

©2018 Centre of Studies in European Union Law
School of Law – University of Minho



Current issues over electronic commerce in Brazil: jertical integration between platforms and payment systems, personal data protection and international regulatory cooperation

Alexandre Veronese*
Marcelo Cunha**

ABSTRACT: This article focuses on the trending issues about vertical integration between payment systems and the electronic commerce platforms from a Brazilian perspective. It describes the increasing international electronic commerce and it indicates three kinds of potential risks to consumers: direct, indirect and social. It shows that vertical integration can bring some benefits, which are very difficult to measure due to the related risks. The article creates a model of the remote commerce based on an evolution of a typology of typical trade relations to shed some light over the current automatization. Afterwards, the article states that the leakage of personal information coupled with vertical integration is a major threat to electronic businesses. It describes two international cases of mass data leakage to demonstrate the difficulties faced by the national systems in regulating transnational electronic commerce and data protection. Then, the article performs an assessment of the Brazilian legal system to conclude that there is a grave lack of integration of the electronic commerce regulations and that there is an absence of international cooperation provisions designed for electronic commerce. It concludes that Brazilian law may benefit from international experiences of personal data protection, and that the new legal provisions must take in account the risks associated with internationalization and vertical integration.

KEYWORDS: electronic commerce – vertical integration – data protection – risks – Brazil.

* Professor of Social and Legal Theory at the Law School of the University of Brasilia (UnB), PhD in Sociology from the Institute of Social and Political Studies (IESP) of Rio de Janeiro State University (UERJ) and Head of the Telecommunications Law Research Group (GETEL UnB). ORCID: 0000-0002-2287-1005.

** Auditor at the Brazilian Court of Audit (TCU), Master of Law from the University of Brasilia (UnB), Researcher at GETEL UnB. ORCID: 0000-0001-9631-8256.

I. Introduction¹

Money exchange through electronic payment systems is an important engine for commercial relations between citizens and enterprises in the contemporary world.² The Internet has enabled e-commerce operations ranging from big retail electronic stores – e.g. Amazon –, to small suppliers, even clustered in collective vending systems – e.g. ETSY. However, the payments of these commercial relations almost exclusively take place through inter-banking systems and, in particular, via the use of a credit card. New electronic partners have appeared such as PayPal and PagSeguro UOL in Brazil, notwithstanding that both still base their systems on credit cards. Recently, the use of electronic currencies has grown stronger, such as Bitcoin.³

The central subject of this article is the understanding of the legal framework applicable to e-commerce in light of integration of purchase and sale systems and the means of payment. To discuss the Brazilian legal framework, it will be necessary to address the issue of bank data security and personal data protection. This issue is of special importance when we think about the risks posed to users by a possible integration between e-commerce suppliers and payment systems. Therefore, we could not separate the issue of the risks in commercial relations from the debate about contracts as we can see in the discussions that happen in the international forums dedicated to create transnational legal standards that apply directly to Internet trade.⁴ Thus, technological development has made contractual formation occur more and more remotely and incrementally without direct intervention of concerned parts, as Bruno Deffains and Jane K. Winn expose it. The Authors explain that, in the 1980s, exchange systems began to operate in real time and “*unlike telex or fax technology, it became possible for the first time to form contracts with nothing more than machine-to-machine communications*”.⁵ The problem has become clear since the regulatory concerns did not immediately follow the technological advances. Those concerns only became clear upon the next decade – the 1990s – and they have grown into a draft model-law as the one created by UNCITRAL (United Nations Commission on International Trade Law) especially for e-commerce.

¹The article develops ideas presented at the International Seminar on the “Effectiveness of Law in Light of the Internet Giants’ Power” organized by the University of Brasília (UnB), the Fluminense Federal University (UFF), the Paris Descartes University (Paris 5), the University of Paris 1 – Panthéon Sorbonne and the University of Versailles Saint-Quentin-en-Yvelines from April 13 to 15, 2016. The Authors are especially grateful to Professor Dominique Legeais from Paris Descartes University (Paris 5) for the debate that was crucial to this final version of the article. The Authors are also thankful to the Brasília Federal District Research Support Foundation (FAPDF), to the Brazilian Foundation for the Coordination of the Superior Education Personnel (CAPES) and to the French Embassy in Brazil.

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

⁴ United Nations Conference on Trade and Development, “Developing electronic commerce legislation”, accessed May 17, 2018, http://unctad.org/en/Pages/DTL/STI_and ICTs/ICT4D-Legislation.aspx.

⁵ Bruno Deffains and 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.

After that initial time, the doubts began to spread and the debate evolved to solutions that tried to mesh legal uncertainty problems – the former focused on the debate about electronic contracts – and technical security ones, the latter related to cryptography and information systems. We can describe the contemporary international panorama by the radicalization of two facts. The first fact is the rapid increase of supplier chains whose operation is completely automatic and electronic. That fact has a huge impact on the expansion of B2B (business to business) e-commerce relations. The second fact is the expansion of the direct e-commerce among the small suppliers model business; the B2C (business to consumers) became widespread. However, there is a tendency that such small B2C use big market companies – e.g. Amazon or e-Bay – as intermediaries or brokers. Therefore, the market experiences a tendency towards concentration in a few Internet giants. Nevertheless, there is still some space for some C2C (consumer-to-consumer) commerce. Nonetheless, the consumer's dependence on the broker big platforms puts some doubts over some optimistic visions of a potential downstream market (horizontal).

At the core of this process is the vertical integration of electronic payment methods with e-commerce tools. Vertical integration possesses some advantages in terms of costs, security and reliability related to the gains of scale provided by the big companies' investment power. Thus, at the beginning, an Internet platform that carries out more e-commerce transactions could invest more in security systems because of its greater profit margin. A large brokerage firm could also offer lower prices to its users, since the gains of scale would potentially lower its costs. Actually, the vertical integration of e-commerce and payment could bring some potential advantages directly to the suppliers and indirectly to the consumers. In terms of companies' advantages, they could lower their operation costs, since they would spend less money on brokerage services such as credit card operators and other electronic payment solutions. The users could enjoy some indirect advantages either by experiencing faster transactions or by perceiving the reduction of costs and risks.

However, there are never potential advantages without some risks. The first ensemble of risks go straight to the users. It resides in personal and bank information leaks. In this paper, the description of two international large-scale leak cases highlight the risk of keeping personal and banking information on storage systems from service and product providers. In the leak cases committed by frauds against companies, the harm to the users is direct. However, it is somewhat difficult to prove the guilt of the companies, which are victims of the fraudster's actions after all. The second ensemble of risks is indirectly assigned to users. It is the threat of potential improper use of their banking and personal information by Internet intermediaries, providers, e-commerce brokers or electronic payment systems. The users' bank information – together with the information about the purchases made by them – can serve as an element to increase the companies' profit when they use them in targeted marketing operations, for example. The third and last ensemble of risks goes on society. It refers to the threat that new integrated purchase systems can offer to national banking systems and the potential offenses against competition law.

To explore those three ensembles of risks, the first part of the article analyses the cryptography and Internet privacy issues to underline the technological and legal challenges faced when establishing security measures on social and economic relations via networks operated with open protocols and with wide interconnection. The

first part of the paper concludes that social trust is the key element to guarantee the proper functioning of commercial relations and that this subject needs much more legal awareness. The second part of the article analyses two international cases of banking data leaks and draws a speculative parallel with the new scenario of privacy and cryptography issues on the Internet after the Edward Snowden case of 2013.⁶

The last part of the article focuses on Brazilian law, highlighting the current legislation and its applicability to personal and banking data leak situations. The analysis of Brazilian law leads to two main conclusions. The first conclusion relates to the national jurisdictional limits to achieve standards of protection against fraud and damages when dealing with global commercial relations. It points the lack of success of the current legal Brazilian framework especially when compared to the European Union model based on the Directive 2000/31/EC (electronic commerce) and on the Directive 95/46/EC (personal data protection). The General Data Protection Regulation (Regulation 2016/679/EU) has recently replaced the former Directive on personal data protection. The second conclusion focuses the necessary utilization of the judicial cooperation systems as a means to the end of strengthening the international commerce – and foreign users. The judicial cooperation will be a global necessity in order to develop a more reliable regulatory system to grant secure commercial relations.

II. Privacy, cryptography and social trust

The subject of retention of banking and credit data by intermediaries is central to contemporary e-commerce development. That topic directly connects to encryption and its uses in commercial trade through the Internet. It is clear that cryptographic systems are at the core of the security of the exchange information debate, especially after the social trust problem that emerged with the Edward Snowden case (2013)⁷ and the recent Cambridge Analytica case (2017-2018). In this section, we will initially discuss the evolution of the trade systems in general to demonstrate that the operation of modern commerce has always relied on brokers and intermediaries. After that description, we will reach the current point in which it will be possible to understand the difficulty in establishing a reliable brokerage mode applicable to the new e-commerce systems. It is usual to state the solution to the problem and risks in electronic commerce with advanced cryptography.⁸ Unfortunately, the possibility of third parties collecting and analysing a massive amount of data somewhat increases the fear of frauds and potential illegal practices on Internet. Both the Edward Snowden revelations and the Cambridge Analytica case pose a new questions agenda.⁹

The national and international banking systems have their own rules regarding security of transactions made between them and their clients as well, and between their clearing and remittance systems. It is easy to notice that several national banking systems have invested a lot in encryption systems to increase the confidence

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 and Paul A. Pavlou, “Perceived information security, financial liability and consumer trust in electronic commerce transactions”, *Logistics Information Management* 15 (2002): 358-68. Pauline Ratnasingham, “The importance of trust in electronic commerce”, *Internet Research* 8 (1998): 313-21.

⁹ Markus Jakobsson, ed., *The death of the Internet* (New Jersey: John Wiley & Sons, 2012).

level on clients' transactions as indicated by Marc Lacoursière and Édith Vézina on the Canadian situation.¹⁰ In 2007, the Authors mentioned that there was a need for greater legal regulation of the Quebec's trade systems to provide security to consumers regarding local banks. They pointed, in particular, to the fragility of the Canadian provincial legal system in comparison to the international ones on the aspect of granting more security to local banking users in order to enhance their sense of confidence. They conclude that, in 2007, the Canadian banking sector would have less interest in such development. To face their hypothesis, the Authors emphasized that the clearing international systems (BIC/SWIFT), which operate as a worldwide bank and a banking relations register¹¹, were using public key cryptography methods with great success and that this system should be widely used in Canada. In the Brazilian case, the solution came from the same technical path. The Brazilian National Institute of Information Technology (ITI) manages the National Public Key Infrastructure (ICP-Brazil). This system has been a suitable tool used in the Brazilian financial and banking sector, which has invested many resources in computerizing its communication systems over the years.¹²

However, if this article's exposition continued towards banking systems, it would divert from its original subject since our focus is not the analysis of the Brazilian banking systems or any other financial operators in their usual functions. The main point of this paper is to ponder about the existence of risks to consumers banking – and credit card – data managed by third parties (merchants or electronic systems) in the context of commercial operations. The abstract model presented in this paper aims to highlight the importance of the broker role on commercial transactions and to understand the current paradigm in which e-commerce innovations emphasize the three ensembles of risks mentioned at the introduction – direct, indirect and social risks. This model considers three basic abstract types of remote consumer transactions, which show the complexity of contemporary business practices.

The first type of remote shopping is the old system based on catalogs in which the customer places the order via traditional mail or telephone. In that type, catalogs offer products and services in lists. The customer can order and pay with various methods. The consumer accessed the product catalog and purchased them by means of postal (or bank) check or even by means of a previous bank deposit. In a remote past, the purchase of foreign books in Brazil has taken place in this way. The consumer contacted directly a bookseller or a publisher from another city or country and ordered the desired book. Another way was to search for a bookseller that had several catalogs and served as a trusted broker usually charging for this service.

This first type of remote shopping evolved into a second one in which consumers accessed information from physical or online catalogs. Suppliers were no longer contacted via physical stores, mediate systems or via traditional payment systems. As the relation began to take place directly, it became necessary to use different means of payment. In the previous type, there was no retention of any

¹⁰ Marc Lacoursière and Édith Vézina, "La sécurité des opérations bancaires par Internet", *Revue Juridique Thémis* 41 (2007): 89-156.

¹¹ Susan V. Scott and Markos Zachariadis, *The Society for Worldwide Interbank Telecommunication (SWIFT): cooperative governance for network innovation, standards and community* (London: Routledge, 2014). Susan V. Scott and Markos Zachariadis, "Origins and development of SWIFT, 1973–2009", *Business History* 54 (2012): 462-82.

¹² Alberto Luiz Albertin, "Comércio eletrônico: um estudo no setor bancário", *Revista de Administração Contemporânea* 3 (1999): 47-70.

client banking data by the supplier. However, in the new model, the supplier receives credit card data to carry out the transaction. In an initial moment, there were not even electronic machines for credit cards billing. Card numbers were copied into the commercial transaction invoice. Yet, there was trust that the supplier would not use again the card numbers for another purchase. This system evolved. At first, it uses telephone, or facsimile or traditional mail means. Afterwards, the electronic mail was the mean of communication of the credit card numbers. It was a past phase to the current moment with electronic purchases in automated systems.

The contemporary systems differ from the previous for a simple reason: it has become an entirely automated and digital system. All types, however, use the same logic, which still prevails: the existence of a consumer and a supplier sharing trust to effect a monetary exchange involving the commercial relation. Noteworthy, that old systems have become digital. Therefore, the security issues have gained a complex dimension due to two elements. First, suppliers have some database to hold the banking information stock. The second element relates to the intrinsic risks of Internet data transmissions. Both elements merge into an increasing possibility of damage occurrence and mostly they mesh into the additional difficulty in holding one of concerned parts accountable for eventual frauds or violations. The table below summarizes all three models in an abstract appreciation of their potential risks.

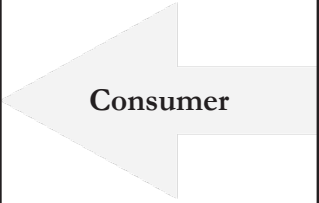
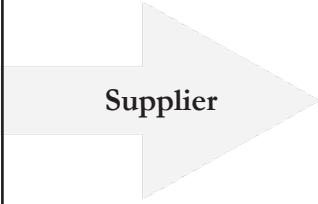
Figure 1. Abstract models of indirect customer relationship

Means of information	Business relationship mode	Monetary exchange system	Information storage by supplier	Assessment of risks to users / consumers
Indirect physical catalog	In person with third-party	Payment in person	No	Low risk, because the buyer performs the operation in person
Direct physical catalog	Letter or telephone	Check or bank deposit	No	Low risk, because the operation consumes the means (check, e.g.) during the transaction
Direct physical catalog	Letter or telephone	Credit card data	Maybe	High risk, because the merchant can retain the consumers data
Catalog in website	Email, after a website access	Credit card data	Maybe	High risk, because merchant can retain the consumers data
	Website access	Bank transfer	No	Moderate risk, because operation goes through the bank system, but can a third party may illegally access it
Catalog by cell phone terminal	Mobile app	Credit card data	Maybe	High risk, because merchant can retain the consumers data

What is important to retain from all abstract types indicated above is the

existence of two main factors that never change in the evolution of the remote purchases system. The first factor is the existence of a transaction system managed by a third party, either a bank or a credit card operator, to accomplish the commercial relation. The second factor is the possibility of data retention by third parties during the billing moment. A simplification is indicated in the figure below.

Figure 2. Brokerage abstract models

	Broker	
 Consumer	Bank - cash	 Supplier
	Bank - check	
	Bank - transfer	
	Card - personal use	
	Card - indirect and physical	
	Card - indirect and remote	

To summarise, there is always an intermediary or broker between the consumer (purchaser) and the supplier in modern purchasing relations. Thus, even in commercial transactions paid in cash, the national monetary system serves as a broker. After all, bills (banknotes) are legal commitments that some money will be paid. What is the liability for using a fake bill (banknote) to conduct a transaction? In case one of the parties has knowledge, of course, the responsibility for using fake bills (banknotes) relies on the one acting with the absence of good faith in the transaction. However, using fake bills (banknotes) with a devious intent is sometimes hard to prove. In that case, who will be liable? Will it be the consumer purchaser or the supplier? The blame usually falls on who owns and uses the disreputable mean. A large part of the problem merges intrinsically meshed with the confidence and the trust that both parties have with the intermediary or broker. The liability of the broker is crucial to the legal debate on this matter because this is central to the wellness of the contracts' resolution.

Nevertheless, we need to see contemporary issues that demonstrate the risks' perception and how they relate with confidence and trust. The first is the possibility of the consumer's data retention in supplier databases, which has become especially true due to the widespread credit cards usage. The second is the future emergence of more-than-integrated purchase systems: the use of monetary transactions systems, in which the suppliers are also users and owners of a once third-party system. In other words, it is the potential development of integrated purchase systems in which the supplier is also the controller of the monetary transaction system.¹³ Therefore, that integration between the suppliers and purchase systems change the scales of the distribution of liabilities because the merged system will also absorb both kind of rights and duties. If the supplier keeps the users' bank and personal data, it could share some degree of liability for some eventual damages. However, if the enterprises controls both the systems, their liability will considerably grow. To examine those two

¹³Thierry Dissaux, "Paiements, monnaie, banque électroniques: quelle évolution pour la banque?", *Revue d'économie financière* 53 (1999): 113-32.

issues, as well as supplier systems rights and duties, we will describe two international data leakage cases. Notwithstanding, it will be important to mention a little about cryptography before. The cryptographic systems are the daily technological means to grant the security of transactions in order to increase user and consumer trust.

In a previous paper about the organization of the Brazilian national digital certification system, Christiana Freitas and Alexandre Veronese have already argued that cryptography has a subtle issue within itself: citizens' right to keep secrets from the State, other citizens or enterprises. In addition, the paper dealt with the State's right to access to some person's information and, thus, ensure social, economic and legal relations security.¹⁴ In a simplified form, the kind of cryptography that has relevance to the contemporary debate is based on digital certification systems whereby, apart from compelling a huge computational capacity use for unauthorized content decoding, it is possible to authenticate the messages sender and receiver. The systems both encrypt data and authenticate the end-line users. For this purpose, such systems use asymmetric cryptographic algorithms in public key systems. The technical process uses also provide the inviolability guarantee by authorized third parties – public-key infrastructures (PKI) – being subject to constant audit in their operations. In Brazil's case, the National Institute of Information Technology (ITI) manages the ICP-Brazil system. The ITI is an agency within the Chief of Staff Office of the Brazilian Presidency of the Republic. The Brazilian digital certificate system grants and audits the operation of several technical subsystems used by the Brazilian banking system, for example. Therefore, the Brazilian national banking transactions use this system. However, what about international transactions? To reflect on that issue, the next section of this article will approach two well-known international cases of leakage of banking data held by electronic service providers.

III. Two banking data leak cases with transnational impacts

Due to online purchases and banking transactions via Internet, as well as to the existence of weaknesses in stored information security mechanisms, the occurrence of personal data leak cases has intensified all around the world. Given the high number of individuals affected in different countries and due to their legal repercussions, it is relevant to describe two emblematic cases. The first case was the personal data leakage from the PlayStation Network, in 2011, which reached around 77 million users' accounts.¹⁵ The PlayStation Network is an online gaming service accessed via Internet from several countries in which it is possible to purchase and to download games and other types of apps and media. In addition, this service allows game play within other network associates. Sony Corporation owns the PlayStation network and also develops and manufactures the videogame consoles for it. In addition, in its current generation – PlayStation 4 –, it is imperative to have a network account to play online matches. Many Internet services are going through the same path. Microsoft and Apple are demanding accounts and it is sometimes mandatory that the users provide their credit card information.

According to Sony's official statement, between April 17th and 19th, 2011, a

¹⁴ Christiana Freitas and Alexandre Veronese, "Segredo e democracia: certificação digital e software livre", *Informática Pública* 8 (2007): 9-26.

¹⁵ "Sony PlayStation suffers massive data breach", *Reuters*, April 26, 2011, accessed March 26, 2016, <http://www.reuters.com/article/us-sony-stoldendata-idUSTRE73P6WB20110426>.

non-authorized invasion of the PlayStation Network and Qriocity service, also maintained by this company, had successfully obtained personal data from their associates, which included at least name, address, country, email address, date of birth, login information and network access password.¹⁶ Sony did not exclude the possibility of data theft related to means of payments, such as credit card number and expiration date. The company also announced emergency measures in response to the cyber-attack. In this regard, the company interrupted both services and hired an external consultancy to investigate the incident. Sony stated that it also took some technical measures to increase network infrastructure security focusing on the user's personal data protection. In early May 2011, Sony resumed some of PlayStation Network services and offered to its associates compensation that included free game downloading and thirty days of differentiated services accessing.¹⁷

In the United States, lawyers filed several class actions demanding compensation for damages against Sony. After a brief time, there was a consolidation of all the judicial cases into one major class action, and Sony reached, in 2014, an agreement that avoided the final trial. That agreement predicted benefits to affected users that included financial compensation, free games and free offers to online services access depending on the type of subscription that each affected individual had at the cyber-attack time. However, it all took place without Sony recognizing any corporate responsibility for the event. The media estimated that the amount paid reached 15 million US dollars.¹⁸ The PlayStation Network case also caught the attention of several agencies in different countries, especially focusing on the effectiveness of Sony's personal data security policies and some possible regulation improvements in this subject. Also, in 2011, the US House of Representatives Energy and Commerce Committee questioned Sony about the leak, the company policy to protect data, privacy, and the consumer's compensation plan.¹⁹ In the United Kingdom, an independent administrative agency responsible for regulating personal data protection fined Sony in 250 thousand pounds sterling.²⁰ The Privacy Commissioner of Canada, who is the official responsible for reporting the state of privacy laws enforcement to Parliament, highlighted the global characteristic of PlayStation Network's leak case and the substantial extension of damages to its customers worldwide. In the 2011 annual report, he stated the need to regulate such kinds of business environments.²¹

¹⁶ "Sony customer notification US States (excluding Puerto Rico and Massachusetts)", Sony Computer Entertainment, 2011a, accessed March 26, 2016, <http://us.playstation.com/news/consumeralerts>.

¹⁷ "Some PlayStation Network and Qriocity services to be available this week", Sony Computer Entertainment, 2011b, accessed Mar. 26, 2016, <https://blog.eu.playstation.com/2011/05/01/some-playstation-network-andqriocity-services-to-be-available-this-week>.

¹⁸ "Sony settles PSN hack lawsuit for \$15 million", ZDNET, July, 24, 2014, accessed April 5, 2016, <http://www.zdnet.com/article/sony-settles-psn-hack-lawsuit-for-15-million>.

¹⁹ "Sony's Response to the U.S. House of Representatives", Sony Computer Entertainment, May 4, 2011, accessed April 5, 2016, <http://blog.us.playstation.com/2011/05/04/sonys-response-to-the-u-s-house-ofrepresentatives>.

²⁰ Information Commissioner's Office of the United Kingdom, "Data protection rights: what the public want and what the public want from data protection authorities", May, 2015, accessed April 5, 2016, <https://ico.org.uk/media/about-the-ico/documents/1431717/data-protection-rights-what-the-public-want-andwhat-the-public-want-from-data-protection-authorities.pdf>.

²¹ 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", June, 2012, accessed April 5, 2016, https://www.priv.gc.ca/information/ar/201112/2011_pipeda_e.asp.

Another global scale personal and banking data leak case, which became notorious especially for causing personal embarrassment to victims, was the Ashley Madison social network breach. In this case, millions of users had their contact data and means of payment information published on several websites. Ashley Madison is a paid access social network in which married individuals seek to know people and to establish love affairs, obviously extramarital. The Canadian company Avid Life Media manages this Internet service. It stated to have more than 44 million registered users in 53 countries, in 2016. The company also stated to be the global leader on discreet meeting for married people. In Brazil, the Ashley Madison network has approximately three million registered users.²² In addition, in France, newspapers pointed that this network has between 330 thousand and 700 thousand users.²³

According to a report by Avid Life Media on its official website, in July 2015 there was a cyber-attack to its systems and non-authorized access to Ashley Madison network user's information.²⁴ In addition, the company informed that it took security measures in its network to cease the attack and that it was working with governmental agencies to investigate the criminal offence. News reported that a hacker group named The Impact Team was responsible for Ashley Madison attack. That hacker group threatened to leak user's personal data including names, real addresses, sexual fantasies and credit card numbers, if Avid Life Media did not cease operating its social network.²⁵ Avid Life Media's subsequent official statements affirmed that this attack was not an act of hacker activism, but a criminal one.²⁶ In addition, it offered a 500 thousand Canadian dollars reward for information that could lead to author's identification.²⁷ The company's president resigned a month after the attack.²⁸ Afterwards, the hackers leaked some files of Ashley Madison user's personal and banking data in the web. Besides the identity of married people seeking for extramarital relations, they revealed a large number of that network's female users were possibly nothing more than cybernetic robots. The network used these robots to simulate conversations.^{29/30} In addition, the disclosure of user names

²² "Ashley Madison reúne 3 milhões de brasileiros 'para traição'; SP lidera", *TECHTUDO*, July 22, 2015, accessed April 2, 2016, <http://www.techtudo.com.br/noticias/noticia/2015/07/ashleymadison-reune-3-milhoesde-brasileiros-para-traicao-sp-lidera.html>.

²³ "Ashley Madison leak could affect large number of European users", *Deutsche Welle*, August 24, 2015, accessed April 2, 2016, <http://www.dw.com/en/ashley-madison-leak-could-affect-large-number-of-europeanusers/a-18669182>.

²⁴ "Statement from Avid Life Media", Avid Life Media, July 20, 2015, accessed April 9, 2016, <http://media.ashleymadison.com/statement-from-avid-life-media-inc-july-20-1225pm>.

²⁵ "Extramarital affair website Ashley Madison has been hacked and attackers are threatening to leak data online", *Business Insider*, July 20, 2015, accessed April 9, 2016, <http://www.businessinsider.com/cheatingaffair-website-ashley-madison-hacked-user-data-leaked-2015-7>.

²⁶ "Statement from Avid Life Media", Avid Life Media, August 18, 2015, accessed April 9, 2016, <http://media.ashleymadison.com/statement-from-avid-life-media-inc-august-18-2015>.

²⁷ "Statement from Avid Life Media", Avid Life Media, August 24, 2015, accessed April 9, 2016, <http://media.ashleymadison.com/statement-from-avid-life-media-august-24-2015>.

²⁸ "Statement from Avid Life Media", Avid Life Media, August 28, 2015, accessed August 9, 2016, <http://media.ashleymadison.com/statement-from-avid-life-media-august-28-2015>.

²⁹ "Ashley Madison condemns attack as experts say hacked database is real", *The Guardian*, August 19, 2015, accessed April 9, 2016, <https://www.theguardian.com/technology/2015/aug/19/ashley-madisons-hackedcustomer-files-posted-online-as-threatened-say-reports>.

³⁰ "Ashley Madison Code Shows More Women, and More Bots", *GIZMODO*, August 31, 2015, accessed April 9, 2016, <http://gizmodo.com/ashley-madison-code-shows-more-women-and-more-bots-1727613924>.

caused some cases of suicide.³¹ In the same way as in the PlayStation case, lawyers filled several class actions in Canada – the company’s headquarters country – and in the United States. In the first country, two law firms sued for 576 million dollars in compensation of damages in behalf of Canadian network users.³²

Both cases illustrate how companies with transnational commerce activity that manipulate sensitive personal and banking data with millions of users in tens of countries are still vulnerable to leaks and to cyber-attacks. The websites that hold the consumer’s sensitive information, like their user’s credit card number or extramarital cases, have a duty to shield privacy rights ensured by the different jurisdictions in which they operate. In that sense, as highlighted in this article, the rapid evolution of information and communication technologies applied to online transactions cannot ignore the need of implementing more security. It is clear that some of that effective security will need to rely on the most advanced cryptography technical measures. In the same way, it will be necessary to redesign many of the national legislations on consumer relations in order to adapt them to contemporary international e-commerce. They must consider the virtual environment in which those operations now take place and its inherent risks, create security obligations to companies and ensure compensation for victims of personal and banking data leaks. In the next section, there is a description of the current Brazilian legislation as well as some of the main proposals in discussion related to personal and banking data protection in transactions via Internet.

IV. The Consumer Protection Code and the Internet Legal Framework Statute³³ for the Internet: e-commerce regulations in Brazilian law

Brazil has a Consumer Protection Code, which rules on consumer relations in the country: Federal Statute 8,078 was signed into law on 11 September 1990. This statute conveys rules protecting the consumer, defining them as a physical (singular) person or legal entity that is the final user of a purchase or use of products or services, within a paid contract. The Consumer Protection Code deals with consumer-supplier relations in general and it rules about civil liability related to consumer damages caused by defects on products or services. Therefore, the Code also determine rules to deal with abusive commercial practices and illegal contractual clauses.³⁴ In Brazil, these consumer protection rules affect commercial relations regardless of the environment in which they occur.³⁵ The Brazilian Federal Decree number 7,962 dated 15 March 2013, created specific legal provisions concerning e-commerce contracting,

³¹ “Toronto police investigating possible Ashley Madison suicides”, *Fortune*, August 24, 2015, accessed April 9, 2016, <http://fortune.com/2015/08/24/ashley-madison-suicide>.

³² “Ashley Madison faces huge class-action lawsuit”, BBC, August 23, 2015, accessed April 9, 2016, <http://www.bbc.com/news/business-34032760>.

³³ Some authors translate this statute as “Brazilian Civil Rights Framework for the Internet” or “Civil Rights-based framework for the Internet”. Alexandre Veronese and Noemy Melo once used the expression “Internet Civil Legal Framework”: Alexandre Veronese and Noemy Melo, “O Projeto de Lei 5.276/2016 em contraste com o novo Regulamento Europeu (2016/679 UE)”, *Revista de Direito Civil Contemporâneo* 14 (2018): 71-99. Notwithstanding, the translation on this article is better, since the statute cover both civil (private) and public provisions.

³⁴ Claudia Lima Marques, *Confiança no comércio eletrônico e a proteção do consumidor* (São Paulo: Editora Revista dos Tribunais, 2004).

³⁵ Ricardo Luis Lorenzetti. *Comércio eletrônico* (São Paulo: Editora Revista dos Tribunais, 2004).

in addition to the Code.³⁶ The Decree provides standards to electronic consumer relations, demanding clear information about products, services and suppliers, ease of access to the consumer help service and determines that the consumer has the right to cancel the contract within seven days, counting the day after the purchase (“the right of regret”). Another important rule concerns the implementation of effective security measures for the treatment of payment and the use of consumer data by online shopping websites or broker systems (Article 3, subsection VII of the Decree). Thus, Brazilian law expressly determines that suppliers must adopt security systems to prevent the leaking of the consumer’s personal and banking data. Non-compliance with such obligations may result in administrative penalties (Article 56 of the Consumer Protection Code) and lawsuits. There are some special civil procedural rules to protect the consumers from pleading in court (Articles 81 to 90 of the Code). It is also possible to file liability lawsuits and class actions to pursue against the damages raised from consumer relations (Articles 91 to 100 of the Code). Therefore, the Brazilian legal system provides for administrative penalties and damages compensation due to non-compliance of supplier’s and their failure to adhere to the obligation of safeguarding consumer personal and banking data. For this reason, Ellen Sartori considers that the country already has a legal framework to protect the consumer’s personal data, although she demands a more detailed and comprehensive legislation, similar to the European model.³⁷

Furthermore, other Brazilian statutes seek to protect personal and banking data on the Internet and to refrain deliberate leaks. The Internet Legal Framework Statute – Brazilian Federal Statute number 12,965, dated of 23 April 2014 – partly regulates the Internet in the country, providing several rules to users, to companies and to government agencies. It expressly indicates the freedom of speech as a foundation principle for the use of Internet in Brazil (Article 2). It also states the protection of privacy and personal data as principles (Article 3, subsections II and III). Moreover, the Internet Legal Framework Statute establishes several rights to the users in the country in its Article 7. Subsection I grants the guarantee of intimacy and privacy. Subsection III determines the inviolability and secrecy of the user’s stored private communications. Also, subsection VII states the right of non-disclosure to third parties of users’ personal data, including their connection records and their records of access to internet applications, unless with their express, free and informed consent or in accordance with the cases provided by law. In Article 8, the Internet Statute grants the guarantee to the right of privacy and to freedom of speech as a necessary condition for the full exercise of the right to access to the Internet. It also asserts as unlawful the contractual clauses that violate the secrecy of private communications. Article 8 also declares as void the contractual clauses that forbids the resolution of disputes in Brazil. Regarding the protection of personal data and the content of private communications, as well as the storage and disclosure of an Internet application’s connection and access logs, the Internet Statute provides, in Article 10, for protection of intimacy, privacy, honor and image of involved parties. It also determines that security and confidentiality measures and procedures shall

³⁶ Têmis Limberger, Jânia M.L. Saldanha and 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.

³⁷ 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.

be informed in a clear manner, and must fill any regulation standards (Article 10, paragraph 4).

Whether an operation of collection, storage or treatment of personal data takes place in the Brazilian territory, Article 11 of the Internet Statute states that there must be compliance to Brazilian law. When at least one of the terminals is in Brazil, this rule of jurisdiction also applies. In addition, the Brazilian jurisdiction applies if the data was collected in the national territory. This even applies to activities carried out by a legal entity placed abroad, if it offers services to the Brazilian public or at least one enterprise of the same economic group is in Brazil (Article 11, paragraph 2). The Internet Statute also requires that Internet connection and application providers disclose information concerning compliance with Brazilian legislation (Article 11, paragraph 3) and it leaves for future regulation to specify oversight procedures (Article 11, paragraph 4).

The Internet Statute prescribes administrative penalties for infringements of its rules, apart from other possible civil, criminal and administrative punishments (Article 12). Those penalties may be isolated or cumulative applied: a warning, fine, temporary suspension and prohibition to exercise activities of storage and treatment of logs or personal data. That Statute also provides that if the fault comes from a foreign company, its subsidiary, branch, office or establishment in Brazil, will be jointly responsible for paying the fine (Article 12). Thus, the Internet Statute imposes obligations for Internet service providers and products suppliers to preserve confidentiality of personal data, whether there is a consumer relation and whether the legal entity is based in Brazil, as long as it offers its services in the country. It also creates its own penalty system, which can be cumulatively applied with sanctions from the Consumer Protection Code and other applicable civil liabilities and criminal sanctions.

The Brazilian legislation also establishes criminal punishments to personal data leaks on the Internet, as stated in Brazilian Federal Statute No. 12,737, dated 30 November 2012, which became known as “Carolina Dieckmann Act” in remembrance of a Brazilian actress who was victim of blackmail and leakage of intimate photographs on the Internet. That case had considerable impact in Brazilian media.³⁸ This Statute included in the Brazilian Criminal Code the crime of “computing device invasion” (Article 154-A), which can impose the punishment of imprisonment from three months to one year combined with a fine. It also imposes the same punishment on whoever “produces, offers, sells or disseminates a device or computer program” for that purpose (Article 154-A, paragraph 1). However, Brazilian law does not consider the act of invading a computing device without the intent of obtaining, adulterating or destroying data or gaining illicit advantages as a crime. The penalty shall be increased if an invasion causes economic losses (Article 154-A, paragraph 2). The penalty shall also be increased if the captured data is covered by confidentiality or relates to private electronic communications, trade or industrial secrets, or the invasion results in remote control of the device under attack. In such cases, the penalty shall be imprisonment from six months to two years combined with a fine if the conduct is not considered a more serious crime (Article 154-A, paragraph 3). The penalty shall also be increased if there is disclosure, commercialisation or

³⁸“Carolina Dieckmann prestará depoimento sobre publicação de fotos íntimas”, *Folha de São Paulo*, May 6, 2012, accessed March 26, 2016, <http://www1.folha.uol.com.br/ilustrada/1086411-carolina-dieckmann-prestaradepoimento-sobre-publicacao-de-fotos-intimas.shtml>.

transmission of obtained data to third parties (Article 154-A, paragraph 4) or the victim is one of the listed authorities in Article 154-A, paragraph 5. The “Carolina Dieckmann Act” also amended Article 298 of the Brazilian Criminal Code, which describes the crime of “forgery of private documents” in order to include credit and debit cards within the concept of private documents, thus criminalizing the use of leaked banking data.

It is important to show that Brazilian law seeks to establish legal provisions to protect the confidentiality of personal and banking data in an ever-changing technological environment. The expansion of types of means of payment in electronic transactions brokered by telecommunications devices and managed by non-financial institutions is a spreading phenomenon across different jurisdictions and it demanded the creation of specific legal rules in Brazil. Articles 6 to 15 of the Federal Statute No. 12,865, dated 9 October 2013, allowed telecommunications companies to offer payment services through mobile phones as a way of promoting financial inclusion policies. That Statute also demands the protection of personal data in the operation.

The technological evolution enables social inclusion through information and communication technologies, but it brings new challenges for companies, to States and to societies. There are many technical issues as, for example, the burden of developing communication structures to support the expansion of e-commerce.³⁹ On the other hand, sales of virtual services and products bring other challenges, since the delivery and use of the acquired products or services are entirely provided by electronic means.⁴⁰ However, the most relevant and urgent current issue relates to the security of personal and banking information. This central issue appears to be manifold as we shall consider the escalation of virtual financial operations and the growing number of actors, systems and devices related to online transactions. In the Brazilian case, there are some legal rules that may be useful on that matter. However, effective consumer protection relates not only to the existence of legal provisions. It relies completely on the social use by all the parties involved. Therefore, the legal principles such as those provided by the Consumer Protection Code and the Internet Legal Framework Statute will only be regarded as legal means of protection when the different social actors to guide their relations effectively use them. Nevertheless, it seems clear that those statutes are not enough to generate a comprehensive normative set and Brazil still requires a specific legislation for personal data protection. The standards must be similar to those that are in place in Europe through Directive 2000/31/EC (electronic commerce) and Directive 95/46/EC (personal data protection) replaced by Regulation (EU) 2016/679 (General Data Protection Regulation).⁴¹

The main objective of this article is to demonstrate that collection of banking data into automated systems managed by corporate conglomerates or corporations increase the risk of massive leaks. Several countries, including Brazil, have limited means of repression against those risks. On the other hand, the preventive control of those integrated purchasing systems is also complex. An effective control system

³⁹ Allain Rallet, “Commerce électronique ou électronique du commerce?”, *Réseaux* 106 (2001): 17-72.

⁴⁰ Fabrice Lequeux and Allain Rallet, “Un Internet peut en cacher un autre: vers l'avènement des marchés du multimédia en ligne”, *Réseaux* 124 (2004): 207-44.

⁴¹ Laura Schertel Mendes and 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.

would rely upon transnational cooperation systems for its proper operation. It is true that national banking systems have a cooperative regime, which is able to provide confidence in international trade. However, even systems as SWIFT are under scrutiny of national authorities of personal data protection due to risks related to money laundering and terrorism.⁴² In summary, the debate on the vertical integration of e-commerce structures is still incipient and it has not yet focused on issues related to the aggregation of transaction systems to the supply systems. In general, the current academic literature still addresses whether it is appropriate to integrate the offer of digital content to the means of provision, an issue known as net neutrality.⁴³ It is evident that the future regulatory risks relate to the vertical and international integration of e-commerce, as to say, the constitution of corporate conglomerates that aggregates the sale of goods and services with the payment systems.

V. Conclusion

This paper described a contemporary problem related to e-commerce: the integration between automated commercial transaction systems and the supply of goods and services. At first, it mentioned the quantitative expansion of e-commerce and its relation to the automatization of trade. It presented a typology of the evolution of transaction systems to highlight the increased risks of leaks in concentrated systems. It cited two international leak cases – Sony PlayStation and Ashley Madison – to demonstrate the potential of massive and extensive damages that may happen due to the large gathering of consumer's banking data in integrated purchasing systems. This exposition highlighted that an *a posteriori* legal defense against these violations is very complicated and that different countries have asymmetric means of defense against those violations. The study of Brazilian Law demonstrates that its contemporary legislation has some norms that grant preventive protection and seek to pursue the repression of violations within its national jurisdiction. Nevertheless, such legal prescriptions are dispersed in many different legal statutes and there are no rules providing for international cooperation and for the structuring of enforcing and protection measures.

To wrap up, this article points at two debates that must happen in Brazil. The first one is the establishment of a legal framework for personal data protection, which must integrate itself with the existing legal norms. It also must encompass an international cooperation system in accordance with European Law. The second one is the debate on risks of vertical integration between the means of transaction and the supply of goods and services via e-commerce, especially due to internationalization of corporations. Those questions were not fully addressed by the Brazilian National Congress on the approval of the Internet Legal Framework Statute, even though its explanatory memorandum mentioned this regulatory debate.

In fact, the use of payment systems in new business models with the integration between Internet access provision services and the financial sector is not a commercial option in Brazil yet. However, any future debate on the integration of e-commerce operations needs to face the cardinal issue of personal data protection. Such future

⁴² Anthony Amicelle, "The great (data) bank robbery: terrorist finance tracking program and the SWIFT affair", *Research Questions* 36 (2011), accessed April 9, 2016, <http://www.sciencespo.fr/cepi/en/content/great-data-bankrobbery-terrorist-finance-tracking-program-and-swift-affair>.

⁴³ Nicolas Curien and Winston Maxwell, *La neutralité d'Internet* (Paris: La Découverte, 2011).

debate must also focus on the problem of the competition protection, taking into account the international scenario. We can say that the debate cannot only take the Brazilian law perspective or not only just one national law point of view. It also requires the appreciation of the legal, economic and social frameworks of many different countries that have already held these discussions, in order to explore the possibility of legal cooperation as a way to mitigate the limits of local jurisdiction in disputes with large transnational companies.

What was the consequence of the Edward Snowden disclosure case in 2013? It was the growing concern from managers and technicians in the European Union about insufficient protection of the cooperation agreements of this social and economic bloc in relation to the United States of America. Those concerns led to a review of all European Union legislation about personal data protection. It has also served to expand the interest in increasing enforcement by several national authorities. It was for this reason that Liane Colonna depicted Europeans' reaction of immediate suspicion to the interaction between great companies of the United States of America and the government of that country and its reflection in European Union law on personal data protection.⁴⁴ From another perspective, Juhi Tariq stated his opinion that United States companies should be concerned about the changing panorama due to the Edward Snowden disclosure case.⁴⁵ With regard to Brazil, this major international affair seems not to have caught systematic attention from national legislators and regulators, although Alessandro Molon indicates that the approval of the Internet Legal Framework Statute would have been a consequence of this event⁵¹. In short, there is demand for regulatory debate on the dimensioning of banking and personal data national protection – through integrated legislation – to measure risks and potentialities of vertical integration processes that, nevertheless, are ongoing around the world in different markets. Yet, this debate must consider administrative and judicial cooperation as a focal point for the effectiveness of contemporary means of protection.

⁴⁴ Liane Colonna, "PRISM and the European Union's data protection directive", *The John Marshall Journal of Information Technology & Privacy Law* 30 (2013): 227-51, <http://repository.jmls.edu/jitpl/vol30/iss2/1/>.

⁴⁵ 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.
⁵¹ Alessandro Molon, "A legislação e a internet: ideais, desafios e avanços com o Marco Civil da Internet", *Cadernos Adenauer* 16 (2015): 107.