-addiction-to-technology-similar-to-drug-cravings-study-finds.html>.

ITU. Newsroom. Press Release. *ITU releases 2014 ICT figures. Mobile-broadband penetration approaching 32 per cent Three billion Internet users by end of this year*. Disponível em < http://www.itu.int/net/pressoffice/press_releases/2014/23.aspx#.U9WDnbFiNBm >.

LEO, R. Alan. Harvard Medical Schol. *Writing the Book in DNA*. August 16, 2012. Disponível em < http://hms.harvard.edu/news/writing-book-dna-8-16-12>.

LEONARDI, Marcel. *Tutela e Privacidade na Internet*. São Paulo: Saraiva, 2012, p. 23.

LIMA, Paulo Marco Ferreira. *Crimes de Computador e Segurança Computacional*. 2ª ed., São Paulo: Atlas, 2011.

LITECOIN – Disponível em < https://litecoin.org/pt/>.

LONGHI, João Victor. e BORGES, Gabriel Oliveira de Aguiar. *Marketing cruzado na Internet e publicidade abusiva: a necessária proteção à privacidade do consumidor*. IN: Direito do Consumidor. XXI Congresso Nacional CONPEDI/UNINOVE. São Paulo: Funjab, 2013, Disponível em <http://www.publicadireito.com.br/publicacao/uninove/livro.php?gt=11>.

MATURANA R., Humberto. *Cognição, Ciência e Vida cotidiana*. Organização e tradução: Cristina Magro, Victor Paredes. - Belo Horizonte: Ed. UFMG, 2001.

MINISTÉRIO PÚBLICO FEDERAL. Procuradoria da República em Mato Grosso do Sul. *MPF/MS descobre "estelionato mercadológico" e vazamento de dados sigilosos de clientes da Oi em todo o país devem ser interrompidos*. Disponível em < http://www.prms.mpf.mp.br/servicos/sala-de-imprensa/noticias/2013/08/mpf-ms-descobre-201cestelionato-mercadologico201d-e-vazamento-de-dados-sigilosos-de-clientes-da-oi-em-todo-o-pais-devem-ser-interrompidos>.

MORIMOTO, Carlos E. *Zettabyte (ZB).* Hardware.com.br. [s.l.], 26 de junho de 2005. Disponível em < http://www.hardware.com.br/termos/zettabyte-zb>.

NEGROPONTE, Nicholas. *Vida digital.* Tradução: Sérgio Teralloli; supervisão técnica Ricardo Rangel. São Paulo: Companhia das letras, 1995.

NERY, Rosa Maria de Andrade. *Introdução ao pensamento jurídico e à teoria geral o direito privado*. São Paulo: Editora Revista dos Tribunais, 2008

NOHARA, Irene Patricia. *Reforma Administrativa e Burocracia: impacto da eficiência na configuração do direito administrativo brasileiro*. São Paulo: Atlas, 2012

OABSP. Comissão de Ciência e Tecnologia. Certificados e Assinatura Digital. *Internet, ciberespaço, cibercultura e cibersocialização.* São Paulo: 2013. Disponível em <http://www2.oabsp.org.br/asp/certificadodigital/internet.html>.

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. Reports and Publications. *A Guide for Businesses and Organizations: Privacy Toolkit: Canada's Personal Information Protection and Electronic Documents Act*. April 16, 2014. Disponível em <http://www.priv.gc.ca/information/pub/gd_index_e.asp>. Acesso em: 19 abr. 2014

PERLES, João Batista. *Comunicação: conceitos, fundamentos e história*. Biblioteca on-line de ciências da comunicação. Portugal, [s.d]. Disponível em <http://www.bocc.ubi.pt/pag/perles-joao-comunicacao-conceitos-fundamentos-historia.pdf>

PORTAL DEPENDÊNCIA DE TECNOLOGIA. *Definições: o que é dependência de tecnologia?* [s.l.] [s.d]. Disponível via web em < http://dependenciadetecnologia.org/dependencia-de-tecnologia/definicoes/>.

PORTAL IDGNOW!. *O Marco Civil e a proteção de seus dados pessoais – o que muda?* Disponível em < http://idgnow.com.br/blog/circuito/2014/04/29/o-marco-civil-e-a-protecao-dos-seus-dados-pessoais-o-que-muda/>.

PORTAL IG. *Gasto de empresas com vazamento de dados pode chegar a R$ 9 mi no Brasil.* Economia empresas. Disponível em < http://economia.ig.com.br/empresas/2013-08-13/gasto-de-empresas-com-vazamento-de-dados-pode-chegar-a-r-9-mi-no-brasil.html>.

PORTAL O GLOBO.COM. *Vazamento de 152 milhões de contas de usuário da Adobe pode ter sido o maior da história*. Disponível em < http://oglobo.globo.com/sociedade/tecnologia/vazamento-de-152-milhoes-de-contas-de-usuario-da-adobe-pode-ter-sido-maior-da-historia-10725973>.

_____. *Hackers que vazaram dados de PMs serão investigados.* Disponível em: < http://oglobo.globo.com/rio/hackers-que-vazaram-dados-de-pms-serao-investigados-9969301>.

PORTAL TERRA. *Tráfego de dados na Internet ultrapassará o "zettabyte" em 2016*. [s.l.], 30 de maio de 2012. Disponível em <http://tecnologia.terra.com.br/internet/trafego-de-dados-na-internet-ultrapassara-o-quotzettabytequot-em-2016,024bfe32cdbda310VgnCLD200000bbcceb0aRCRD.html>.

PORTAL RECLAMEAQUI. Disponível em << http://www.reclameaqui.com.br/>.

_____. *Vazamento de dados pessoais pela Internet – E-mail de promoção de ingressos para a Copa 2014*. Disponível em <http://www.reclameaqui.com.br/8664929/ingresso-com/vazamento-de-dados-pessoais-pela-intenet-e-mail-de-promocao>.

PORTAL SEARCHSECURITY. Disponível em < http://searchsecurity.techtarget.com/definition/data-breach>.

PRICEWATERHOUSE. *Pesquisa Global de Segurança da Informação 2014 da PwC.* Disponível em < http://www.pwc.com.br/pt_BR/br/publicacoes/servicos/assets/consultoria-negocios/pesq-seg-info-2014.pdf>.

QUEIROZ, Ruy de. *A evolução do conceito de privacidade*. Instituto Brasileiro de Direito da Informática. Disponível em http://www.ibdi.org.br/site/artigos.php?id=230.
ROCHA, Camilo. *E-mail exibe dados de clientes do site Ingresso.com*. O Estado de São Paulo. Caderno Economia, B14, 14 de mar. 2014. Disponível em < http://estadao.br.msn.com/link/e-mail-exibe-dados-de-clientes-do-site-ingressocom>.

SILVEIRA, Vladmir Oliveira da. ROCASOLANO. Maria Mendez. *Direitos Humanos: conceitos, significados e funções*. São Paulo: Saraiva, 2010.

SYMANTEC**.** *Pesquisa sobre Custo e Gestão da Informação: resultados da América Latina*. Disponível em < http://www.symantec.com/content/pt/br/enterprise/images/theme/state-of-information/2012-SOI-PDF-LAM-PORT-v2.pdf>.

_____. *Estudo da Symantec e Ponemon Institute Revela que Negligência Humana e Erros de Sistema são Responsáveis por Dois Terços dos Vazamentos de Dados.* Disponível em <http://www.symantec.com/pt/br/about/news/release/article.jsp?prid=20130605_01>

_____. *Estudo da Symantec e Ponemon Institute Revela que Negligência Humana e Erros de Sistema são Responsáveis por Dois Terços dos Vazamentos de Dados*. Disponível em <http://www.symantec.com/pt/br/about/news/release/article.jsp?prid=20130605_01>

_____. *Relatório de Ameaças à Segurança na Internet de 2014, Volume 19*. Disponível em < http://www.symantec.com/pt/br/security_response/publications/threatreport.jsp>.

UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa. Disponível em <http://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046>

UNISYS CORPORATION. U*nisys Security Index Tm: Brazil***.** April, 2013. Disponível na Internet via <http://www.unisyssecurityindex.com/usi/brazil>.

VERIZON. *Data Breach Investigations Report Verizon 2014.* Disponível em < http://www.verizonenterprise.com/DBIR/2014/>.

VIEIRA, Tatiana Malta. *O Direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação*. Porto Alegre: Sergio Antonio Fabris Ed., 2007.

WESTIN, Alan. *Apud* VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação*. Porto Alegre: Sergio Antonio Fabris Ed., 2007.