

## Compras integradas e proteção de dados bancários no contexto da Diretiva (UE) 2015/2366: os novos prestadores de serviços de pagamento <sup>1</sup>

*Integrated purchasing and banking data protection in the context of Directive (EU) 2015/2366: new payment service providers*

Submetido(submitted): 13/09/2018  
Parecer(revised): 10/10/2018  
Aceito(accepted): 02/11/2018

Dominique Legeais\*

### Abstract

**Purpose** – *The article analyses the limits of protection of bank users’ data in France, framing them as personal data. Its legal analysis is made amidst a context of radical changes in the European and French personal data protection law as well in the banking regulation, which is being transformed by the new payment services regulation.*

**Methodology/approach/design** – *The article brings an interlacement of some new legal sources from the European and French law to appraise the limits of banking data protection. It tests the application of some legal norms in order to evaluate the potential protection in two areas: the security of the banking data on a new environment of payment services (fintechs and other new firms); the possibility of protection against the unauthorized data commercial usage.*

**Findings** – *The article concludes that the European and French banking and payment services law have not the desired level of protection against bad commercial practices in a context, which is marked by both the retailers and payment services integration as well the presence of the big techs. The data protection law must complement the banking and payment services regulation in order to provide the desired level of protection.*

**Practical implications** – *The article demonstrates the possibility of testing new kinds of legal regulation – data protection – to archive social and economic security in a different sector, like baking and commerce.*

---

<sup>1</sup>Texto derivado do seminário internacional “A efetividade do direito em face do poder dos gigantes da Internet – Brasil e França”, realizado na Universidade de Brasília no período de 13 até 15 de abril de 2016. Agradece-se ao apoio financeiro da Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), da Fundação de Amparo à Pesquisa do Distrito Federal (FAPDF), da Embaixada da França no Brasil e das universidades brasileiras e francesas envolvidas. Texto traduzido por Germana Henriques Pereira de Souza. Revisão técnica de Alexandre Veronese.

\*Professor Titular (Professeur Agregé) de Direito Privado e Diretor do CEDAG (Centre des droits des affaires et de gestion) da Faculté de Droit et Sciences Politiques da Université Paris Descartes (Paris Cité). Atua na área de direito comercial, bancário e de seguros, sendo autor de diversas publicações relativas aos direitos das novas tecnologias e suas interações com os domínios jurídicos clássicos. Destacam-se: LEGEAIS, Dominique. *Droit commercial et des affaires*. 24. ed. Paris: Sirey, 2018; LEGEAIS, Dominique. *Droit des sûretés et garanties du crédit*. 12. ed. Paris: LGDJ / Lextenso, 2017; LEGEAIS, Dominique. *Opérations de crédit*. 2. ed. Paris: Lexisnexis, 2018 (Traité). E-mail: [dominique.legeais@parisdescartes.fr](mailto:dominique.legeais@parisdescartes.fr).

**Originality/value** – *The article departs from a new concept of banking data, built from the meshing of the concepts of banking information and sensible personal data. From this conceptual frame, it can evaluate the level of protection granted by the European and French law in order to sketch a possible protective regime.*

**Keywords:** *data protection, banking information, personal data, big techs, banking regulation.*

### Resumo

**Propósito** – O artigo analisa as possibilidades de proteção dos dados bancários na França, entendidos como uma categoria específica dos dados pessoais. A análise jurídica é realizada em meio a um contexto de aceleradas mudanças, seja na legislação de proteção de dados da Europa e da França, seja na transformação em marcha do direito bancário europeu pelo advento do direito dos serviços de pagamento.

**Metodologia/abordagem/design** – O artigo realiza o cruzamento de fontes jurídicas recentes, oriundas do direito europeu e do direito francês para examinar as possibilidades de proteção dos dados bancários. Ele testa a aplicação de normas jurídicas em prol da potencial aplicação de proteção em dois temas: segurança dos dados bancários em meio ao novo panorama jurídico dos serviços de pagamento (*fintechs* e outros); e a proteção contra a exploração comercial dos dados bancários.

**Resultados** – O artigo conclui que o direito bancário e dos novos serviços de pagamento francês e europeu não possuem, ainda, força protetiva em face das práticas comerciais eletrônicas, marcadas pela integração empresarial e pela atuação dos gigantes da Internet. Para que o direito bancário e dos novos serviços de pagamento possa proteger os consumidores e os usuários, far-se-á necessária sua complementação pelo direito da proteção de dados.

**Implicações práticas** – O artigo demonstra a possibilidade de testagem de novos meios de regulação jurídica – proteção de dados pessoais – para alcançar uma área diferente da vida social e econômica, como o direito bancário e as práticas comerciais.

**Originalidade/relevância do texto (opcional)** – O artigo parte de uma construção inovadora do conceito de dados bancários a partir da conjugação das informações bancárias com o conceito de dados pessoais sensíveis. A partir dessa construção teórica, ele testa a aplicabilidade de normas de proteção do direito bancário europeu e francês para avaliar um potencial regime específico de proteção.

**Palavras-chave:** proteção de dados, informações bancárias, dados pessoais, gigantes da Internet, regulação bancária.

## Introdução

Analisar as compras integradas e os dados bancários em um mesmo artigo é como atravessar dois mundos em profunda transformação devido ao desenvolvimento dos gigantes da Internet: o *e-commerce* e o sistema bancário. No centro dessas duas atividades encontram-se os dados bancários. Eles estão tradicionalmente no coração das transações bancárias. No âmbito estrito dessa atividade, eles já estão suscitando dificuldades (é o caso do *scoring* e da transmissão de dados para fora da União Europeia). Os dados bancários estão, hoje, no centro do comércio *online*, pois, de um lado, possibilitam que o pagamento seja efetuado e, de outro, promovem a prospecção de clientes. Ainda, os dados estão em processo de mudança funcional: de objeto tradicional da proteção pelo sigilo bancário, eles estão, agora, praticamente se tornando bens comercializáveis.

A consolidação das práticas de compras integradas pode ser um marco relevante para definir a abertura radical do antigo mercado cativo de serviços bancários, com um potencial ainda imponderável de consequências. É possível definir a integração de compras quando existe uma agregação do fornecedor dos produtos e dos serviços com a plataforma de execução dos pagamentos. Tradicionalmente, essas duas atividades estavam separadas e os pagamentos estavam sob o controle de bancos. A atual conformação jurídica permite que uma grande empresa de vendas *online*, como a *Amazon*, por exemplo, tenha o seu próprio sistema de pagamentos. Esse novo cenário aproxima o tradicional direito bancário do emergente direito da proteção de dados pessoais. E, assim, aparecem novos desafios a serem enfrentados.

O termo “dados bancários” deve ser explicado. Não existe uma definição jurídica específica. No âmbito da nova Diretiva (UE) 2015/2366<sup>2</sup>, cuja data final para transposição era o dia 13 de janeiro de 2018, as credenciais de segurança personalizadas são definidas como dados pessoais fornecidos a um usuário do serviço de pagamento pelo prestador de serviços de pagamento para fins de autenticação, nos termos do artigo 4º (31)<sup>3</sup>. Já os dados de pagamento sensíveis

---

<sup>2</sup> Nota do revisor técnico. A primeira Diretiva de Serviços de Pagamento (DSP) foi a Diretiva 2007/64/CE. UNIÃO EUROPEIA: Parlamento Europeu e Conselho. Directiva 2007/64/CE, 13 nov. 2007, relativa aos serviços de pagamento no mercado interno, que altera as Directivas 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE e revoga a Directiva 97/5/CE. Disponível: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32007L0064>. Acesso em: 9 jul. 2018. Ela foi substituída

pela DSP 2, que será mencionada ao longo do artigo.

<sup>3</sup> Nota do revisor técnico: “Artigo 4º (...) 31) (...) elementos personalizados fornecidos pelo prestador de serviços de pagamento a um utilizador de serviços de pagamento para efeitos de autenticação” (UNIÃO Europeia: Parlamento Europeu e Conselho. Directiva (UE)

são aqueles que incluem informações de segurança personalizadas e que podem ser usadas para se cometer fraudes<sup>4</sup>. No que diz respeito às atividades dos prestadores de serviços de iniciação de pagamentos<sup>5</sup> e de prestadores de serviços de informação sobre contas, o nome do titular da conta e o número da conta não constituem dados de pagamento sensíveis, de acordo com a Diretiva.

A caracterização como “dados bancários” pode ser aplicada a vários elementos de vinculação de uma pessoa porque eles se tratam de uma subcategoria do conceito jurídico de dados pessoais. Trata-se, em primeiro lugar, de informações coletadas: o número da conta; o número do cartão da conta; e, mais geralmente, a identificação financeira do titular da conta. Também podem ser: os destinatários de uma transferência ou depósito; o saldo de uma conta; o objeto de um pagamento ou de uma dívida. Esse é o núcleo duro dos dados bancários.

Por permitirem a realização das transações e dos pagamentos, esses dados devem ser mantidos seguros. Disso depende a sustentabilidade do sistema de compras *online*. Porém, os dados bancários também podem ser elementos extraídos da análise de uma conta, de seu histórico de operações, permitindo, assim, que um perfil de seu titular seja definido, o *profiling*. Esses comentários baseados nos dados podem ser feitos através de *scoring* ou de pesquisas conduzidas pelos bancos. É, então, permitido identificar e recensear quais são os fornecedores de uma pessoa, o seu estilo de vida e o seu poder de compra. Esses dados revelam a vida mais íntima de uma pessoa. Eles são, portanto, muito valiosos para o incremento das atividades de prospecção comercial.

Assim, pelo fato de representarem um potencial valor econômico considerável, os dados bancários são objeto, hoje, de toda a atenção dos variados atores da economia. Isso ocorre porque, até o advento da hegemonia dos gigantes da Internet, os dados bancários suscitavam pouca atenção pública. Por um lado, apenas os bancos titulares das contas bancárias detinham o monopólio sobre os pagamentos; logo, a proteção jurídica do sigilo bancário garantia, assim, os direitos inerentes aos titulares das contas. Por outro lado, de uma forma geral,

---

2015/2366, 25 nov. 2015, relativa aos serviços de pagamento no mercado interno. Disponível: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32015L2366>. Acesso em 6 jul. 2018).

<sup>4</sup> Nota do revisor técnico: “Artigo 4º (...) 32) (...) dados, incluindo credenciais de segurança personalizadas, que podem ser utilizados para cometer fraudes. Para as atividades dos prestadores do serviço de iniciação do pagamento e dos prestadores de serviços de informação sobre contas, o nome do titular da conta e o número da conta não constituem dados de pagamento sensíveis” (UNIÃO Europeia: Parlamento Europeu e Conselho. Diretiva (UE) 2015/2366, 25 nov. 2015, relativa aos serviços de pagamento no mercado interno. Disponível: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32015L2366>. Acesso em 6 jul. 2018).

<sup>5</sup> Nota do revisor técnico: a Diretiva utiliza a denominação “prestador” de uma forma geral. Essa será a denominação aqui adotada.

havia uma menor circulação desses dados; afinal, o cliente não precisava comunicar os dados da sua conta para terceiros em prol de dispor de serviços cotidianos.

## 2. O novo cenário jurídico europeu para os serviços de pagamento

A consolidação jurídica da abertura do mercado para outros prestadores de serviços que eram, tradicionalmente, somente realizados pelos bancos está mudando o cenário econômico da Europa. Nos últimos anos, existem novos prestadores de serviços de pagamento responsáveis por essa função que, no entanto, não são os banqueiros usuais dos clientes. A nova Diretiva (UE) 2015/2366 – Diretiva de Serviços de Pagamento, também conhecida como DSP 2 –, expande ainda mais o número de participantes para incluir, precisamente, aqueles que surgiram com o advento da Internet<sup>6</sup>. Houve a criação de um estatuto jurídico europeu para os serviços pagamentos por meio de terceiros. O artigo 1º (1º) da Diretiva assim define os prestadores de serviços de pagamento:

Artigo 1.º Objeto (...). 1. A presente diretiva estabelece as regras nos termos das quais os Estados-Membros distinguem as seguintes categorias de prestadores de serviços de pagamento: a) instituições de crédito, na aceção do artigo 4.º, n.º 1, ponto 1, do Regulamento (UE) n.º 575/2013 do Parlamento Europeu e do Conselho, incluindo as suas sucursais, na aceção do ponto 17 do n.º 1 desse artigo, quer a sede dessas sucursais esteja situada na União, quer, nos termos do artigo 47.º da Diretiva 2013/36/UE e do direito nacional, fora da União; b) instituições de moeda eletrónica, na aceção do artigo 2.º, ponto 1, da Diretiva 2009/110/CE, incluindo, nos termos do artigo 8.º dessa diretiva e do direito nacional, as suas sucursais, caso essas sucursais estejam situadas na União e a sua sede esteja situada fora da União, na medida em que os serviços de pagamento prestados por essas sucursais estejam associados à emissão de moeda eletrónica; c) instituições de giro postal autorizadas pelo direito nacional a prestar serviços de pagamento; d) instituições de pagamento; e) O BCE e os bancos centrais nacionais, quando não atuem na qualidade de autoridades monetárias ou de outras autoridades públicas; f) os Estados-Membros

---

<sup>6</sup> Além da DSP 2, já citada na nota anterior, havia um projeto de novo regulamento em debate na União Europeia, quando o artigo foi produzido, em 2016. Todavia, com passar do tempo, o referido projeto foi aprovado: Regulamento (EU) 2017/2055. UNIÃO EUROPEIA. Regulamento Delegado (UE) da Comissão, que complementa a Diretiva (UE) 2015/2366 do Parlamento e do Conselho no que respeita às normas técnicas de regulamentação relativas à autenticação forte do cliente e às normas abertas de comunicação comuns e seguras. Disponível: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R2055>. Acesso em: 6 jul. 2018.

ou as respetivas autoridades regionais ou locais, quando não atuem na qualidade de autoridades públicas

Ora, tal como foi redigido, esse estatuto é uma revolução: os bancos vão dar a chave de acesso de seu bem mais precioso: os dados das contas bancárias. Está-se reinventando o mundo dos bancos, cortando-se a sua cadeia de valor. Assim, novas estruturas (*fintechs*) estão se instalando no mercado, com base no artigo 1º, 1 (b) da Diretiva (UE) 2015/2366. Como consequência anunciada dessa alteração do mundo bancário, o modelo clássico de rentabilidade dos bancos tradicionais entrou em colapso. Vários serviços que somente poderiam ser prestados pelos bancos, desde gestão de contas até a concretização de pagamentos, agora são explorados por novos prestadores. Foi assim, por conseguinte, necessário que os bancos encontrassem outras fontes de receita, a partir de elementos que eles já dispõem. Os dados bancários se tornaram, então, naturalmente uma nova fonte de renda, ainda que, para isso, se tenham praticadas graves violações ao sigilo bancário, outro pilar tradicional do direito bancário. O desenvolvimento de plataformas de vendas *online* também contribuiu para as mudanças. O pagamento seguro é a chave de seu sucesso. Mas, os dados de referência também fazem parte do perfil do cliente, que é útil para a prospecção. No âmbito dos cartões de crédito, há uma prática de ofertas promocionais personalizadas vinculadas a cartões de pagamento que combinam análise dos dados de transação e publicidade direcionada.

Uma nova perda de espaço se avizinha no horizonte: as compras integradas, nas quais o fornecedor de bens e serviços pode criar ou agregar uma *fintech* ao processo de compra e venda, para, desse modo, suprimir a necessidade das instituições bancárias. Nas compras integradas, dois modelos são implementados. A plataforma pode solicitar a intervenção de um terceiro, como o *Paypal*, para garantir o pagamento seguro. Esse terceiro pode, ele mesmo, tornar-se um gigante da Internet no futuro. Porém, a plataforma pode, também, ser a própria prestadora dos serviços de pagamento. O desenvolvimento do *m-payment – mobile payment* – deve ser acrescentado a esse quadro. Ele designa uma nova modalidade de pagamentos a ser realizado por meio das operadoras de telefonia móvel. Assim, se, no dia de hoje, a maioria dos projetos ou dos serviços existentes são feitos por meio de cartão de crédito, o mesmo poderá não acontecer no dia de amanhã. As grandes empresas da Internet anunciaram, de fato, planos de utilizar sistemas de pagamentos por meio de celulares sem passar por um mecanismo de cartão bancário, recorrendo, para tanto, à moeda eletrônica e aos meios de carteiras digitais (*digital wallet*) gerenciadas pelos gigantes da Internet.

Teria sido fundamental que o legislador europeu tivesse fornecido respostas claras para as questões emergentes, tendo em vista os desafios, os

princípios jurídicos envolvidos e os interesses sociais e econômicos conflitantes. No entanto, paradoxalmente, mesmo quando os textos fundamentais estão sendo preparados, tanto com relação aos serviços de pagamento, quanto com relação aos dados pessoais, subsiste o predomínio da sensação de certo vazio ou, pelo menos, de certa imprecisão. A particularidade dos dados bancários não é praticamente levada em conta. A Diretiva (UE) 2015/2366, de 23 nov. 2015 (DSP 2), é reveladora nesse sentido. Até mesmo os especialistas em direito comercial concordam que essa área jurídica ainda está em construção. No entanto, é essencial adotar uma postura inquisitiva. Deve-se privilegiar o comércio – e sua prospecção de clientes – ou deve-se proteger a privacidade do consumidor cujos dados bancários, bem como os dados médicos, certamente fazem parte de sua vida privada?

Os desafios vão muito além do consumidor titular de uma conta bancária e que dá início a um pagamento. A resposta não pode, por essa razão, ser puramente contratual. O cliente está numa situação de inferioridade e não mede os problemas e as consequências das autorizações solicitadas. O cliente precisa apenas de duas garantias. Em primeiro lugar, ele precisa que sua compra, através do comércio *online*, seja bem-feita. E, também, ele requer que a comunicação de seus dados, seja para um vendedor ou para um prestador de serviços de pagamento, não se torne fonte de possíveis fraudes, das quais ele poderia ser vítima. Em segundo lugar, nenhum consumidor, espontaneamente, deseja que os seus dados bancários possam ser transmitidos a outros para fins comerciais e que possam, posteriormente, favorecer uma prospecção agressiva de publicidade.

Nesse contexto de abertura do mercado de pagamentos para novas empresas, o usuário quer perceber um avanço: pagamentos facilitados ao máximo e com um menor custo, sem que todas as garantias tradicionais – como o sigilo e a segurança – sejam enfraquecidas. Pode o novo modelo econômico possibilitado pela revolução digital ainda permitir essa conciliação? Ou, deve-se admitir que o novo comércio suscita inevitavelmente a redução do sigilo bancário e da perda de controle de uma pessoa sobre parte dos seus dados bancários? Esses são os dois lados do debate que está apenas começando. Quem será o vencedor da transformação em curso: os bancos tradicionais, as *fintechs* (empresas de tecnologia financeira) ou o cliente que recebe propostas de novos serviços por novos atores? Em suma, o direito bancário ilustra, assim, perfeitamente, os desafios atuais do direito dos dados pessoais. Eles são um elemento da vida privada ou um valor patrimonial? Como conciliar o privado e o comércio? O direito positivo parece trazer uma resposta mista. Nos próximos tópicos se examinarão questões com parte das respostas. Será frisado que, se a segurança dos dados bancários parece ter sido assegurada, o mesmo não acontece com a comercialização desses dados.



### 3. Proteção dos dados bancários versus compras integradas

A proteção de dados bancários é o primeiro desafio do desenvolvimento de sistemas de compras integradas, uma vez que ela é do interesse de todos os agentes envolvidos. Essa exigência foi levada em conta tanto pelas autoridades responsáveis pela proteção de dados, quanto por aquelas que são responsáveis pelo direito dos serviços de pagamento.

#### 3.1. A proteção assegurada pelo direito da proteção dos dados pessoais

Trata-se de uma questão global. A segurança dos dados relacionados é efetivada por meio de normas técnicas que, fatalmente, conseguirão se impor em todo o mundo. Não obstante, é importante que haja efetividade das normas jurídicas – mesmo locais – para a mesma finalidade. Um exemplo aclara a questão, no caso francês. A *Commission nationale de l'informatique et des libertés* (Comissão Nacional de Informática e das Liberdades, CNIL) é uma importante guardiã da privacidade e das liberdades na França. Como não é de se estranhar, ela desempenhou um papel importante nessa área. A autoridade administrativa se encarregou rapidamente de um importante e exemplar caso e fez tudo que estava em seu alcance para resolver uma questão de violação de dados em sistemas de pagamentos.

No caso concreto, a CNIL rapidamente usou o seu poder de sanção contra um operador que não respeitava as regras impostas pela Lei francesa de proteção de dados: a *FNAC Direct*<sup>7-8</sup>. A decisão administrativa (Deliberação 2013-358, de 14 nov. 2013) alertou à *FNAC Direct* que é indispensável obter o consentimento das pessoas cujos dados bancários podem ser registrados. Segundo a decisão mencionada, o serviço de registro dos dados bancários, que permite evitar a reinserção pelo cliente de seus dados durante acessos subsequentes, deve ser diferenciado das modalidades de execução do contrato de venda ou do tipo de acesso em que os dados bancários foram fornecidos pela primeira vez. O

---

<sup>7</sup> LAUSSON, Julien. CNIL: des données bancaires stockées en clair sur Fnac Direct. Le monde. 27 jul. 2012. Disponível: <https://www.numerama.com/magazine/23287-cnll-des-donnees-bancaires-stockees-en-clair-sur-fnac-direct.html>. Acesso em: 9 jul. 2018.

<sup>8</sup> FRANCE: CNIL. Délibération de la formation restreinte n° 2012-214 du 19 juillet 2012 portant avertissement à l'encontre de la société X. Disponível: <https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT00026224040&fastReqId=770915872>. Acesso em: 9 jul. 2018.



tratamento de dados efetuado no âmbito das modalidades de execução de um contrato em que o titular dos dados é parte não exige, com efeito, o consentimento dessa pessoa nos termos do artigo 7º da Lei de Informática e Liberdades, da França (Lei de Proteção de Dados)<sup>9</sup>. O mesmo artigo 7º também estabelece que o consentimento não é obrigatório quando o tratamento de dados busca realizar o interesse legítimo perseguido pelo responsável ou pelo destinatário, desde que os interesses ou os direitos, assim como as liberdades fundamentais da pessoa em causa, não sejam violados. A CNIL também especificou, na citada Deliberação 2013-358, que convinha fixar e respeitar um período de conservação dessas informações bancárias. Segundo a autoridade administrativa, ainda, os dados deveriam ser mantidos de acordo com as melhores medidas de alta segurança. Em um segundo momento, ela emitiu uma recomendação sobre o uso de meios de pagamento<sup>10</sup>. No estado atual da legislação francesa, bem como dos procedimentos de pagamento, o propósito central da Deliberação da CNIL consistiu em especificar as recomendações da entidade administrativa às garantias mínimas que devem ser cumpridas pelas instituições quando os seus técnicos implementarem o tratamento de dados relativos aos cartões de pagamento.

A CNIL, assim, também deliberou sobre a coleta de dados bancários e não apenas sobre os procedimentos em relações de compra e venda. Segundo a decisão administrativa, durante qualquer transação, os dados que podem ser coletados são os seguintes: o número do cartão; a data de validade; e o criptograma visual. No que diz respeito à segurança dos dados, a CNIL considera que os estabelecimentos comerciais devem proteger todos os dados que permitam a criação de contas, sobretudo aqueles relativos ao cartão de pagamento, assim como as empresas devem proteger os servidores de estocagem e de transmissão, com o claro objetivo de evitar qualquer utilização fraudulenta desses dados, especialmente após uma falha de segurança. A CNIL recomenda, por fim, na Deliberação 2013-358, a necessidade do estabelecimento de meios de autenticação reforçada do titular do cartão de pagamento para garantir que foi ele mesmo quem deu origem ao ato de pagamento à distância.

---

<sup>9</sup> FRANCE. Loi n° 78-17, relative à l'informatique, aux fichiers et aux libertés (Lei 17/1978, relativa à informática, aos arquivos e às liberdades), 6 jan. 1978. Disponível: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20180201>. Acesso em: 9 jul. 2018.

<sup>10</sup> FRANCE: CNIL. Délibération n° 2013-358 du 14 novembre 2013 portant adoption d'une recommandation concernant le traitement des données relatives à la carte de paiement en matière de vente de biens ou de fourniture de services à distance et abrogeant la délibération n° 2003-034, 19 jun. 2003. Disponível: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028275157>. Acesso em: 9 jul. 2018.

A adaptação de disposições jurídicas de proteção, extraídas de normas gerais tem um motivo claro. Tanto o novo Regulamento Geral de Proteção de Dados<sup>11</sup>, quanto a Lei de Informática e Liberdades<sup>12</sup>, da França, não contêm dispositivos específicos para proteção dos dados bancários. Assim, talvez seja necessário esperar pela interpretação e pela atuação administrativa por parte da CNIL. Tal reação deve ocorrer em breve, uma vez que – como já indicado acima – tanto as normas jurídicas europeias, quanto a legislação francesa, determinam meios jurídicos de proteção, tais como a obrigação de comunicar ao titular qualquer violação de seus dados pessoais.

### **3.2. A proteção dos dados bancários assegurada pela Lei dos serviços de pagamento, de 2013**

O conjunto do direito francês aplicável aos serviços de pagamento é afetado diretamente pelo desenvolvimento tecnológico das compras integradas por meio de aplicativos de Internet<sup>13</sup>. As autoridades demonstraram capacidade de resposta, pois apesar de a legislação francesa ter sofrido diversas reformas, ela está prestes a ser reformulada novamente pela transposição da DSP 2<sup>14</sup>. A proteção de dados bancários é o resultado de uma dupla ação. Por um lado, é necessário que todos os atores estejam sujeitos às mesmas restrições; por outro

---

<sup>11</sup> UNIÃO EUROPEIA: Parlamento Europeu e Conselho. Regulamento (UE) 2016/679, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), 27 abr. 2016. Disponível: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679>. Acesso em: 9 jul. 2018.

<sup>12</sup> FRANCE. Loi n° 78-17, relative à l'informatique, aux fichiers et aux libertés (Lei 17/1978, relativa à informática, aos arquivos e às liberdades), 6 jan. 1978. Disponível: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20180201>. Acesso em: 9 jul. 2018.

<sup>13</sup> O direito francês referente aos meios de pagamento está consolidado no Code monétaire et financier. FRANÇA. Code monétaire et financier. Disponível: <https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006072026>. Acesso em: 9 jul. 2018.

<sup>14</sup> Nota do revisor técnico. O presente artigo foi escrito em 2016. A transposição do DSP 2 ao direito francês ocorreu em 2017. Houve profunda modificação do Code monétaire et financier em razão dessa transposição. FRANÇA. Ordonnance n° 2017-1252, portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, 9 ago. 2017. Disponível: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000035394629>. Acesso em: 9 jul. 2018.

lado, é necessário que as regras aplicáveis sejam reforçadas para garantir a segurança máxima do setor.

A abertura para novos prestadores, em relação aos serviços antes típicos dos bancos, no que diz respeito aos serviços de pagamento, já ocorreu, como indicado antes. Em uma reforma anterior, uma nova categoria de partes interessadas foi inserida no sistema, aquela dos prestadores de serviços de pagamento, como, por exemplo, as operadoras de telefonia móvel. O artigo L311-2, inciso I, item 8, do *Code monétaire et financier* (Código Monetário e Financeiro), com a redação dada pela Ordenança 2013-544, de 27 jun. 2013, define como “operadores conexos às operações bancárias” as emissoras e gestoras de moedas eletrônicas, por exemplo.

A prática recente trouxe novos atores que são puros produtos da Internet. Os serviços de agregação de informações permitem que os clientes de vários bancos se beneficiem de uma visão consolidada de todas as suas contas em uma única interface. Os serviços de iniciação de pagamento permitindo que o cliente solicite a um terceiro que apresente e execute transações de pagamento aos bancos em seu nome<sup>15</sup>. Não obstante, esses novos serviços podem criar riscos. De fato, se retomarmos o exemplo dos serviços de agregação de informações, a centralização das informações com as quais eles operam, requer acesso às contas *online* para fazer o *download* das informações diretamente dos vários bancos. É por esse motivo que se designam como agregadores de informação. Se alguns prestadores de serviços oferecem funções análogas de acordo com as instituições de crédito e segundo seus processos de autenticação, a maioria contenta-se em pedir aos clientes os dados de autenticação para os diferentes sistemas bancários *online* para poder representá-los nas diversas operações

Embora este modo de gestão seja indubitavelmente mais simples para o usuário e, ainda, que ele permita ao prestador de serviços de informações sobre contas centralizar os dados, ele é, no entanto, juridicamente questionável sob vários aspectos. Observe-se também que a operação de agregação é idêntica no que concerne aos serviços de iniciação de pagamento. Nesse caso, assim como na agregação, o prestador recebe os meios de autenticação, permitindo o reconhecimento do cliente pelo seu prestador de pagamento e agindo no lugar deste último. Até então, apesar da existência técnica do serviço, não havia normas jurídicas sobre eles. Em suma, todos esses novos atores – intermediários – poderiam, em tese, representar uma ameaça à segurança dos dados bancários dos seus clientes.

---

<sup>15</sup> Nota do revisor técnico. Essas modalidades de serviços de pagamento vieram a ser integradas no artigo L314-1 do *Code monétaire et financier* (Código Monetário e Financeiro), em 2017, como citado anteriormente.

A Diretiva (UE) 2015/2366 conseguiu regular esses casos por meio da criação de uma nova figura jurídica: o prestador de pagamento externo. Ela exige a obtenção prévia de uma autorização expedida por uma autoridade competente para oferecer tais serviços e que a supervisão desses novos operadores seja feita do mesmo modo que a de qualquer prestador de serviços de pagamento. Mas, ao mesmo tempo, a Diretiva pretende aumentar a concorrência no mercado de pagamentos, o que pode soar contraditório. Várias disposições da Diretiva refletem esse desejo de regular esses novos atores (artigos 66 e 69, por exemplo). Estas disposições seriam suficientes?

A *Fédération bancaire française* (Federação Bancária Francesa, FBF) expressou sua preocupação, ressaltando o fato de que a segurança de pagamentos seria um grande problema para os bancos<sup>16</sup>. Entretanto, os novos ingressantes no mercado não podem se tornar um fator de enfraquecimento. Duas fraquezas podem ser destacadas: de um lado, os requisitos cautelares para que os terceiros, prestadores de serviços de pagamento, obtenham a autorização do estabelecimento são insuficientes. De outro, o acesso às contas por meio de identificadores bancários apresenta um sério problema de segurança. Esse modo de conectar-se com os bancos representa um risco sistêmico à rede bancária e aos clientes. Além disso, ele também põe em causa a mensagem de segurança transmitida aos clientes por seus bancos com relação ao caráter estritamente confidencial de seus identificadores.

Três propostas foram, então, formuladas pela *Fédération bancaire française*: (1) todos os prestadores e atores dos meios e serviços de pagamento deveriam estar sujeitos ao mesmo nível de requisitos relativos à segurança e à supervisão de dados; (2) todos os prestadores e atores dos meios e serviços de pagamento deveriam assumir os mesmos deveres e se beneficiar dos mesmos direitos; e (3) todos os prestadores e atores dos meios e serviços de pagamento deveriam compartilhar equitativamente as responsabilidades no uso dos dados bancários de seus clientes.

Deve-se ver nessas propostas uma reação dos bancos para se tentar limitar a entrada de concorrentes? O que é certo é que o novo panorama – trazido pela Diretiva (UE) 2015/2366 – irá beneficiar os Gigantes da Internet. Eles terão, agora, a possibilidade de recorrer a agentes especializados ou a possibilidade de se converterem, eles próprios, em partícipes na cadeia de pagamentos, assumindo, portanto, a condição de entidades de crédito, de prestadores de serviços de pagamento ou, ainda, de prestadores de serviços de pagamento terceirizados. Em

---

<sup>16</sup> FÉDÉRATION bancaire française. La révision de la Directive Services de Paiement, 9 out. 2015. Disponível: [http://www.fbf.fr/fr/espace-presse/fiches-reperes/la-revision-de-la-directive-services-de-paiement-\(dsp2\)](http://www.fbf.fr/fr/espace-presse/fiches-reperes/la-revision-de-la-directive-services-de-paiement-(dsp2)). Acesso em: 9 jul. 2018.

suma, seja qual for o seu *status*, o pagamento será considerado juridicamente seguro.

De acordo com esses desenvolvimentos iniciais, parece que o cliente não deve temer a explosão de novos métodos de pagamento e de novos prestadores, já que, em qualquer caso, os seus pagamentos estarão seguros e, se tal não for o caso, ele não terá que suportar as consequências. Parece razoável concluir que – atendidos os rigores técnicos e jurídicos – será verossímil afirmar que todos os atores envolvidos terão alguns interesses convergentes. Tal não é o caso, entretanto, quando se trata de questionar a comercialização de dados bancários, como será visto na próxima seção. Em relação a esse último tema, os interesses dos Gigantes da Internet, sejam ou não prestadores de serviços de pagamento, são claramente opostos aos dos clientes, no que tange aos seus dados bancários.

#### 4. Os riscos de comercialização de dados bancários

A segurança dos dados é um desafio. Não obstante, a limitação da comercialização dos dados coletados é um dos mais claros e novos desafios, trazidos pelo desenvolvimento da Internet e pela digitalização das relações sociais e econômicas. Isso se deve ao fato de que o modelo econômico de desenvolvimento de todos os atores, tradicionais ou novos, depende da exploração desse novo sedimento de valores – os dados pessoais. Já é notório que os gigantes da Internet estão tentando tirar proveito dos dados bancários recuperados ou, ainda, querem comprá-los daqueles que os possuem ou que estabeleceram um perfil do cliente<sup>17</sup>.

Podemos supor que a proteção do interesse do cliente não será necessariamente uma prioridade. Quando os bancos detinham o monopólio, o cliente era protegido pelo sigilo bancário quase absoluto, mas esse tempo já passou. Como, então, garantir a proteção do detentor de dados? A resposta deve ser buscada em duas direções. A primeira direção é observar a proteção que poderia resultar da aplicação da legislação bancária. A segunda direção seria olhar a proteção que poderia advir da legislação referente aos dados pessoais. As respostas, todavia, parecem incompletas, imprecisas ou inadequadas em ambos os casos.

---

<sup>17</sup> VINCENT, Claude. La ruée vers l'or des données personnelles. LesEchos.fr, 7 mar. 2013. Disponível: [https://www.lesechos.fr/07/03/2013/lesechos.fr/0202599460114\\_la-ruée-vers-l-or-des-donnees-personnelles.htm](https://www.lesechos.fr/07/03/2013/lesechos.fr/0202599460114_la-ruée-vers-l-or-des-donnees-personnelles.htm). Acesso em: 16 jul. 2018.

## 4.1. A proteção insuficiente da legislação bancária

A legislação bancária é duplamente inadequada para oferecer proteção jurídica no nível abstrato que seria ideal. De um lado, o sigilo bancário não parece cobrir todos os usos possíveis dos dados pessoais, como será visto no primeiro tópico dessa seção. De outro lado, a lei atual e o debatido projeto para uma nova lei dos serviços de pagamento<sup>18</sup> está plena de lacunas, como será indicado no segundo tópico.

### 4.1.1. A proteção insuficiente do sigilo bancário (*secret bancaire*)

Obviamente, os dados bancários deveriam ser protegidos pelo sigilo bancário. Porém, imediatamente surgem duas questões. A primeira: quais dados bancários estão sujeitos ao sigilo bancário? A segunda: quem é obrigado a proteger o sigilo bancário? No que se refere ao objetivo do sigilo bancário, não há, infelizmente, certezas, em relação às respostas. O sigilo bancário é conhecido como sigilo profissional, ou seja, ele não está definido de forma clara e simples<sup>19</sup>. A única informação puramente confidencial atingida pelo sigilo bancário, no contexto francês é o montante de um saldo, de um crédito, vinculado em uma conta. Assim, o nome, o registro e o local da sede social do titular estão cobertos por outro sigilo: o profissional. Para o leitor estrangeiro, faz-se necessário transcrever o dispositivo:

Art. L511-33

I. Todo membro de um conselho de administração e, conforme aplicável, de um conselho fiscal, bem como toda pessoa que, a qualquer título, participe da direção ou da gestão de um

---

<sup>18</sup> Nota do revisor técnico. O presente artigo foi escrito em 2016. A transposição da DSP 2 ao direito francês ocorreu em 2017. Houve profunda modificação do Code monétaire et financier em razão dessa transposição. FRANÇA. Ordonnance n° 2017-1252, portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, 9 ago. 2017. Disponível:

<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000035394629>.

Acesso em: 9 jul. 2018.

<sup>19</sup> Nota do revisor técnico. O conceito de sigilo bancário na França, de acordo com o Code monétaire et financier, é coberto pelo sigilo profissional (*secret professionnel*), definido nos artigos L511-33 e L511-34. Eles foram alterados pela transposição ao direito francês da DSP 2, como mencionado na nota anterior. Será utilizada a redação posterior à incorporação da DSP 2 ao direito francês.

estabelecimento de crédito ou de um organismo mencionado no item 5 do artigo L. 511-6 ou aquele que está empregado por algum desse possui dever de sigilo profissional.

Além dos casos previstos em lei, o segredo profissional não pode ser oposto contra a Autoridade de Controle Prudencial e de Resolução, nem contra o Banco Central da França, nem contra o Instituto de Emissão dos Departamentos Ultramarinos, nem contra a autoridade judiciária que atua no âmbito de uma ação criminal, nem contra as comissões de inquérito criadas pela aplicação do artigo 6 da Ordenança n° 58-1100, de 17 de novembro de 1958, relativo ao funcionamento das assembleias parlamentares.

Os estabelecimentos de crédito e as sociedades de financiamento podem, ao revés, comunicar as informações acobertadas pelo sigilo profissional, por um lado, às agências de avaliação para a finalidade de avaliação dos seus produtos financeiros e, de outra parte, às pessoas com as quais elas negociem, concluindo ou executando as operações abaixo listadas, desde que essas informações sejam necessárias para estas:

1° Operações de créditos efetuados, diretamente ou indiretamente, para um ou mais estabelecimentos de crédito ou sociedades de financiamento;

2° Operações sobre instrumentos financeiros, de garantias ou de seguro destinadas à cobertura de um risco de crédito;

3° Investimentos de capital ou de controle no âmbito de um estabelecimento de crédito, de uma empresa de investimentos ou de uma sociedade de financiamento;

4° Cessões de ativos ou de fundos de comércio;

5° Cessões ou transferências de contas à receber ou de contratos;

6° Contratos de prestação de serviços concluídos com um terceiro em vista de lhe confiar funções operacionais importantes;

7° Para avaliar ou elaborar qualquer tipo de contrato ou de operação, desde que as pessoas pertencem ao mesmo grupo empresarial que o autor do estudo.

Além dos casos expostos acima, os estabelecimentos de crédito podem comunicar as informações acobertadas pelo sigilo profissional, caso a caso, somente quando as pessoas interessadas fornecerem expressamente a permissão para tanto.

As pessoas que sejam receptoras das informações acobertadas por sigilo profissional, as quais lhes tenham sido fornecidas para as finalidades das operações acima listadas, devem conversar sua confidencialidade, seja a operação finalizada, ou não. Em todos os casos, na hipótese de que a operação supramencionada seja finalizada, essas pessoas receptoras podem, por sua vez, transmitir as informações acobertadas pelo sigilo profissional, nas mesmas condições que são referidas no presente artigo, para outras pessoas com as quais elas negociam, firmem ou executem operações referidas anteriormente.



O conceito de sigilo profissional protege as informações relativas à pessoa do cliente, bem como suas coordenadas, acaso essas se tratem de informações precisas. É o que ocorre com informações que podem ser quantificadas. A abrangência legal do sigilo bancário deveria ser entendida de modo mais amplo? Nesse sentido, o sigilo bancário deveria se estender aos outros elementos deduzidos a partir do estudo da conta? Ou, ainda, ele deveria acobertar as análises do perfil do cliente estabelecido pelo próprio banco? Nada é menos certo, com base no exame da legislação. No caso da segunda pergunta feita antes: quem são os destinatários a observância jurídica do sigilo bancário? Eles estão definidos no art. L511-13-1 do Código Monetário e Financeiro (*Code monétaire et financier*), ou seja, trata-se das usuais instituições de crédito. O dever do sigilo profissional, assim, não se aplica aos outros prestadores.

Ainda, cabe notar que a proteção resultante do sigilo profissional pode ser enfraquecida pela possibilidade oferecida ao cliente de suprimir o sigilo bancário. Em um caso concreto, uma cláusula desse tipo não foi considerada abusiva por decisão judicial. Por meio desse acórdão, o Tribunal aceitou a validade de uma cláusula pela qual um cliente autorizava seu banco a compartilhar os dados que lhe diziam respeito com qualquer entidade do mesmo grupo bancário, para fins de prospecção comercial, ou ainda, permitia o compartilhamento dos dados em agrupamentos de empresas. A autorização também se referia ao direito de comunicar os dados aos institutos de sondagem para fins estatísticos. O direito do cliente foi respeitado na medida em que ele havia dado sua autorização prévia e que ele tinha o direito de retirá-la a qualquer momento. Os contratos de conta, incluem, assim, uma autorização para uso dos dados bancários. Os arquivos eletrônicos podem, portanto, ser explorados pelos bancos assim que forem declarados à CNIL.

#### **4.1.2. A proteção insuficiente da Lei de serviços de pagamento**

Os regulamentos europeus existentes – ou em preparação – provavelmente não protegerão os detentores dos dados, ou seja, as pessoas interessadas. O projeto de Regulamento sobre os serviços de pagamento é omissivo<sup>20</sup>. O artigo 94 da

---

<sup>20</sup> UNIÃO EUROPEIA. Regulamento Delegado (UE) da Comissão, que complementa a Diretiva (UE) 2015/2366 do Parlamento e do Conselho no que respeita às normas técnicas de regulamentação relativas à autenticação forte do cliente e às normas abertas de comunicação comuns e seguras. Disponível: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R2055>. Acesso em: 6 jul. 2018.

Diretiva sobre Serviços de Pagamento autoriza o tratamento dos dados pessoais pelos sistemas de pagamento e pelos prestadores de serviços quando necessário para garantir a prevenção, investigação e a detecção de fraudes nos pagamentos. Cito:

Artigo 94 - Proteção de dados

1. Os Estados-Membros permitem o tratamento de dados pessoais pelos sistemas de pagamento e pelos prestadores de serviços de pagamento quando tal for necessário para salvaguardar a prevenção, a investigação e a detecção de fraudes em matéria de pagamentos. A informação das pessoas sobre o tratamento de dados pessoais e sobre qualquer outro tratamento de dados pessoais para efeitos da presente diretiva é efetuada nos termos da Diretiva 95/46/CE, das regras nacionais que transpõem essa diretiva e do Regulamento (CE) n.º 45/2001.
2. Os prestadores de serviços de pagamento só acedem aos dados pessoais necessários para a prestação dos seus serviços de pagamento, e só os tratam e conservam, com o consentimento expresso do utilizador de serviços de pagamento<sup>21</sup>.

A comunicação aos particulares de informações sobre o tratamento dos dados pessoais era, assim, realizada em conformidade com os termos da antiga Diretiva 95/46 CE – substituída pelo Regulamento (UE) 2016/679 (RGPD) – e com as normas nacionais que a transpuseram aos sistemas jurídicos dos Estados-membros. Ainda, essa comunicação ocorria em sintonia com o Regulamento (CE) 2001/45<sup>22</sup>. Esta é a cláusula usual de varredura (*clause balais habituelle*). O projeto DSP 2 não aborda a questão do marco jurídico para as práticas de oferta promocional relativas aos cartões de pagamento que permitem às instituições de crédito e de pagamento analisar as informações de compra eletrônica para subsidiar as suas operações de marketing e publicidade.

Tendo em vista essas deficiências do direito bancário francês e europeu, a expectativa de proteção mais forte somente poderá advir do direito de proteção dos dados pessoais. Afinal, essa é a primeira finalidade desse ramo jurídico.

---

<sup>21</sup> UNIÃO EUROPEIA. Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) 1093/2010, e que revoga a Diretiva 2007/64/CE. Disponível: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32015L2366&from=PT>. Acesso em: 1/8/2018.

<sup>22</sup> UNIÃO EUROPEIA. Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de Dezembro de 2000, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados. Disponível: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32001R0045>. Acesso em: 1/8/2018.

## **4.2. A proteção da comercialização por meio do direito dos dados pessoais**

Após visualizar a insuficiente proteção oferecida pelo direito bancário, pode-se postular que a comercialização de dados bancários – adquiridos ou comprados de terceiros – pode ser proibida pelas cláusulas gerais do direito de proteção de dados pessoais. Todavia, até mesmo com esse parâmetro jurídico, atingir-se-ia um ponto delicado ou até mesmo incompleto. Um reforço protetivo pode ser encontrado na proibição de certas cláusulas, em razão de elas serem consideradas abusivas.

### ***4.2.1. Dados bancários protegidos no âmbito da proteção dos dados pessoais***

Os dados bancários, como todos os dados pessoais, constituem parte de uma esfera privada, ao mesmo tempo em que perfazem um valor patrimonial. No âmbito dos dados pessoais, o grau de proteção pode depender da qualificação, portanto, que lhes é dada. É possível, desse modo, compreender que o debate sobre a qualificação dos dados pessoais seja essencial para o tema e, ainda, que seja um requisito prévio à definição de um regime jurídico de proteção.

#### ***4.2.1.1. A qualificação dos dados bancários como dados pessoais***

Essa qualificação ainda pressupõe muitas perguntas. A primeira diz respeito à delimitação de dados bancários qualificados como dados pessoais. Esses dados não estão expressamente definidos em nenhum texto. O Regulamento Delegado visa proteger apenas os dados econômicos, de identificação e de localização<sup>23</sup>. A proteção dos dados bancários seria melhor garantida se eles fossem qualificados como dados sensíveis, nos mesmos termos do direito de proteção dos dados pessoais. Essa qualificação é usada atualmente para os dados raciais ou religiosos. Por essa razão, consequências jurídicas importantes são extraídas dessa qualificação. Quando se referem aos dados bancários, essa

---

<sup>23</sup> UNIÃO EUROPEIA. Regulamento Delegado (UE) da Comissão, que complementa a Diretiva (UE) 2015/2366 do Parlamento e do Conselho no que respeita às normas técnicas de regulamentação relativas à autenticação forte do cliente e às normas abertas de comunicação comuns e seguras. Disponível: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R2055>. Acesso em: 6 jul. 2018.

possibilidade deveria, ao menos, ser debatida pelos juristas. Aliás, o Regulamento Geral de Proteção de Dados Pessoais é omissivo acerca desse assunto específico.

Por outro lado, a aplicação do Regulamento (UE) 2013/611, de 24 de junho 2013, relativo a medidas sobre a notificação das violações de dados pessoais nos termos da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho sobre privacidade e as comunicações eletrônicas poderia constituir um avanço, considerando-se os seus artigos 2º e 3º. O artigo 2º (1 e 2) desse Regulamento determina que “(...) o operador deve notificar todos os casos de violação de dados pessoais à autoridade nacional competente (...)”, “(...) no prazo de 24 horas após a detecção dessa violação, se possível”. O artigo 3º (1), determina que:

Caso a violação de dados pessoais seja suscetível de afetar negativamente os dados pessoais ou a privacidade de um assinante ou de outra pessoa, o operador deve notificar essa violação não só à autoridade nacional competente, como prevê o artigo 2.º, mas também ao assinante ou à outra pessoa em causa<sup>24</sup>.

Ainda, o artigo 3º (3) do Regulamento acima citado impõe que essa notificação “(...) ao assinante ou a outra pessoa em causa deve ser efetuada sem demora indevida após a detecção da violação de dados pessoais (...)” e que ela “(...) é independente da notificação da violação de dados pessoais à autoridade nacional competente, a que se refere o artigo 2.º (...)”<sup>25</sup>. Há apenas uma exceção para esse prazo restrito, no caso de haver a possibilidade de risco “(...) à eficácia da investigação da violação de dados pessoais (...)”, nos termos do item 5 do mesmo artigo 3º. No entanto, este avanço técnico e jurídico é frágil e até mesmo incerto. Por essa razão, foi emitido um parecer em prol de várias alterações no então projeto de DSP 2, por parte da Autoridade Europeia de Proteção de Dados<sup>26</sup>.

---

<sup>24</sup> UNIÃO EUROPEIA: Parlamento Europeu e Conselho. Regulamento (UE) n.º 611/2013 da Comissão, de 24 de junho de 2013, relativo às medidas aplicáveis à notificação da violação de dados pessoais em conformidade com a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho relativa à privacidade e às comunicações eletrônicas. Disponível: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:32013R0611>. Acesso em: 9 jul. 2018.

<sup>25</sup> Idem.

<sup>26</sup> UNIÃO EUROPEIA: Autoridade Europeia de Proteção de dados. Sumário Executivo do Parecer da Autoridade Europeia de Proteção de Dados sobre uma proposta de diretiva do Parlamento Europeu e do Conselho relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2006/48/CE e 2009/110/CE e que revoga a Diretiva 2007/64/CE, e uma proposta de Regulamento do Parlamento Europeu e do Conselho relativo a comissões de intercâmbio aplicáveis a operações de associadas a cartões, 5 dez. 2013. Jornal Oficial da União Europeia, Bruxelas, 8 fev. 2014. Disponível:

Não existe, portanto, qualquer definição específica na proposta de DSP 2. Por conseguinte, é compreensível que o Grupo Europeu de Peritos (*Trans Europe Experts*) da Sociedade de Legislação Comparada (*Société de Législation Comparé*) tenha proposto que os dados bancários sejam adicionados à lista de tipos de dados sensíveis que requereriam um tratamento especial contido no artigo 9º do Regulamento Geral de Proteção de Dados<sup>27</sup>. Foi também proposto que os intermediários não regulamentados que oferecem serviços de pagamento ou agem como intermediários de instituições bancárias também devem estar sujeitos a obrigações mais rigorosas no que diz respeito aos dados sensíveis que processam. Devido a essas incertezas, não é de se estranhar que o regime jurídico de comercialização de dados ainda esteja em construção.

#### 4.2.1.2. O regime geral e a proteção específica dos dados bancários

Tal como se encontra, em França, a comercialização de dados bancários está sujeita apenas ao direito geral da Lei de Informática e Liberdades<sup>28</sup>. Porém, uma evolução está em andamento. No ano de 2016 foi aprovado pelo Parlamento e pelo Conselho o novo Regulamento Geral de Proteção de Dados (RGPD). Tal diploma é aplicável ao setor bancário e financeiro, em seus termos gerais e dará continuidade ao acordo alcançado, em dezembro de 2015, pela Comissão, pelo Parlamento e pelo Conselho de Ministros da União Europeia. Ele será aplicado a todos os tratamentos de dados pessoais relativos aos residentes da União Europeia, inclusive se a organização de processamento dos dados não for sediada em seu território.

A transparência ocupa um lugar preponderante nessa legislação. O texto exige que as organizações forneçam informações detalhadas às pessoas sobre o tratamento de seus dados. Além disso, os responsáveis pelo tratamento têm novas obrigações. Mesmo se o atual sistema de envio de relatórios periódicos à autoridade administrativa de controle for suprimido, os encarregados deverão conservar os registros internos dos procedimentos que estão implementando. Além disso, eles terão de notificar as violações de dados para as autoridades

---

[https://edps.europa.eu/sites/edp/files/publication/13-12-05\\_opinion\\_payments\\_ex\\_sum\\_pt.pdf](https://edps.europa.eu/sites/edp/files/publication/13-12-05_opinion_payments_ex_sum_pt.pdf). Acesso em: 1/8/2018.

<sup>27</sup> MOREL-MAROGER, Juliette; ROUSSILLE, Myriam; STORRER, Pierre. Données et services bancaires. In: MARTIAL-BRAZ, Nathalie (dir.). La proposition de règlement européen relative aux données à caractère personnel: propositions du réseau Trans Europe Experts. Paris: Société de Législation Comparé, 2014, p. 414-416.

<sup>28</sup> FRANÇA. Loi 78-17, 6 jan. 1978, relative à l'informatique, aux fichiers et aux libertés. Disponível:

<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460>. Acesso em: 1/8/2018.

administrativas de controle e, também, para as pessoas interessadas, caso isso represente um risco. Se por um lado, há a fixação de mais obrigações, por outro lado, mais direitos são concedidos às pessoas interessadas, incluindo-se o direito de se opor a certos tipos de tratamento, como, por exemplo, quando pode haver consequências jurídicas ou afetar a pessoa de modo significativo. Um novo direito à portabilidade de dados também foi criado para facilitar a transferência de dados de um prestador para outro, quando isso for tecnicamente possível. Existe também a obrigação de se designar um encarregado pela proteção dos dados pessoais. Por último, o RGPD pretende ser inovador no que se refere ao processo de controle das regras de proteção de dados pessoais, destacando-se, em particular, a cooperação entre as várias autoridades administrativas dos Estados-membros.

O Regulamento Geral de Proteção de Dados (RGPD) foi aprovado no início de 2016 e entrou em vigor em 2018, cerca de dois anos após a data de publicação no Jornal Oficial da União Europeia. A aplicabilidade específica do Regulamento Geral do setor bancário vai depender ainda de uma construção jurídica e técnica. Um exemplo é a fixação de regime de conformidade para setores específicos, feita pela CNIL<sup>29</sup>. A formação de um pacote de conformidade para o setor bancário permitiria visualizar a questão de forma mais clara. Apesar das inovações, não é certo que essas novas regras jurídicas sejam suficientes, já que os contratos celebrados com os usuários de Internet tendem a construir a privação de algumas de suas prerrogativas. Teria sido mais oportuno que os dados bancários, assim como os dados de saúde, fossem tratados de um modo especial. Por essa razão, a proteção mais eficaz poderia advir da implementação do direito das cláusulas abusivas.

### 4.3. A proteção de dados bancários e o direito do consumidor (cláusulas abusivas)

A *Commission des clauses abusives* (Comissão de Cláusulas Abusivas, CCA), assim como a CNIL, rapidamente percebeu a dificuldade de proteção dos usuários. Foi elaborado um relatório sobre as cláusulas abusivas introduzidas nos contratos de uso ofertados pelos gigantes da Internet. Os dados bancários também foram objeto do documento<sup>30</sup>. A CCA e a *Direction Générale de la concurrence*,

<sup>29</sup> FRANÇA: Commission nationale d'informatique et des libertés. Les packs de conformité sectoriels. Disponível: <https://www.cnil.fr/fr/packs-de-conformite>

<sup>30</sup> FRANÇA: Commission des clauses abusives. Recommandation 14-02: contrats de fourniture de services de réseaux sociaux, 7 nov. 2014. Disponível: <http://www.clauses-abusives.fr/recommandation/contrats-de-fourniture-de-services-de-reseaux-sociaux-nouveau>. Acesso em: 1/8/2018.

de la consommation et de la répression des fraudes (Direção Geral da Concorrência, Consumo e Repressão às Fraudes, DGCCRF) tomaram medidas contra o Facebook<sup>31</sup>.

Após a CNIL, a DGCCRF, ou seja, o órgão administrativo francês de repressão contra as fraudes, notou a presença – nos termos de contrato – de cláusulas abusivas que criam um desequilíbrio significativo entre os direitos e as obrigações das partes, em detrimento dos usuários. Entre elas, incluem-se aquelas previstas na declaração de direitos e de responsabilidades da rede social e que conferiam ao Facebook o poder discricionário de remover conteúdo ou informações publicadas pelos usuários na sua rede. Também foi considerado abusivo o direito de alterar unilateralmente suas condições de uso sem que o usuário seja informado previamente ou tenha dado seu consentimento prévio. Nas condições relativas aos pagamentos feitos pelos usuários, a DGCCRF também considerou abusivas cláusulas tais como “o direito de modificar unilateralmente suas condições de uso sem informar previamente o consumidor”, ou ainda, “o direito de modificar ou rescindir unilateralmente o seu serviço de pagamento sem informar primeiro o consumidor”.

Os contratos entre o *Facebook* e seus usuários se referem, ao mesmo tempo, a duas empresas: o *Facebook Ireland Ltd.* e o *Facebook Payments International Ltd.* Por essa razão, foram essas empresas que acabaram sendo instadas pela DGCCRF a “remover ou alterar” no prazo de 60 dias, as “cláusulas contratuais consideradas abusivas em relação aos usuários não profissionais da rede social”. O cumprimento dessa determinação deveria acontecer sem prejuízo dos recursos administrativos ou judiciais de que dispõem essas empresas para contestar essa medida. O Facebook também foi notificado pela CNIL, que lhe pediu, sobretudo, para interromper o rastreamento de seus usuários fora dos limites das suas páginas e do seu serviço. Assim, a CNIL determinou um prazo de três meses ao *Facebook* para que o serviço respeitasse a francesa Lei de Informática e Liberdades no tocante aos procedimentos de coleta e de utilização dos dados dos seus usuários. Em síntese, os órgãos relacionados à proteção dos consumidores e as entidades de proteção de dados pessoais estão conseguindo manejar uma atuação sistemática do direito do consumidor e do direito da proteção de dados para fixar um regime protetivo. O mesmo processo pode ser imaginado em outros setores.

---

<sup>31</sup> BERNE, Xavier. Plusieurs clauses contractuelles de Facebook jugées abusives par la DGCCRF, 9 fev. 2016. Next Inpact. Disponível: <https://www.nextinpact.com/news/98461-plusieurs-clauses-contractuelles-facebook-jugees-abusives-par-dgccrf.htm>. Acesso em: 1/8/2018.



## 5. Conclusão

A transformação da economia contemporânea – na Europa e fora dela – passa necessariamente por um acelerado processo de digitalização e de modificação do cenário empresarial de prestação dos diversos serviços. Os legisladores europeu e francês têm se esforçado para produzir novas normas jurídicas com o objetivo de estimular essa transformação, sem abrir mão da necessária segurança que deve ser mantida. Tanto o direito bancário europeu, quanto o francês, contudo, não possuem, em si mesmos, uma capacidade protetiva completa em face do novo panorama das práticas comerciais eletrônicas, em especial, se for levada em conta a participação cada vez maior dos gigantes da Internet.

Assim, ao mesmo tempo em que existe uma evidente marcha regulatória no âmbito do tradicional direito bancário, outras áreas começam a ser atraídas para um espaço misto de normalização, como o direito empresarial, dos contratos, do consumidor, entre outros. As novas práticas de mercado – estimuladas pelo legislador, ou não – acabam por demandar soluções para lidar com novos desafios. O cenário de convergência regulatória ainda é incerto, uma vez que os processos de mudança estão em progressão. Porém, já é possível enxergar no horizonte um incontornável diálogo jurídico entre duas áreas específicas, como foi descrito no presente artigo.

Para que os direitos bancários europeu e francês possam proteger os consumidores e os usuários de serviços bancários, far-se-á necessária uma futura complementação desses ramos jurídicos pelo novo direito da proteção de dados. Esse novo ramo do direito deverá ter a capacidade de ser adaptado para regular e proteger situações muito diversas, do ponto de vista econômico e social. Ainda, parece evidente que a atuação administrativa dos órgãos responsáveis por sua observância, tal como a CNIL, será muito relevante para que sejam atingidos os desejados resultados em termos de proteção dos cidadãos, seja em face da digitalização das relações sociais e econômicas, seja em face da evidente força econômica das empresas digitais de caráter transnacional que, atualmente, são denominadas como as gigantes da Internet.

## 6. Referências bibliográficas

- BERNE, X. *Plusieurs clauses contractuelles de Facebook jugées abusives par la DGCCRF, 9 fev. 2016. Next Inpact*. Disponível: <https://www.nextinpact.com/news/98461-plusieurs-clauses-contractuelles-facebook-jugees-abusives-par-dgccrf.htm>. Acesso em: 1/8/2018.
- FÉDÉRATION bancaire française. *La révision de la Directive Services de Paiement, 9 out. 2015*. Disponível: [http://www.fbf.fr/fr/espace-presse/fiches-reperes/la-revision-de-la-directive-services-de-paiement-\(dsp2\)](http://www.fbf.fr/fr/espace-presse/fiches-reperes/la-revision-de-la-directive-services-de-paiement-(dsp2)). Acesso em: 9 jul. 2018.
- FRANÇA. *Code monétaire et financier*. Disponível: <https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006072026>. Acesso em: 9 jul. 2018.
- FRANÇA. *Loi n° 78-17, relative à l'informatique, aux fichiers et aux libertés (Lei 17/1978, relativa à informática, aos arquivos e às liberdades), 6 jan. 1978*. Disponível: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20180201>. Acesso em: 9 jul. 2018.
- FRANÇA. *Ordonnance n° 2017-1252, portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, 9 ago. 2017*. Disponível: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000035394629>. Acesso em: 9 jul. 2018.
- FRANÇA: Commission des clauses abusives. *Recommandation 14-02: contrats de fourniture de services de réseaux sociaux*, 7 nov. 2014. Disponível: <http://www.clauses-abusives.fr/recommandation/contrats-de-fourniture-de-services-de-reseaux-sociaux-nouveau>. Acesso em: 1/8/2018.
- FRANÇA: Commission nationale d l'informatique et des libertés. *Les packs de conformité setoriels*. Disponível: <https://www.cnil.fr/fr/packs-de-conformite>
- FRANÇA: Commission Nationale de l'informatique et libertés. *Délibération de la formation restreinte n° 2012-214 du 19 juillet 2012 portant avertissement à l'encontre de la société X*. Disponível: <https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id>

=CNILTEXT000026224040&fastReqId=770915872. Acesso em: 9 jul. 2018.

FRANÇA: Commission Nationale de l'informatique et libertés. ***Délibération n° 2013-358 du 14 novembre 2013 portant adoption d'une recommandation concernant le traitement des données relatives à la carte de paiement en matière de vente de biens ou de fourniture de services à distance et abrogeant la délibération n° 2003-034, 19 jun. 2003.*** Disponível: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028275157>. Acesso em: 9 jul. 2018.

LAUSSON, J.. ***CNIL: des données bancaires stockées en clair sur Fnac Direct. Le monde.*** 27 jul. 2012. Disponível: <https://www.numerama.com/magazine/23287-cnil-des-donnees-bancaires-stockees-en-clair-sur-fnac-direct.html>. Acesso em: 9 jul. 2018.

MOREL-MAROGER, J; ROUSSILLE, M.; STORRER, P.. Données et services bancaires. In: MARTIAL-BRAZ, Nathalie (dir.). ***La proposition de règlement européen relative aux données à caractère personnel: propositions du réseau Trans Europe Experts.*** Paris: Société de Législation Comparé, 2014, p. 414-416.

UNIÃO EUROPEIA. ***Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) 1093/2010, e que revoga a Diretiva 2007/64/CE.*** Disponível: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32015L2366&from=PT>. Acesso em: 1/8/2018.

UNIÃO EUROPEIA. ***Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de Dezembro de 2000, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados.*** Disponível: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32001R0045>. Acesso em: 1/8/2018.

UNIÃO EUROPEIA. ***Regulamento Delegado (UE) da Comissão, que complementa a Diretiva (UE) 2015/2366 do Parlamento e do Conselho no que respeita às normas técnicas de regulamentação relativas à autenticação forte do cliente e às normas abertas de comunicação comuns e seguras.*** Disponível: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R2055>. Acesso em: 6 jul. 2018

UNIÃO EUROPEIA: Autoridade Europeia de Proteção de dados. *Sumário Executivo do Parecer da Autoridade Europeia de Proteção de Dados sobre uma proposta de diretiva do Parlamento Europeu e do Conselho relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2006/48/CE e 2009/110/CE e que revoga a Diretiva 2007/64/CE, e uma proposta de Regulamento do Parlamento Europeu e do Conselho relativo a comissões de intercâmbio aplicáveis a operações de associadas a cartões, 5 dez. 2013*. Jornal Oficial da União Europeia, Bruxelas, 8 fev. 2014. Disponível: [https://edps.europa.eu/sites/edp/files/publication/13-12-05\\_opinion\\_payments\\_ex\\_sum\\_pt.pdf](https://edps.europa.eu/sites/edp/files/publication/13-12-05_opinion_payments_ex_sum_pt.pdf). Acesso em: 1/8/2018.

UNIÃO Europeia: Parlamento Europeu e Conselho. *Directiva (UE) 2015/2366, 25 nov. 2015, relativa aos serviços de pagamento no mercado interno*. Disponível: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32015L2366>. Acesso em 6 jul. 2018).

UNIÃO EUROPEIA: Parlamento Europeu e Conselho. *Directiva 2007/64/CE, 13 nov. 2007, relativa aos serviços de pagamento no mercado interno, que altera as Directivas 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE e revoga a Directiva 97/5/CE*. Disponível: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32007L0064>. Acesso em: 9 jul. 2018.

UNIÃO EUROPEIA: Parlamento Europeu e Conselho. *Regulamento (UE) 2016/679, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), 27 abr. 2016*. Disponível: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679>. Acesso em: 9 jul. 2018.

UNIÃO EUROPEIA: Parlamento Europeu e Conselho. *Regulamento (UE) n.º 611/2013 da Comissão, de 24 de junho de 2013, relativo às medidas aplicáveis à notificação da violação de dados pessoais em conformidade com a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho relativa à privacidade e às comunicações eletrônicas*. Disponível: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:32013R0611>. Acesso em: 9 jul. 2018.

VINCENT, Claude. *La ruée vers l'or des données personnelles*. LesEchos.fr, 7 mar. 2013. Disponível: [https://www.lesechos.fr/07/03/2013/lesechos.fr/0202599460114\\_la-ruée-vers-l-or-des-donnees-personnelles.htm](https://www.lesechos.fr/07/03/2013/lesechos.fr/0202599460114_la-ruée-vers-l-or-des-donnees-personnelles.htm). Acesso em: 16 jul. 2018.