UNIO - *EU Law Journal*. Vol. 4, No. 2, Julho 2018, pp 73-89.
®2018 Centro de Estudos em Direito da União Europeia
Escola de Direito – Universidade do Minho

Desafios do comércio eletrónico no Brasil: integração vertical entre fornecedores e meios de pagamentos, proteção de dados pessoais e cooperação regulatória internacional

Alexandre Veronese*
Marcelo Cunha**

SUMÁRIO: O artigo trata do problema emergente da integração vertical dos meios de pagamento com a oferta dos serviços de venda no comércio eletrónico contemporáneo. É descrito o aumento do comércio eletrónico e são indicados três tipos de riscos aos consumidores: diretos, indiretos e sociais. É indicado que a integração vertical pode oferecer benefícios. Todavia, que essas vantagens potenciais são difíceis de mensurar em face dos riscos. É produzido um modelo de comércio remoto com uma evolução da tipologia de relações de troca, para evidenciar a automatização contemporânea dos processos comerciais. Depois, é indicado que o risco de vazamento de dados pessoais e bancários figura como um problema grave, em razão da integração vertical dos modelos de comércio eletrónico. Para evidenciar o problema, são descritos dois casos internacionais, para demonstrar a dificuldade de combate dos vários países em razão da centralização dos dados pelas empresas. Após isso, é realizada uma avaliação da legislação brasileira para evidenciar a sua limitação em razão da sua falta integração com outros campos da regulação, bem como pela inexistência de previsão de meios de cooperação internacional e sua efetividade. Por fim, a conclusão do artigo indica a necessidade de discutir o panorama do comércio eletrónico integrado com o olhar dirigido para experiências internacionais de proteção de dados pessoais e bancários, bem como dos riscos da internacionalização e da integração vertical.

PALAVRAS-CHAVE: comércio eletrónico – integração vertical – proteção de dados – riscos –Brasil.

---

* Professor de Teoria Social e do Direito [Faculdade de Direito, Universidade de Brasília (UnB)], Doutor em Sociologia pelo Instituto de Estudos Sociais e Políticos (IESP) [Universidade do Estado do Rio de Janeiro (UERJ)], Coordenador do Grupo de Estudos em Direito das Telecomunicações da UnB (GETEL UnB). ORCID: 0000-0002-2287-1005.
** Auditor do Tribunal de Contas da União (Brasil), Mestre em Direito pela Universidade de Brasília (UnB), Pesquisador do GETEL UnB. ORCID: 0000-0001-9631-8256.

I. Introdução[1]

A movimentação por meio de sistemas de pagamento eletrónico é um importante motor das relações de comércio entre os cidadãos e as empresas no mundo contemporáneo.[2] A Internet tem possibilitado o funcionamento do comércio eletrónico em várias formas. Assim, pode haver desde grandes lojas eletrónicas de varejo – Amazon, por exemplo –, até pequenos fornecedores, reunidos em sistemas coletivos – ETSY, por exemplo. Todavia, a quase exclusividade dos pagamentos dessas relações comerciais se dá por meio de sistemas interbancários e, em especial, pela via de cartão de crédito. É certo que apareceram, ainda, novos parceiros eletrónicos, como o sistema Paypal no exterior e o sistema Pag-seguro UOL, no Brasil, ainda baseados em cartões de crédito. Mais recentemente tem ganhado força o movimento de utilização de moedas eletrónicas, como o Bitcoin.[3] [4]

O problema central do presente artigo se dirige à compreensão do marco jurídico aplicável ao comércio eletrónico em face da integração dos sistemas de compra e venda com os meios de pagamento. Para discutir o marco jurídico brasileiro, será necessário tratar da questão da segurança dos dados bancários e da proteção dos dados pessoais. O tema é de especial relevo ao se pensar no risco colocado aos usuários pela possível integração dos fornecedores no comércio pela Internet com os sistemas de pagamento O tema dos riscos e das relações comerciais é indissociável do debate sobre os contratos, como é debatido nos fóruns internacionais que se dedicam a formação de um padrão jurídico transnacional que possa ser aplicado sem sobressaltos às trocas. Assim, o desenvolvimento tecnológico permitiu que a formação de acordos ocorresse cada vez mais de forma remota e, de forma incremental, sem a intervenção direta dos interessados, como expõem Deffains e Jane K. Winn. Os Autores explicam que, nos anos 1980 do século XX, os sistemas de troca começaram a funcionar em tempo real e "foi possível pela primeira vez formar contratos apenas com comunicações entre máquinas".[5] O problema se tornou evidente, uma vez que o avanço tecnológico não veio acompanhado, inicialmente, de uma preocupação regulatória, a qual somente se tornou evidente na década seguinte – 1990 – e frutificou nas primeiras tendências de formar projetos de lei modelo como aquela criada pela UNCITRAL (Comissão das Nações Unidas para o Direito Comercial Internacional) para o comércio eletrónico.

Após este período inicial, as questões começaram a se espraiar para a conjugação de uma discussão que misturava a resolução dos problemas de segurança jurídica

---

[1] Este texto desenvolve algumas das ideias originariamente aventadas no Seminário Internacional "A efetividade do direito em face do poder dos gigantes da Internet", organizado pela Universidade de Brasília (UnB), Universidade Federal Fluminense (UFF), Université Paris Descartes, Université Paris 1 – Panthéon-Sorbonne e Université de Versailles Saint-Quentin-en-Yvelines, entre 13 e 15 de abril de 2016. Os Autores agradecem especialmente ao Professor Dominique Legeais, da Université Paris Descartes, pelo debate então entabulado e que aqui se reflete. Agradecem ainda à Fundação de Apoio à Pesquisa do Distrito Federal (FAPDF), à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e à Embaixada da França no Brasil.

[2] Eric Brousseau, "Commerce électronique: ce que disent les chiffres et ce qu'il faudrait savoir", *Economie et statistique* 339-340 (2000): 147-70.

[3] Jonathan B. Turpin, "Bitcoin: the economic case for a global, virtual currency operating in an unexplored legal framework", *Indiana Journal of Global Legal Studies* 21 (2014): 355-68.

[4] Reuben Grinberg, "Bitcoin: an innovative alternative digital currency", *Hastings Science & Technology Law Journal* 4 (2012): 159-208.

[5] Bruno Deffains e Jane K. Winn, "The effect of electronic commerce technologies on business contracting behaviors", in *Governance, regulations and powers on the Internet*, ed. Eric Brousseau *et al.* (Cambridge: Cambridge University Press, 2012), 345.

– focalizada no debate acerca dos contratos eletrónicos – e de segurança técnica, relacionada com criptografia e sistemas de informação. O atual panorama internacional pode ser descrito pela radicalização de dois cenários. O primeiro é o incremento veloz na formação de cadeias de fornecedores, cujo funcionamento é totalmente eletrónico. Tal cenário possui enorme impacto na expansão das relações comerciais eletrónicas B2B (*business to business*). O segundo cenário é a expansão do comércio eletrónico direto entre pequenos fornecedores, todavia mediado por grandes empresas, havendo grande concentração. Ele poderia ser visto como um comércio C2C (*consumer to consumer*). Não obstante, a dependência dos consumidores de plataformas de intermediação descaracteriza a otimista visão de um potencial comércio de baixo para baixo (horizontal).

No centro desses processos de concentração está a integração vertical dos meios eletrónicos de pagamento com as ferramentas de comércio. A integração vertical possui algumas vantagens, em termos de custos, de segurança e de confiabilidade, relacionadas com o aumento da escala e o potencial de investimento da grande firma. Deste modo, uma plataforma que realize mais transações, em princípio, poderia investir mais em sistemas de segurança, em razão da sua maior margem de lucro. Também, uma grande empresa de intermediação poderia oferecer preços menores aos seus usuários, uma vez que a escala potencialmente baixaria os seus custos. Logo, haveria benefícios potenciais que a integração vertical poderia trazer diretamente aos fornecedores e indiretamente aos usuários. No campo dos benefícios às empresas, elas poderão diminuir os seus custos operacionais, uma vez que desembolsariam menos recursos para pagar pelos serviços dos intermediários, como os operadores de cartões de crédito e sítios eletrônicos de compra. No caso dos usuários, eles poderiam fruir de benefícios indiretos, seja pelo aumento na velocidade das transações, seja pela minoração dos custos e dos seus riscos.

Todavia, não existem potenciais vantagens sem riscos. O primeiro conjunto de riscos é diretamente impingido aos usuários e reside no risco do vazamento de dados pessoais e bancários. Neste artigo serão tratados dois casos internacionais de vazamento em larga escala, que evidenciam o risco do depósito de dados pessoais e bancários em sistemas de armazenagem de fornecedores de serviços e de produtos. Em caso de vazamento, cometido por fraude contra a empresa, o usuário é prejudicado e a sua reparação tem se mostrado muito problemática, já que é muito difícil comprovar a culpa da empresa que, afinal de contas, também é prejudicada pela ação dos fraudadores. O segundo conjunto de riscos é indiretamente atribuído aos usuários e está configurado na ameaça colocada pelo potencial uso indevido dos seus dados bancários e pessoais pelos fornecedores ou intermediários. As informações bancárias – em conjunto com as compras realizadas – podem servir como elemento a ser utilizado pelas empresas para majorar os seus lucros, em operações de marketing dirigido, por exemplo. O terceiro e último conjunto de riscos é imposto à sociedade como um todo e se refere à ameaça que os novos sistemas de compras integradas podem oferecer aos sistemas bancários nacionais e ao direito da concorrência.

Para apreciar esses três conjuntos de riscos, na primeira parte deste trabalho serão analisados a questão criptográfica e o tema da privacidade na Internet, a fim de demonstrar a enorme dificuldade tecnológica e jurídica envolvida no processo de produzir segurança e garantias nas relações sociais e económicas por meio de redes de comunicações que trabalham com protocolos abertos e com interconexão ampla. A conclusão parcial da primeira parte reside no fato de que a confiança social é um ponto central para o bom funcionamento das relações comerciais e que o assunto

precisa de mais atenção jurídica. Na segunda parte do texto serão analisados dois casos internacionais de vazamento de dados bancários, bem como será realizado um paralelo especulativo com a nova conjuntura do tema da privacidade e da criptografia na Internet após o caso Snowden.[6]

A última parte do trabalho focaliza o direito brasileiro, com destaque para a legislação vigente e da sua aplicabilidade em situações de vazamento de dados pessoais e bancários. A análise do direito brasileiro é perpassada por dois pontos. O primeiro se relaciona com os limites da jurisdição nacional para atingir padrões de proteção contra fraudes e contra danos havidos em relações comerciais no mercado global. É indicada a insuficiência do atual marco legal, em especial se comparado com o modelo europeu, baseado na Diretiva 2000/31/CE (comércio eletrônico) e na Diretiva 95/46/CE (proteção de dados pessoais), essa última substituída pelo atual Regulamento Geral sobre a Proteção de Dados (Regulamento 2016/679/UE). O segundo e último tema da conclusão aprecia a possibilidade de cooperação jurisdicional como um modo de efetivar direitos dos cidadãos de outros países e como uma possibilidade regulatória a ser buscada.

II. Privacidade, criptografia e a confiança social

O tema da privacidade dos dados cadastrais e da retenção das informações bancários e de crédito nas compras eletrónicas é central para o desenvolvimento do comércio eletrónico contemporáneo. Esse tema se relaciona diretamente com a criptografia e os seus usos nas trocas comerciais por meio da Internet. É evidente que os sistemas criptográficos estão no centro do debate sobre segurança nas trocas de informação e, portanto, no coração do problema da confiança social, especialmente após a ocorrência do caso Snowden.[7] Na presente secção, iremos tratar inicialmente da evolução dos sistemas de trocas comerciais em geral, para demonstrar que o comércio moderno sempre se baseou em intermediários para poder se realizar. Após essa descrição, chegaremos ao ponto atual, no qual será possível compreender a dificuldade para o estabelecimento de um modo de distribuição de confiança nos novos sistemas eletrónicos de comércio. A questão havia sido considerada como parcialmente resolvida com o uso da criptografia avançada[8] [9]. Contudo, o caso Snowden colocou uma nova agenda de perguntas, em razão da possibilidade de coleta e análise maciça de dados por terceiros, que potencializa o receio das conhecidas práticas de fraude e de violação potenciais na Internet.[10]

Os sistemas bancários nacionais e internacionais possuem regulamentação própria em relação à segurança das transações havidas entre eles e seus clientes, bem como entre os seus sistemas de compensação e de remessas. No caso das transações bancárias, é fácil notar que diversos sistemas bancários nacionais têm investido em criptografia para viabilizar o aumento de confiança nas transações realizadas por clientes, como

[6] Bernard Benhamou, "La gouvernance de l'internet après Snowden", *Revue Politique Étrangère* 79 (2014):14-30.

[7] Regina Connolly, "Trust in commercial and personal transactions in the digital age" in *The Oxford handbook of Internet studies*, ed. William H. Dutton (Oxford: Oxford University Press, 2014): 262-82.

[8] Ramnath K. Chellappa e Paul A. Pavlou, "Perceived information security, financial liability and consumer trust in electronic commerce transactions", *Logistics Information Management* 15 (2002): 358-68.

[9] Pauline Ratnasingham, "The importance of trust in electronic commerce", *Internet Research* 8 (1998):313-21.

[10] Markus Jakobsson (ed.), *The death of the Internet* (New Jersey: John Willey & Sons, 2012).

bem indica a narrativa de Autores canadianos.[11] Tais Autores mencionavam em 2007 que havia a necessidade de maior regulamentação jurídica dos sistemas de comércio do Québec para dotar os consumidores de segurança em relação aos bancos locais. Em especial, indicavam a fragilidade dos sistemas jurídicos das províncias canadianas em relação aos sistemas internacionais para outorgar mais segurança aos usuários bancários locais de modo a majorar o sentimento de confiança. No cerne, a preocupação estava dirigida ao diagnóstico de que o setor bancário no Canadá estaria pouco interessado em favorecer tal desenvolvimento. Para cotejar sua hipótese, os Autores frisavam que os sistemas internacionais de compensação (BIC/SWIFT) – os quais funcionam como um cadastro mundial de bancos e de relações bancárias[12] [13] – estavam se utilizando de métodos de criptografia de chaves públicas com bastante sucesso e que tal sistema deveria ser utilizado no Canadá de forma generalizada. No caso brasileiro, a solução se deu pelo mesmo caminho técnico. A infraestrutura de chaves públicas (ICP-Brasil), mantida pelo Instituto Nacional de Tecnologia da Informação (ITI), se mostra um ferramenta adequada ao uso do setor bancário brasileiro, que tem investido muitos recursos ao longo de anos em informatização dos seus sistemas de comunicação.[14]

De qualquer forma, o foco do presente texto não é propriamente analisar a atuação dos sistemas bancários e dos demais operadores financeiros em suas funções usuais. O ponto central do presente trabalho é apreciar em que medida há risco de que os dados bancários – e de cartões de crédito – dos consumidores sejam manejados por terceiros (comerciantes ou sistemas eletrónicos) no âmbito de operações comerciais. O objetivo do modelo abstrato que será trabalhado é evidenciar a importância do papel do intermediário nas transações comerciais e entender o paradigma atual, no qual as inovações do comércio eletrónico evidenciam os três conjuntos de riscos, mencionados na introdução – riscos diretos, riscos indiretos e riscos sociais. Será construído um modelo com três tipos básicos de relações comerciais de consumo de caráter remoto. Os tipos são abstratos e apenas buscam apenas evidenciar a complexidade das práticas comerciais contemporâneas.

O primeiro tipo de compras remotas é o antigo sistema de consumo por meio de catálogos, no qual os pedidos eram realizados por meio postal ou por meio telefónico. Naquele tipo, os catálogos traziam listagens de produtos e serviços que podiam ser requisitados e pagos por variados modos de pagamento. O consumidor acessava o catálogo de produtos e os adquiria por meio de um cheque postal (ou, bancário) ou, ainda, por meio de um depósito bancário prévio. A antiga aquisição de livros estrangeiros, em um passado remoto, no Brasil, se dava desta forma. O consumidor entrava em contato diretamente com um livreiro ou com editor de outra cidade, fosse do Brasil, fosse do exterior, e encomendava o livro desejado. Outra forma era procurar um livreiro, o qual possuía diversos catálogos e servia como um terceiro de confiança na relação, usualmente cobrando um valor por tal serviço.

Deste primeiro tipo remoto de compras se evoluiu para um segundo tipo, no qual os consumidores acessavam as informações em catálogos físicos ou *on-line* e contatavam

[11] Marc Lacoursière e Édith Vézina, "La sécurité des opérations bancaires par Internet", *Revue Juridique Thémis* 41 (2007):89-156.

[12] Susan V. Scott e Markos Zachariadis, *The Society for Worldwide Interbank Telecommunication (SWIFT): cooperative governance for network innovation, standards and community* (London: Routledge, 2014).

[13] Susan V. Scott e Markos Zachariadis, "Origins and development of SWIFT, 1973–2009", *Business History* 54 (2012): 462-82.

[14] Alberto Luiz Albertin, "Comércio eletrônico: um estudo no setor bancário", *Revista de Administração Contemporânea* 3 (1999): 47-70.

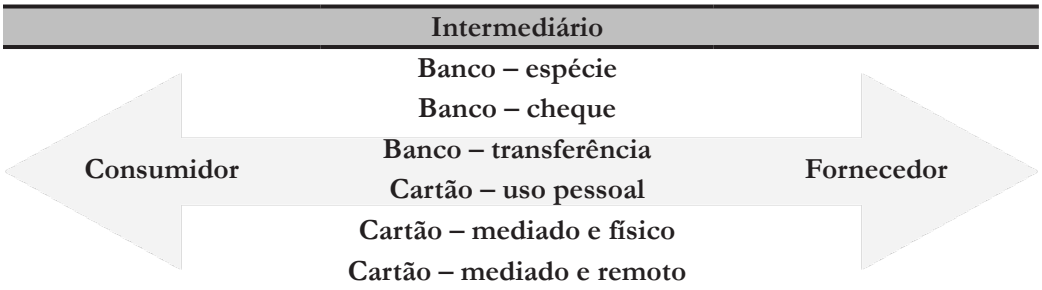
os fornecedores não mais por sistemas mediados por uma loja física ou por sistemas de pagamento tradicionais. Como a relação começou a se dar de forma direta, começou a ser necessária a utilização de meios de pagamento diferentes. No tipo anterior, não havia a retenção de qualquer dado bancário do cliente pelo fornecedor. Porém, no novo modelo, havia o envio dos dados de cartão de crédito para que o fornecedor realizasse a operação. Em um momento inicial, sequer havia máquinas eletrónicas para a cobrança do cartão de crédito. Os números do cartão eram copiados em um boleto da operação. No caso da compra remota, havia uma relação de confiança de que os números do cartão não seriam utilizados para outra compra por parte do fornecedor. Depois do uso do telefone (ou, *fac-simile*) e da via postal, este envio do número de cartão podia se dar por meio de correio eletrónico. Foi uma fase pretérita ao momento atual, de compras eletrónicas em sistemas automatizados.

O tipo atual é diverso do anterior por uma questão simples: tornou-se um sistema integralmente automatizado e digital. Os dois tipos anteriores são baseados na mesma lógica que ainda impera: há um consumidor e um fornecedor, que partilham um sistema de confiança para realização da troca monetária que envolve a relação comercial. Contudo, o sistema passou a ser completamente digital. A segurança ganhou uma dimensão complexa por dois elementos. O primeiro é o estoque de informação bancária na posse do fornecedor em algum banco de dados. O segundo está relacionado com os próprios riscos de transmissão por meio da Internet. Os dois elementos se fundem no aumento da possibilidade de ocorrência do dano e, principalmente, no acréscimo da dificuldade de responsabilização de uma das partes. O quadro abaixo sintetiza os três modelos em uma apreciação abstrata de riscos potenciais.

Figura 1: Modelos abstratos de relação de consumo mediada

Meio de informações	Modo da relação comercial	Sistema de troca monetária	Guarda de informações pelo fornecedor	Avaliação dos riscos aos usuários / consumidores
Catálogo físico mediado	Pessoal com terceiro	Pagamento pessoal	Não	Baixo risco, pois a operação se consuma pessoalmente
Catálogo físico direto	Carta ou telefone	Cheque ou depósito bancário	Não	Baixo risco, pois a operação consome o meio
Catálogo físico direto	Carta ou telefone	Dados do cartão de crédito	Talvez	Alto risco, pois o comerciante pode reter os dados
Catálogo em sítio eletrônico	Correio eletrónico Acesso ao sítio eletrónico	Dados do cartão de crédito	Talvez	Alto risco, pois o comerciante pode reter os dados
	Acesso ao sítio eletrónico	Transferência bancária	Não	Baixo risco, pois a operação se consuma junto ao sistema bancário
Catálogo por terminal celular	Aplicação móvel	Dados do cartão de crédito	Talvez	Alto risco, pois o comerciante pode reter os dados

O que importa reter de todos os tipos abstratos acima indicados é a existência de dois fatores centrais em relação ao tempo e à evolução nos sistemas de compras remotas. O primeiro fator é a existência de um sistema de transação, gerenciado por um terceiro para a concretização da relação comercial, seja ele um banco ou uma operadora de crédito. O segundo fator é a possibilidade da retenção dos dados de acesso ao meio de operação de cobrança destes sistemas terceiros que começa a ser compartilhado entre o consumidor e o fornecedor. Uma simplificação é possível e elucidativa, como será indicado na figura abaixo.



Em suma, sempre existiu um intermediário na relação de compra entre o consumidor e o fornecedor. Assim, mesmo nas relações comerciais que utilizam moedas em espécie é evidente que o sistema monetário nacional serve como intermediário. Afinal, as cédulas monetárias são promessas de valor. Qual a responsabilidade pelo uso de uma cédula falsa para realização de uma transação? Se houver ciência de uma das partes, é claro que a responsabilidade pelo uso da moeda falsa recairá na parte que atua com má fé na relação. Contudo, a má fé no uso de uma moeda falsa é, por vezes, difícil de ser comprovar. Neste caso, de quem será responsabilidade? Ela será do consumidor ou do fornecedor? Em princípio, a responsabilidade é daquele que detinha e utilizou o meio inidóneo. O debate acerca da responsabilidade civil do intermediário nas trocas é crucial, portanto, para o debate jurídico no tema em questão, pois se relaciona com a resolução dos contratos.

Há duas questões contemporáneas que demonstram o aumento dos riscos. O primeiro já foi mencionado e é a possibilidade de haver a retenção dos dados dos consumidores por parte dos fornecedores, em bancos de dados. Isto se tornou especialmente real com os cartões de crédito. O segundo é um processo em marcha, que é o aparecimento de sistemas de compras que são mais do que integrados – ou seja, o uso de sistemas de transação monetária – no qual o fornecedor é, também, um usuário de um sistema terceiro. É o potencial aparecimento de sistemas fundidos de compras, nas quais o fornecedor é o detentor do sistema de transação monetária.[15] O ponto central, portanto, está diretamente relacionado com a esfera de direitos e de deveres dos intermediários e dos fornecedores, em especial, nas trocas que utilizam sistemas de cartões de crédito. O dever de sigilo e de guarda incólume dos dados bancários e pessoais dos usuários. Para examinar estas duas questões, bem como o rol de direitos e deveres dos sistemas de fornecimento, serão descritos dois casos internacionais de vazamentos de dados. Porém, antes, será importante mencionar um pouco da questão da criptografia, porque é sobre essa tecnologia que se depositam

[15] Thierry Dissaux, "Paiements, monnaie, banque électroniques: quelle évolution pour la banque?", *Revue d´économie financière* 53 (1999): 113-32.

os meios para que haja a outorga de segurança nas transações e, assim, a melhoria da confiança dos usuários e consumidores.

Em trabalho anterior, sobre a estruturação de sistemas de certificação digital, Freitas e Veronese já argumentaram que a criptografia possui, em si, uma sutil questão: o direito dos cidadãos a terem segredos em face do Estado, dos demais cidadãos e das empresas; bem como o direito e o dever dos Estados de acessar informações e, assim, garantir a segurança das relações sociais, económicas e jurídicas,[16] De uma forma esquemática e simplificada, a criptografia que possui relevo no debate contemporáneo é baseada em sistemas de certificação digital, por meio dos quais é possível autenticar o emissor e o receptor da mensagem – dados criptografados – além de obrigar o uso de uma enorme capacidade computacional para que haja a decodificação não autorizada do conteúdo. Para tanto, são utilizados algoritmos de criptografia assimétrica, em sistemas de chaves públicas, os quais possuem a garantia da inviolabilidade dada por terceiros autorizados – as infraestruturas –, submetidas elas a constante auditoria no seu funcionamento. No caso do Brasil, o sistema da ICP-Brasil é gerido pelo Instituto Nacional de Tecnologia da Informação (ITI), autarquia vinculada à Casa Civil da Presidência da República. O sistema brasileiro de certificação digital outorga e audita o funcionamento de vários subsistemas técnicos que são utilizados pelo sistema bancário brasileiro, por exemplo. Assim, as transações bancárias nacionais são integralmente cobertas por tal sistema, que possui competência técnica reconhecida. Não obstante, é razoável notar que o referido sistema possui limites em sua operacionalização que se cingem ao sistema de comunicação brasileiro. Assim, é certo que as transações bancárias e comerciais realizadas no Brasil possuem tal proteção. Porém, o que pensar de transações internacionais? Para refletir sobre a questão, a próxima secção do artigo tratará de dois conhecidos casos internacionais de vazamento de dados bancários mantidos por prestadores de serviços eletrónicos.

III. Dois casos de vazamento de dados bancários com impacto transnacional

A ocorrência de casos de vazamento de dados pessoais tem se intensificado em todo o mundo, em decorrência da expansão das compras *online* e de movimentações bancárias via Internet, bem como da existência de fragilidades nos mecanismos de segurança das informações armazenadas. Dois casos emblemáticos merecem estudo, ante o elevado número de indivíduos afetados em diferentes países e em razão da repercussão jurídica. O primeiro é o vazamento de dados pessoais de assinantes da PlayStation Network, ocorrido em 2011, o qual atingiu cerca de 77 milhões de usuários daquela rede.[17] A PlayStation Network é um serviço de acesso a jogos *online*, acessado pela Internet e em diversos países, no qual é possível realizar a compra e o *download* de jogos e outros tipos de aplicativos e mídia. Além disso, o referido serviço possibilita a execução de jogos com outros assinantes da rede. É de propriedade da empresa Sony que também desenvolve e fabrica os consoles de videogame da família PlayStation. Para a atual geração – PlayStation 4 – é obrigatória a assinatura na rede para o uso de partidas *online*.

[16] Christiana Freitas e Alexandre Veronese, "Segredo e democracia: certificação digital e software livre", *Informática Pública* 8 (2007): 9-26.

[17] "Sony PlayStation suffers massive data breach", *Reuters,* 26 de abril de 2011, acesso 26 de março de 2016, disponível em: http://www.reuters.com/article/us-sony-stoldendata-idUSTRE73P6WB20110426.

Conforme declaração oficial da própria Sony, entre os dias 17 e 19 de abril de 2011, uma invasão não autorizada na PlayStation Network (e no serviço Qriocity, também mantido por aquela empresa) conseguiu extrair dados pessoais de seus assinantes – o que incluiu, ao menos, informações sobre nome, endereço, país, endereço de *e-mail*, data de nascimento, *login* e senha de acesso à rede.[18] A empresa não excluiu a possibilidade de que dados de pagamento, tais como número de cartão de crédito e data de expiração, também tenham sido capturados pelo ataque cibernético, No seguimento, a empresa anunciou medidas emergenciais adotadas perante o ataque sofrido: interrompeu ambos os serviços, contratou uma consultoria externa para investigar o ocorrido e tomou providências para aumentar a segurança de sua infraestrutura de rede com foco na proteção de dados pessoais. No início de maio, a Sony retomou alguns dos serviços da PlayStation Network e ofereceu aos assinantes uma compensação que incluiu o *download* gratuito de jogos e o acesso por trinta dias a serviços diferenciados.[19]

Foram então ajuizadas inúmeras ações coletivas (*class actions*) contra empresas do grupo Sony sediadas nos Estados Unidos da América, demandando a reparação dos danos sofridos. Após a reunião de todas as demandas em uma ação coletiva consolidada, os autores e o grupo Sony alcançaram em 2014 um acordo que evitou o julgamento e previu a concessão de benefícios aos usuários afetados, o que incluiu compensações financeiras, jogos gratuitos e oferta de acesso gratuito para serviços *online*, a depender de tipo de assinatura que o indivíduo afetado possuía ao tempo do ataque cibernético – sem que, contudo, a Sony tenha reconhecido responsabilidade pelo ocorrido. Estima-se que o custo total assumido pela Sony no acordo tenha alcançado 15 milhões de dólares.[20] O caso da PlayStation Network chamou ainda a atenção de diversos entes governamentais, em diferentes países, especialmente no que tange à eficácia da política de segurança de dados pessoais adotada pela Sony e possíveis melhorias na regulação desse tema. Ainda em 2011 a comissão de energia e comércio da Câmara de Deputados dos Estados Unidos da América questionou formalmente a Sony sobre o vazamento ocorrido, a política da empresa para a proteção de dados e de privacidade e os planos de compensação aos consumidores.[21] No Reino Unido a entidade administrativa independente responsável por regular a proteção de dados pessoais aplicou uma sanção pecuniária à Sony no valor de 250 mil libras.[22] Ressaltando o caráter global do vazamento da PlayStation Network – e a considerável extensão do dano causado aos assinantes de todo o mundo – o comissário de privacidade do Canadá, responsável por expor ao Parlamento daquele país o estado da aplicação das leis de privacidade, afirmou em seu relatório anual, referente ao ano de 2011, a necessidade de reconhecer

[18] "Sony customer notification US States (excluding Puerto Rico and Massachusetts)", Sony Computer Entertainment, acesso a 26 de março de 2016, http://us.playstation.com/news/consumeralerts.

[19] "Some PlayStation Network and Qriocity services to be available this week", Sony Computer Entertainment, acesso a 26 de março de 2016, https://blog.eu.playstation.com/2011/05/01/some-playstation-network-and-qriocity-services-to-be-available-this-week.

[20] "Sony settles PSN hack lawsuit for $15 million", *ZDNET*, July, 24, 2014, acesso a 5 de abril de 2016, http://www.zdnet.com/article/sony-settles-psn-hack-lawsuit-for-15-million.

[21] "Sony's Response to the U.S. House of Representatives", Sony Computer Entertainment, 4 de maio de 2011, acesso a 5 de abril de 2016, http://blog.us.playstation.com/2011/05/04/sonys-response-to-the-u-s-house-of-representatives.

[22] Information Commissioner's Office of the United Kingdom, "Data protection rights: what the public want and what the public want from data protection authorities", maio de 2015, acesso a 5 de abril de 2016, https://ico.org.uk/media/about-the-ico/documents/1431717/data-protection-rights-what-the-public-want-and-what-the-public-want-from-data-protection-authorities.pdf.

a importância de regular o ambiente empresarial.[23]

Outro caso de vazamento de dados pessoais e bancários em escala global – e que se tornou notório especialmente pelo constrangimento pessoal causado às vítimas – decorreu da invasão sofrida pela rede social Ashley Madison. Aqui houve publicação em sítios da Internet de informações de contato e de meios de pagamento de milhões de usuários. A Ashley Madison é uma rede social com acesso pago, na qual indivíduos casados buscam conhecer pessoas para estabelecer de relações amorosas, obviamente extraconjugais. É administrada pela empresa canadiana Avid Life Media Inc.– que em 2016 declarava possuir mais de 44,4 milhões de usuários cadastrados em 53 países e se afirmava como "o líder mundial em encontros discretos para pessoas casadas". Estima-se que a rede Ashley Madison possua em torno de três milhões de usuários cadastrados no Brasil;[24] já em França, informações jornalísticas indicam entre 330 mil e 700 mil assinantes.[25]

Conforme reportado no *site* oficial da empresa Avid Life Media Inc., em julho de 2015 ocorrera um ataque cibernético aos sistemas daquela empresa e o consequente acesso não autorizado a informações de assinantes da rede Ashley Madison.[26] A empresa informou que já adotara medidas de segurança em sua rede tendentes a cessar o ataque e que trabalhava com agências governamentais para investigar aquele ato criminoso. Notícias afirmaram que um grupo *hacker* denominado *The Impact Team* seria o responsável pelo ataque ao Ashley Madison e teria ameaçado vazar dados pessoais dos assinantes, incluindo nomes e endereços reais, fantasias sexuais e números de cartão de crédito, caso a Avid Life Media não encerrasse a operação de sua rede social.[27] Em declarações oficiais subsequentes, a Avid Life Media afirmou que o ataque sofrido não seria um ato de ativismo *hacker*, mas sim uma ação criminosa,[28] bem como ofereceu recompensa de 500 mil dólares canadianos por informações que pudessem levar à identificação dos autores.[29] O presidente da companhia deixou o cargo no mês seguinte ao ataque.[30] Arquivos com dados pessoais e bancários dos usuários da Ashley Madison foram posteriormente vazados na Internet revelando, além da identidade e de pessoas casadas que buscavam relações extraconjugais, que possivelmente um elevado número das usuárias femininas daquela rede não passavam de robôs cibernéticos programados

[23] Office of the Privacy Commissioner of Canada, "Annual Report of the Office of the Privacy Commissioner of Canada on the Personal Information Protection and Electronic Documents Act for the period from January 1 to December 31, 2011", Junho de 2012, acesso a 5 de april de 2016, https://www.priv.gc.ca/information/ar/201112/2011_pipeda_e.asp.

[24] "Ashley Madison reúne 3 milhões de brasileiros 'para traição'; SP lidera", *TECHTUDO*, 22 de julho de 2015, acesso a 2 de abril de 2016, http://www.techtudo.com.br/noticias/noticia/2015/07/ashleymadison-reune-3-milhoes-de-brasileiros-para-traicao-sp-lidera.html.

[25] "Ashley Madison leak could affect large number of European users", *Deutsche Welle*, 24 de agosto de 2015, acesso a 2 de abril de 2016, http://www.dw.com/en/ashley-madison-leak-could-affect-large-number-of-european-users/a-18669182.

[26] "Statement from Avid Life Media", Avid Life Media, 20 de julho de 2015, acesso a 9 de abril de 2016, http://media.ashleymadison.com/statement-from-avid-life-media-inc-july-20-1225pm.

[27] "Extramarital affair website Ashley Madison has been hacked and attackers are threatening to leak data online", *Business Insider*, 20 de julho de 2015, acesso a 9 de abril de 2016, http://www.businessinsider.com/cheating-affair-website-ashley-madison-hacked-user-data-leaked-2015-7.

[28] "Statement from Avid Life Media", Avid Life Media, 18 de agosto de 2015, acesso a 9 de abril de 2016, http://media.ashleymadison.com/statement-from-avid-life-media-inc-august-18-2015.

[29] "Statement from Avid Life Media", Avid Life Media., 24 de agosto de 2015, acesso a 9 de abril de 2016, http://media.ashleymadison.com/statement-from-avid-life-media-august-24-2015.

[30] "Statement from Avid Life Media", Avid Life Media, 28 de agosto de 2015, acesso a 9 de agosto de 2016, http://media.ashleymadison.com/statement-from-avid-life-media-august-28-2015.

por *script* para simular diálogos.[31] [32] Suspeita-se que a divulgação dos nomes dos assinantes teria provocado alguns casos de suicídio.[33] Tal como no caso PlayStation, diversas ações coletivas foram ajuizadas no Canadá, país em que a Avid Media Life está sediada, bem como nos Estados Unidos. No primeiro país, dois escritórios de advocacia demandaram reparações no valor de 576 milhões de dólares em nome de todos os usuários da rede.[34]

Os casos apresentados ilustram como empresas que possuem atividade comercial transnacional e que manipulam dados pessoais e bancários sensíveis, com milhões de assinantes em dezenas de países, seguem vulneráveis a vazamentos e a ataques cibernéticos. Sítios da Internet que mantêm em seus bancos virtuais informações tão sensíveis quanto o número de cartão de crédito de seu usuário ou a confirmação de um caso extraconjugal têm o dever de resguardar os direitos de privacidade assegurados pelas diferentes jurisdições em que atuam. Nesse sentido, a rápida evolução das tecnologias de informação e comunicação aplicadas nas transações *online* não pode ignorar a necessidade de implantação de mecanismos de segurança e de criptografia cada vez mais eficazes, como ressaltado neste texto. De mesmo modo, as legislações nacionais referentes às relações de consumo devem ser redesenhadas considerando o ambiente virtual em que tais operações agora ocorrem e os riscos existentes, criando obrigações de segurança para as empresas e assegurando a reparação devida às vítimas de vazamentos de dados pessoais e bancários. Na próxima secção há uma descrição da legislação existente no Brasil, bem como algumas das principais propostas em discussão relativas à regulação da proteção de dados pessoais e bancários em transações pela Internet.

IV. Do código de defesa do consumidor ao marco civil da Internet: a dificuldade das pretensões regulatórias do direito brasileiro

As relações de consumo no Brasil são regidas, atualmente, pela Lei Federal n.º 8.078, de 11 de setembro de 1990, conhecida como Código de Defesa do Consumidor. A referida lei veicula normas protetivas ao consumidor – definido como a pessoa física (singular) ou jurídica (coletiva) que seja o destinatário final da aquisição ou fruição de produtos ou serviços. O Código de Defesa do Consumidor trata de forma geral a relação entre consumidor e fornecedor, veiculando normas jurídicas sobre responsabilidade civil referente a danos causados ao consumidor por defeitos e vícios do produto ou serviço, sobre práticas comerciais e sobre cláusulas contratuais, discriminando o que são considerados abusos.[35] [36] As normas jurídicas de proteção ao consumidor incidem,

[31] "Ashley Madison condemns attack as experts say hacked database is real", *The Guardian*, 19 de agosto de 2015, acesso a 9 de abril de 2016, https://www.theguardian.com/technology/2015/aug/19/ashley-madisons-hacked-customer-files-posted-online-as-threatened-say-reports.

[32] "Ashley Madison Code Shows More Women, and More Bots", *GIZMODO*, 31 de agosto de 2015, acesso a 9 de abril de 2016, http://gizmodo.com/ashley-madison-code-shows-more-women-and-more-bots-1727613924.

[33] "Toronto police investigating possible Ashley Madison suicides", *Fortune*, 24 de agosto de 2015, acesso a 9 de abril de 2016, http://fortune.com/2015/08/24/ashley-madison-suicide.

[34] "Ashley Madison faces huge class-action lawsuit", BBC, 23 de agosto de 2015, acesso a 9 de abril de 2016, http://www.bbc.com/news/business-34032760.

[35] Claudia Lima Marques, *Confiança no comércio eletrônico e a proteção do consumidor* (São Paulo: Editora Revista dos Tribunais, 2004).

[36] Ricardo Luis Lorenzetti, *Comércio eletrônico* (São Paulo: Editora Revista dos Tribunais, 2004).

no Brasil, sobre as relações comerciais, independentemente do meio em que ocorram. O Decreto Federal n.º 7.962, de 15 de março de 2013, introduziu disposições jurídicas específicas no Código de Defesa do Consumidor no que se refere às contratações no comércio eletrónico.[37] O Decreto disciplina a relação de consumo eletrónica relativamente às informações sobre produto, serviço e fornecedor (que devem ser claras), bem como sobre atendimento ao consumidor (que deve ser facilitado) e sobre o direito de arrependimento. Tais regras se fazem necessárias ante o ambiente virtual em que ocorrem operações como a compra de produtos e o pagamento de assinatura para fruição de serviços. Uma importante norma trazida pelo Decreto Federal n. º 7.962/2013 diz respeito à necessidade de utilização – pelos *sites* e demais meios eletrónicos usados para oferta de compras coletivas ou modalidades análogas de contratação – de mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor (artigo 3.º, inciso VII). Assim, a legislação brasileira prevê expressamente que os fornecedores – ou seja, os mantenedores de *sites* de venda de produtos ou serviços – têm o dever de adotar sistemas de segurança que impeçam o vazamento de dados pessoais e bancários inseridos pelos consumidores durante compras *online*. O incumprimento de obrigações do fornecedor na relação de consumo implica na possibilidade imposição das sanções administrativas previstas no Código de Defesa do Consumidor (artigo 56.º), bem como na possível aplicação de regras processuais específicas para a defesa do consumidor em juízo (artigos 81.º a 90.º). Pode, ainda, haver o ajuizamento de ações coletivas e individuais de responsabilidade por danos sofridos no âmbito de relações de consumo (artigos 91.º a 100.º). Verifica-se, assim, que o sistema jurídico brasileiro prevê a possibilidade de reparação de danos em relações de consumo decorrentes do incumprimento, pelo fornecedor, do dever de salvaguarda dos dados pessoais e bancários dos consumidores, bem como de aplicação de sanção administrativa por esse facto. É por este motivo que Ellen Sartori considera que já existe um marco de proteção dos dados pessoais dos consumidores no Brasil, apesar de indicar a necessidade de uma legislação específica, nos moldes europeus.[38]

Além disso, outras leis brasileiras buscam proteger os dados pessoais e bancários na Internet e reprimir vazamentos deliberados. A aprovação do chamado Marco Civil da Internet, por intermédio da Lei Federal n.º 12.965, de 23 de abril de 2014, buscou disciplinar a utilização da Internet listando diversas normas jurídicas endereçadas aos usuários e às empresas, bem como determinado a forma de atuação dos entes administrativos. O Marco Civil expressamente indica o respeito à liberdade de expressão como fundamento da disciplina da Internet no Brasil (artigo 2.º), bem como define a proteção da privacidade e a proteção dos dados pessoais, dentre outros, como princípios a serem seguidos (artigo 3.º, incisos II e III). Ademais, determina, no artigo 7.º, uma série de direitos e garantias dos usuários da Internet no Brasil, o que inclui a "inviolabilidade da intimidade e da vida privada" (inciso I), a "inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial" (inciso III), e o "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de Internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei" (inciso VII). O Marco Civil avança ainda

[37] Têmis Limberger, Jânia M. L. Saldanha e Carla A. S. Moraes, "Estado, cidadania e novas tecnologias: o comércio eletrônico e as alterações do Código de Defesa do Consumidor", *Revista de Direito do Consumidor* 22 (2013): 261-82.

[38] Ellen C. M. Sartori, "*Privacidade e dados pessoais: a proteção contratual da personalidade do consumidor na Internet*", Revista de Direito Civil Contemporâneo 9 (2016): 48-104.

mais no artigo 8.º, ao declarar que a garantia do direito à privacidade e à liberdade de expressão é condição para o pleno exercício do direito de acesso à Internet. Pelo Marco Civil, seriam nulas, de pleno direito, as cláusulas contratuais que implicassem uma ofensa ao sigilo das comunicações privadas e que não ofereçam a adoção do foro brasileiro para solução de controvérsias em serviços prestados no Brasil (parágrafo único). No que se refere à proteção de dados pessoais e ao conteúdo de comunicações privadas, bem como à guarda e à disponibilização de registros de conexão e de acesso a aplicações de Internet, o Marco Civil indicou, no artigo 10.º, que deve ser atendida a preservação da intimidade, da vida privada, da honra e da imagem das partes envolvidas. Essa legislação determinou, ainda, que medidas e procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão dos serviços de forma clara – e que os mesmos deveriam atender a padrões definidos em regulamento (§ 4.º do artigo 10.º).

Quanto à recolha, ao armazenamento, à guarda e ao tratamento de registos e dados pessoais, a Lei Federal n.º 12.965 de 2014 obriga, em seu artigo 11.º, o respeito à legislação brasileira e aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e de registros (*caput* do artigo 11.º) quando os dados forem recolhidos/coletados em território nacional ou em comunicações nas quais ao menos um dos terminais seja localizado no país (§ 1.º do artigo 11.º), e mesmo que as atividades sejam exercidas por pessoa jurídica (coletiva) sediada no exterior, se o serviço for oferecido no Brasil ou se ao menos um integrante do grupo económico possua estabelecimento no país (§ 2.º do artigo 11.º). A lei exige ainda que provedores de conexão e de aplicações na Internet prestem informações sobre o cumprimento da legislação brasileira nessas atividades (§ 3.º do artigo 11.º), e deixa para futura regulamentação a especificação do procedimento para apuração de infrações (§ 4.º do artigo 11.º). Há a previsão de penalidades administrativas para as infrações referentes à violação da proteção de dados pessoais e bancários, sem prejuízo de demais sanções cíveis, criminais e administrativas. O Marco Civil institui penalidades no artigo 12.º, que podem ser aplicadas de forma isolada ou cumulativamente: advertência; sanção pucuniária; suspensão temporária; e proibição do exercício de atividades de armazenamento, guarda e tratamento de registros ou dados pessoais. A lei prevê ainda que, se a empresa for estrangeira, a sua filial, sucursal, escritório ou estabelecimento no Brasil responderá solidariamente pelo pagamento da sanção pecuniária (parágrafo único do artigo 12.º). Verifica-se, assim, que o Marco Civil da Internet aprofundou as obrigações que fornecedores de produtos e serviços na Internet devem atender na preservação do sigilo dos dados pessoais que detêm, independentemente da existência de relação de consumo e de a pessoa jurídica (coletiva) estar ou não sediada no Brasil, desde que ofereça seus serviços no país. Criou ainda sistema próprio de sanção que pode ser aplicado cumulativamente com as penalidades do Código de Defesa do Consumidor e das responsabilizações cíveis e criminais aplicáveis.

A legislação brasileira também prevê a aplicação de sanções na esfera criminal em decorrência do vazamento de dados pessoais na Internet. A Lei Federal n.º 12.737, de 30 de novembro de 2012, ficou conhecida como "Lei Carolina Dieckmann" – por referência ao episódio de vazamento na Internet de fotos íntimas de uma atriz em maio de 2011. A vítima sofreu tentativa de extorsão pelo responsável pela captura dos dados e posterior divulgação das imagens. O caso teve considerável repercussão na comunicação social brasileira.[39] A referida lei incluiu no Código Penal brasileiro

[39] "Carolina Dieckmann prestará depoimento sobre publicação de fotos íntimas", *Folha de São Paulo*, 6

a tipificação do delito de "invasão de dispositivo informático" (artigo 154.º-A, *caput*) com a possibilidade de imputação de três meses a um ano de prisão, combinada com a aplicação de multa. Ainda segundo o dispositivo legal, incorre na mesma pena quem "produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador" que tenha por intuito a conduta acima descrita (artigo 154.º-A, §1.º). Ademais, a ocorrência de prejuízo económico em decorrência da invasão é causa de aumento de pena (artigo 154.º-A, §2.º). Nota-se que a invasão a dispositivo que não tenha a intenção descrita no tipo penal não está abarcada pela lei como crime – ou seja, para que haja crime, necessariamente deve haver a finalidade de obtenção, adulteração ou destruição de dados ou informações sem autorização, ou ainda a obtenção de vantagens ilícitas. Tem-se como evento qualificador do crime de invasão de dispositivo informático a obtenção de conteúdo que seja acobertado por sigilo, conforme definido em lei, ou que se refira a comunicações eletrónicas privadas, segredos comerciais ou industriais, bem como se da invasão decorre controlo remoto do dispositivo atacado. Nesses casos, a pena será de reclusão, de seis meses a dois anos, e multa, se a conduta não constitui crime mais grave (artigo 154.º-A, §3.º). Para tais condutas, incide ainda causa de aumento de pena quando ocorrer divulgação, comercialização ou transmissão dos dados obtidos a terceiros (artigo 154.º-A, §4.º), bem como é previsto o incremento se a conduta for praticada contra uma das autoridades listadas no artigo 154.º-A, §5.º. A "Lei Carolina Dieckmann" ainda incluiu, na tipificação do crime de "falsificação de documento particular" constante do artigo 298,º do Código Penal brasileiro, a equiparação do cartão de crédito ou débito a documento particular, o que assegura a criminalização do uso de dados bancários vazados.

Finalmente, nota-se que as pretensões regulatórias brasileiras seguem avançando na criação de mecanismos jurídicos que busquem proteger o sigilo dos dados pessoais e bancários em um ambiente tecnológico em constante mutação. A expansão de formas de pagamento em transações eletrónicas intermediadas por dispositivos de telecomunicações e geridas por instituições não financeiras, fenómeno que se alastra por diferentes jurisdições, mereceu a edição de normas jurídicas específicas no Brasil – trata-se dos artigos 6.º a 15.º da Lei n.º 12.865, de 9 de outubro de 2013. As referidas normas permitiram que empresas do setor de telecomunicações pudessem ofertar serviços de pagamento por meio de terminais de acesso, ou seja, telefones móveis, como meio de programar políticas de inclusão financeira a indivíduos sem acesso ao sistema bancário, sem descuidar da proteção aos dados pessoais, conforme se verifica dos artigos 7.º, IV, e 8.º da Lei n.º 12.865/2013.

A evolução tecnológica, ao tempo em que possibilita a inclusão social por meio das tecnologias de informação e comunicação, também traz novos desafios, tanto para empresas como para os Estados e as sociedades. Existem questões técnicas, como, por exemplo, possibilitar estruturas de comunicação que permitam o pleno desenvolvimento da crescente expansão do comércio eletrônico.[40] De outro lado, a venda de serviços e produtos puramente digitais traz outros desafios, pois a entrega e a fruição do produto ou do serviço adquirido ocorrrem totalmente de forma eletrónica.[41] Todavia, a questão mais relevante e premente da atualidade é relacionada

de maio de 2012, acesso a 26 de março de 2016, http://www1.folha.uol.com.br/ilustrada/1086411-carolina-dieckmann-prestara-depoimento-sobre-publicacao-de-fotos-intimas.shtml.

[40] Allain Rallet, "Commerce electronique ou electronisation du commerce?", *Réseaux* 106 (2001): 17-72.

[41] Fabrice Lequeux e Allain Rallet, "Un Internet peut en cacher um autre: vers l'avènement des marchés du multimédia en ligne", *Réseaux* 124 (2004): 207-44.

com a segurança dos dados pessoais e bancários. A questão central ganha contornos complexos, ao se aventar o incremento de operações financeiras virtuais e o aumento de atores, sistemas e dispositivos relacionados às transações *online*. No caso brasileiro, é certo que existem algumas normas jurídicas que possibilitam sua mobilização em prol de proteção. Contudo, a efetiva proteção dos consumidores não está apenas relacionada com a existência de leis. Ela é diretamente derivada da sua aplicação pelos atores sociais. Assim, princípios como aqueles previstos no Código de Defesa do Consumidor e no Marco Civil da Internet somente serão meios jurídicos de proteção no momento em que forem efetivamente utilizados pelos diversos atores sociais para pautar as suas relações. Não obstante, parece claro que as leis citadas não são suficientes para gerar um conjunto normativo pleno e que o Brasil ainda requer uma legislação específica para a proteção dos dados pessoais, em padrões similares àqueles existentes na Europa, por meio da Diretiva 2000/31/CE (comércio eletrónico) e da Diretiva 95/46/CE (proteção de dados pessoais), substituída pelo Regulamento 2016/679/UE (Regulamento Geral sobre a Proteção de Dados).[42]

O objetivo principal deste texto é demonstrar que a agregação de dados bancários em sistemas automatizados, gerenciados por conglomerados empresariais ou grandes empresas transnacionais, aumenta o risco de vazamentos maciços, contra os quais os diversos países, de entre os quais o Brasil, possuem meios limitados para repressão. De outro lado, o controlo prévio desses dispositivos integrados de compras também é complexo e, para sua boa operacionalização, dependeria de sistemas transnacionais efetivos de cooperação. É certo que os sistemas bancários nacionais possuem regimes de cooperação que têm se mostrado hábeis para fornecer confiança às trocas internacionais. Porém, mesmo sistemas como o SWIFT estão sob o escrutínio das autoridades nacionais de proteção dos dados pessoais, em razão dos riscos relacionados à lavagem de dinheiro e ao terrorismo.[43] Em síntese, o debate sobre a integração vertical das estruturas de comércio eletrónico ainda é incipiente – e não focalizou as questões relativas à agregação dos sistemas de transação com os meios de fornecimento dos bens e serviços. A literatura atual ainda está dirigida, de forma geral, à discussão sobre a oportunidade, ou não, da integração da oferta de conteúdos digitais com os meios de provimento, questão conhecida como neutralidade de rede.[44] É evidente que os riscos regulatórios futuros são relacionados com a integração vertical e internacional do comércio eletrónico, na "formação" de conglomerados empresariais para oferta de produtos e serviços, agregados com sistemas de pagamento.

V. Conclusão

O presente texto realizou a descrição de um problema contemporâneo relacionado com o comércio eletrónico: a integração entre sistemas de transação comercial – automatizados – com a oferta de bens e serviços. Inicialmente, foi mencionada a expansão quantitativa do comércio eletrónico, bem como sua relação com a automatização das trocas. Foi ainda construída uma tipologia da evolução dos sistemas de transação, para evidenciar o aumento dos riscos de vazamento em

[42] Laura Schertel Mendes e Danilo Doneda, "Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016", *Revista de Direito Civil Contemporâneo* 9 (2016): 35-48.
[43] Anthony Amicelle, "*The great (data) bank robbery: terrorist finance tracking program and the SWIFT affair*", Research Questions 36 (2011), acesso a 9 de abril de 2016, http://www.sciencespo.fr/ceri/en/content/great-data-bank-robbery-terrorist-finance-tracking-program-and-swift-affair.
[44] Nicolas Curien e Winston Maxwell, *La neutralité d'Internet* (Paris: La Découverte, 2011).

sistemas concentrados. Foram descritos dois casos internacionais, ocorridos em 2011 e em 2015 – Sony PlayStation e Ashley Madison, respetivamente – para demonstrar o potencial de danos maciços e amplos que podem ocorrer com a centralização de dados bancários dos consumidores em sistemas integrados de compras. A exposição serviu para evidenciar que a defesa judicial contra violações, *a posteriori*, é muito complicada. Também fica claro que os diferentes países possuem meios de defesa assimétricos para se protegerem de tais violações. A leitura do direito brasileiro demonstra que a legislação existente possui elementos que poderiam ser mobilizados para a proteção prévia e para a repressão às violações dentro da jurisdição nacional. Não obstante, as prescrições jurídicas existentes estão esparsas em diferentes diplomas jurídicos e inexistem normas que prevejam a cooperação e a atuação internacional de estruturas de proteção.

Neste sentido, a conclusão do presente artigo é que existem dois debates a travar na literatura e nas políticas públicas do Brasil: a formação de um marco legal para a proteção dos dados pessoais que seja integrado com as normas já existentes, bem como que possua previsão de cooperação internacional nos moldes das disposições europeias; e, por outro lado, um debate sobre os riscos de integração vertical na oferta de meios de transação com a oferta de produtos e serviços por meio de comércio eletrónico, especialmente em razão da internacionalização das empresas. Essas duas discussões não foram realizadas de forma plena aquando da aprovação da Lei n.º 12.865/2013, apesar de o debate regulatório futuro ter sido mencionado na exposição de motivos da Medida Provisória n.º 615, de 17 de maio de 2013, origem da lei federal em questão.[45]

Na prática, a utilização de um sistema de pagamentos com a integração dos serviços de provimento de acesso à Internet acabou por não se consolidar como uma opção de comércio no Brasil. Porém, o debate sobre a integração de operações em comércio eletrónico precisa ser debatido sob o prisma da proteção dos dados pessoais, bem como pela ótica da proteção ao direito da concorrência, tendo o olhar dirigido ao panorama internacional. Ou seja, o debate não pode ser realizado somente na perspetiva da regulação brasileira e requer a apreciação do marco jurídico, económico e social dos diversos países que já tenham travado tais discussões, de forma a prospectar a

[45] "Nos últimos anos, tem crescido a participação de instituições não financeiras na provisão de serviços de pagamento, principalmente por intermédio de cartões de pagamento (crédito ou débito), moedas eletrônicas ou meios eletrônicos de pagamento, a exemplo dos instrumentos disponibilizados para o comércio eletrônico (*e-commerce*) e das transações realizadas mediante dispositivos móveis de comunicação (*mobile payment*). Esse cenário tem o potencial de trazer inegáveis benefícios para a economia nacional – maior competição, redução de custos e preços, aumento da conveniência para os usuários, melhoria na qualidade dos serviços, facilitação da inclusão financeira. Entretanto, existem riscos inerentes às atividades relacionadas aos serviços de pagamento, que, uma vez dimensionados, podem ser mitigados mediante regulação e supervisão setorial, com vistas na promoção da solidez e da eficiência. A adequação do arcabouço normativo, além de possibilitar a mitigação dos riscos, também potencializa o papel de indutor dos agentes públicos na busca de modelos que atendam aos interesses da sociedade, alinhavando-os às políticas públicas existentes. Ademais, a regulação desse setor da economia traz a segurança jurídica demandada para a realização dos investimentos necessários para a implementação e desenvolvimento dos arranjos de pagamento. Considera-se que os arranjos de pagamentos, em especial os relacionados a pagamentos móveis, podem contribuir significativamente para o objetivo do Governo Federal de promover a inclusão financeira da população brasileira. O potencial inclusivo dos pagamentos móveis deve-se à elevada penetração da telefonia móvel no Brasil em todos os segmentos de renda. Ademais, a possibilidade de atuação de novos agentes neste mercado, como as próprias operadoras de telecomunicações, trarão novos investimentos e maior concorrência na provisão de serviços de pagamento."

possibilidade de cooperação jurídica como uma forma de mitigar os limites da atuação da jurisdição local nas contendas com empresas transnacionais de grande porte.

Qual foi a consequência do caso Snowden, em 2013? Foi o aumento das preocupações de gestores e técnicos da União Europeia acerca da insuficiência de proteção prevista nos acordos de cooperação com os Estados Unidos da América. Tais preocupações deram ensejo à revisão de toda a legislação da União Europeia sobre o tema da proteção de dados pessoais, além de ter servido para potenciar a fiscalização por parte das diversas autoridades nacionais. É por esse motivo que Liane Colonna descreve a reação de imediata suspeita, por parte dos europeus, sobre a interação entre as grandes empresas dos Estados Unidos da América com o governo daquele país e do reflexo havido na legislação da União Europeia sobre proteção de dados pessoais.[46] De outra perspetiva, Juhi Tariq alerta as empresas norte-americanas para a mudança do panorama em razão do caso Snowden.[47] Em relação ao Brasil, esse *affair* internacional parece não ter atraído a atenção sistemática do legislador e dos reguladores, apesar de Alessandro Molon indicar que a aprovação do Marco Civil da Internet teria sido uma consequência do ocorrido.[48] Em suma, resulta evidente a necessidade de um debate regulatório com o objetivo de dimensionar a proteção nacional – por meio de uma legislação integrada – dos dados bancários e pessoais, para que seja possível dimensionar de forma equilibrada os riscos e as potencialidades dos processos de integração vertical que, não obstante, estão em marcha nos diversos mercados do planeta. O referido debate não pode deixar de aferir e prever a questão da cooperação administrativa e judicial como um ponto central para a efetividade dos meios de proteção contemporânea.

[46] Liane Colonna, "*PRISM and the European Union's data protection directive*", The John Marshall Journal of Information Technology & Privacy Law 30 (2013): 227-51, disponível em: http://repository.jmls.edu/jitpl/vol30/iss2/1/.

[47] Juhi Tariq, "The NSA's PRISM program and the new EU privacy regulation: why US companies with a presence in the EU could be in trouble", *American University Business Law Review* 3 (2014): 371-82.

[48] Alessandro Molon, "*A legislação e a internet: ideais, desafios e avanços com o Marco Civil da Internet*", Cadernos Adenauer 16 (2015): 107.