https://doi.org/10.58195/emi.v2i1.65

Global Science Publishing

EMI

Economics & Management Information

https://ojs.sgsci.org/journals/emi

Article

Digital Shadow and Its Legality Aspects

André Luís Cateli Rosa

Faculty of Business, University Center of Integrated Colleges of Ourinhos-SP, Ourinhos-SP 19909-100, Brazil

Abstract: It can be said that technology has enabled countless new forms of social relations, which has resulted in a reality that poses challenges to the most conservative sectors. It is in the face of this new scenario that the present investigation will address the concept of digital shadow, as well as the legality of its exploitation by suppliers in consumer relations, considering the right to privacy of consumers who use electronic equipment that transmit digital data. For this purpose, the deductive research method will be used. About the method of procedure, in this research the bibliographic method was used, with research in books, scientific journals and specialized websites on the subject. Finally, it was possible to foresee that the exploitation of consumers' digital shadow by suppliers is illegal.

Keywords: digital shadow; privacy; digital data

1. Introduction

With the arrival of the computer, the spread of mobile telephony and the implementation of broadband internet, profound transformations occurred in commerce and influenced consumer behavior, so that new technologies brought activities that were restricted to schedules and commercial points, such as lan houses, for example. From then on, the beginning of the cultural change that starts to assimilate the virtualization of the real can be seen [1].

It can be said that technology has enabled countless new forms of social relations, which has resulted in a reality that poses challenges to the more conservative sectors of legal science [2]. Its application to commercial relations resulted in new legal scenarios, different from the traditional context, which deserves attention mainly about consumer protection and defense.

The internet has significantly enhanced the scope and use of commerce, providing innovative legal relationships, as it allows not only the completion of the business by electronic means, but also the presentation of contractors and the formation of supporting documentation.

This potentialization is because the internet is a means of communication that allows the communication of many with many, at a chosen moment, on a global scale. It is a new world of communication, defined by Castells [3] as the “Internet Galaxy”, to which he attributes the modification of all domains of social life, given that communication is the essence of human activity.

In the words of Cláudia Lima Marques [4], the internet is “the new space for commerce in the world”. Through it, it is possible to search, order, pay, receive and use various items, such as books, music and other digital products, on portable devices that can be used anywhere, whether in the garden of your home, while shopping at the shopping center or supermarket, when using public transport, when moving by bus or

Received: 30 March 2023; Accepted: 12 April 2023.

* Corresponding: André Luís Cateli Rosa (andrecateli@gmail.com)

subway [5].

There is a new reality in which large suppliers can develop new cultures worldwide, given that the absence of borders, previously imposed by distance and now overcome by electronic transactions that bring everyone together through virtual platforms in time real, enables the dissemination of new products capable of awakening needs in consumers, henceforth shaping their culture, which is now increasingly globalized.

Undoubtedly, we live in a new era. Technological progress made it possible to reduce costs and opened the possibility of "building greater cooperation between all those involved in electronic commerce" [6].

However, the multiplication of electronic commerce and digital networks has facilitated the options for sharing information, knowledge, images, videos, music, among other resources, including consumers' personal data, at low cost and regardless of geographic distance [7].

This ease of sharing data presents a new legal reality in relation to people's intimacy and privacy, which can now be observed, analyzed and studied through their digital traces, left with each access they make on the internet, or even for the simple fact to carry a smartphone.

In this sense, it is up to the legal system to understand the new digital relationships and, in view of them, safeguard the right to privacy, which is a fundamental right, inserted among the personal rights that, due to its historical development, is classified as a fundamental right of the first generation.

This is because, in addition to being a subjective right, it is a positive and essential right in social organization, an institutional guarantee of pluralism and democracy, because if the public is governed by the pretense of equality, the private is at the origin of singularity.

Thus, respect for difference originally implies respect for private life and, therefore, can be considered as an expression or manifestation of freedom, as well as a consequence of human dignity in its condition as the foundation of political order and social peace [8].

The protection of this subjective right requires, then, the individual's knowledge of the existence and characteristics of the databases that have information related to him, so that the extension of the right to privacy, in a specific area such as the digital one, is capable of providing a solution, not for a new threat, but for a way of maintaining the development of digital relationships while preserving the intimacy and privacy of users of new technologies.

It is in the face of this new scenario that the present investigation will address the concept of digital shadow, as well as the legality of its exploitation by suppliers in consumer relations, considering the right to privacy of consumers who use electronic equipment that transmit digital data.

To do so, the deductive method will be used. About the method of procedure, in this research the bibliographic method was used, with research in books, scientific journals and specialized websites on the subject.

Finally, it was possible to foresee that the exploitation of consumers' digital shadow by suppliers is illegal.

2. Digital Shadow: a New Profile (Virtual)

Currently, because of technological advances and, mainly, the use of the internet, fundamental rights and freedoms are somehow threatened, given a new context different from the traditional one. The rights considered most vulnerable are those exercised through this network (the internet), such as freedom of expression, access to information, people's private lives, the secrecy of communications and the protection of personal data.

The right to privacy is threatened, in particular, with the proliferation of large databases, which are generated both by State infrastructure and by the private sector.

This does not mean that the right to privacy was born as a consequence of these new technologies, but rather that these are the creators of a new right to privacy, which even in the face of the same concepts and general parameters, starts to gain new peculiarities.

In a utopian sense, the advancement of information technology should be seen as a scenario of greater freedoms, as technology should not generate fear, but rather the hope of a greater degree of personal and professional development, with the respective growth and development in all areas. aspects.

However, the use of technologies in the information society and, mainly, through information technology,

has allowed tracking, storing, manipulating, matching, crossing, using and easily transmitting pieces of information about people, called "personal data" that can , to a greater or lesser extent and, depending on the use and purpose, negatively affect privacy, confidentiality of communications, honor, freedom of association, religious freedom or any other fundamental right, as well as other rights or interests protected by law . That's because the internet is the biggest showcase for data ever known, and consequently the main security threat of this data itself [9].

It is in this new scenario that the so-called Digital Shadow appears. Everything that is sent over the internet, from users' personal data in a purchase register to a photo posted on Facebook or Instagram, generates the so-called digital identity, even when browsing anonymously, given the possibility of capture of information through cookies.

These cookies are “data programs generated with the main purpose of identifying the user, tracking and obtaining useful data about him, especially based on navigation and consumption data” [10].

Souza and Amaral [11] clarify that cookies perform more than the user navigation tracking function. This is because there are several types of cookies, the most common being session cookies, first-party cookies and third-party cookies.

Session cookies are typically essential for navigation, as they constitute a website's short-term memory as the user moves from one page to another within its domain.

First-party cookies help websites to record information and settings when the user returns to visit a page in the future, allowing settings preferences to be saved, such as menu, themes, language selection, etc.

However, it is estimated that 70% of cookies are third-party cookies, originating from a different domain, offering no benefit to the user. Its use is for tracking, to “learn” about the user's browsing history, online behavior, consumption habits, among other things [11].

In this way, there is a lot of data that leaves traces while browsing the internet, and such data is captured and recorded in a way that the user is not even aware of it. The very fact of accessing the present study through the world wide web is enough to generate a digital trail.

Whether through the computer, smartphone or other digital devices, hundreds of digital traces are left daily: bits of information that are created, stored and collected.

When these digital traces are gathered, it is possible to create user profiles and even tell stories about them. The set of these traces, which makes it possible to draw conclusions about people, is what is currently known as digital shadow.

The “Me and My Shadow” Project points out that the digital shadow is built mainly through location tracking and navigation, adding that smartphones are extremely efficient trackers [12].

The same Project points out that location information collected over time can tell a surprisingly well-detailed story about the user and what their life is like. Adding to this the available public addresses, miscellaneous posts, photos and call logs, the shadow is even more complete.

Location information does not only reveal where you live and work, but also visits to the doctor, banks, universities, bars, friends' houses, etc.

This social mapping using location can also be done through cell phone towers, GPS tracking, location records, WIFI history, IP address, among others.

Every time you make or receive calls or text messages, for example, when communicating with cell phone towers, the location where the services were used is registered with the service providers and becomes part of the digital shadow of user.

In the same way, when activating the smartphone's location service, it works as a constant GPS, collecting records of all the places where it has passed.

Most applications installed on smartphones request access to the user's location with the justification of improving performance. When access is granted, the information is made available not only to the respective developers, but also to Apple or Google, through the APIs, depending on the operating system used.

Through Apple's IOS operating system, for example, the user himself has access to his location over time, information that is certainly also available to Apple itself, which can use it for various purposes.

To do so, just go through the following path in the IOS system: Settings → Privacy → Location Services → System Services → Important Locations → and select one of the recorded locations, which are the most frequent by the user. A map will be made available that even shows the number of times the user has visited the site over time.

This information, which is part of the digital shadow, allows Apple, for example, using algorithms, to identify where the user's home is (where he usually spends the night) and also where his work is (where he usually spends the day).

This digital shadow presents new vulnerabilities to the consumer, typical of the technological era, such as practices called geo-pricing and geo-blocking.

Geo-pricing consists of charging different amounts for the same product and/or service due to the geolocation of the consumer, favoring some over others [13].

By knowing the consumer's location (which is possible due to the geolocation provided by Internet access devices, such as smartphones, tablets, etc.), the supplier can assign different prices to its products and/or services, according to with the purchasing power of people in a particular region or country.

The practice has already been observed in sales of airline tickets and hotel rates. The company Decolar.com was punished for simultaneously offering the same hotel room at different prices to Brazilian and Argentine consumers (a value 49% higher for consumers located in Brazil). On that occasion, the practice of so-called geo-blocking was also verified, which is characterized by blocking the availability of the product or service for consumers of a certain location, while it is available for those of another.

It appears that geo-pricing and geo-blocking practices transcend consumer vulnerability. They go much further: they are likely to cause impacts on the market itself.

The geolocation made possible by smartphone-type devices allows suppliers, through the most diverse applications installed on consumers' devices, to explore their digital shadows and thus follow their routines in real time, such as consumption preferences and the route taken each day. Consumers are often not aware that they are being monitored, as they have agreed to a clickwrap-type adhesion contract, whose numerous mandatory adherence clauses for installing the application have not even been read.

The sudden change in the routine and preferences of consumers allows suppliers to identify, for example, that the consumer has lost his job, as he no longer makes that route daily, which theoretically increases the risk of defaulting on obligations assumed. Under these circumstances, it is natural for insurers to increase the price of insurance premiums and for credit houses to increase the interest rates on their lines of credit.

It appears that the internet has enabled the supply network subjects to act in new ways towards consumers, through the exploration of their digital shadows and contractual connectivity resulting from new economic needs that require different contractual forms from traditional legal types [14]. These are businesses typical of the current technological scenario. However, it is necessary to reflect on the legality of these practices.

3. Conclusion

The expansion of electronic commerce, resulting from new technologies, brought more dynamics to business relations, providing the transfer of the most diverse data in real time through the world wide web.

When surfing the internet, or even simply by carrying a smartphone in their pockets, consumers leave a digital trail, predominantly resulting from their browsing and location, capable of building their profile and stating their preferences, which is currently called digital shadow.

This digital shadow is often used by suppliers of products and/or services in order to implement more assertive commercial strategies, with the aim of seducing the consumer and leading him to the realization of consumption.

It was verified that the access and use of consumers' digital shadow by suppliers, as a rule, does not find express consent, which is done, when done, through accessions via clickwrap, which do not always express the real will of the contractor.

As a result, there was a need to rethink the right to privacy, taking into account these new electronic relationships and the current legal system.

Through the study of the legal system, it was possible to foresee that the exploitation of consumers' digital shadow by suppliers is illegal.

Funding

Not applicable.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

Data is available upon request from the corresponding author.

Conflicts of Interest

The authors declare no conflict of interest.

References

1 do Canto RE. *A Vulnerabilidade dos Consumidores No ComÉRcio Eletrônico: a Reconstrução da Confiança na Atualização do CÓDigo de Defesa do Consumidor*; Editora Revista dos Tribunais: São Paulo, Brazil, 2015; 20.

2 Cateli Rosa AL, do Carmo VM. Validade da Tributação em Relação a Monetização Auferida Por Meio do Fornecimento Gratuito de Dados e do Desenvolvimento e Disponibilização Gratuitos de Programas e Aplicativos. *Revista JurÍDica Unicuritiba* 2018; **3**: 156–189.

3 Castells M. A GalÁXia da Internet: Reflexões Sobre a Internet, Os NegÓCios e a Sociedade; Tradução de Maria Luiza X. de a. *Borges. Rio de Janeiro: Jorge Zahar*, 2003; **1**: 225.

4 Marques CL. *Confiança no ComÉRcio Eletrônico e A Proteção do Consumidor: um Estudo de NegÓCios JurÍDicos de Consumo no ComÉRcio Eletrônico*; Editora Revista dos Tribunais: São Paulo, Brazil, 2004; 33.

5 Dholakia RR. *Technology and Consumption: Understanding Consumer Choices and Behaviors*; Springer: New York, NY, USA, 2012; 174.

6 Aguado DC. Assistencia Extrajudicial Al Consumidor Transfronterizo Europeo. *Cuadernos de Derecho Transnacional* 2018; **10**: 45–69.

7 Reygadas L. Dones, Falsos Dones, Bienes Comunes Y ExplotaciÓN en Las Redes Digitales: Diversidad de La Economia Virtual. *Desacatos. Revista de Ciencias Sociales* 2018; **16**: 70–89.

8 Rebollo Delgado L. *El Derecho Fundamental a la Intimidad*; Dykinson: Madrid, Spain, 2005; 118–119.

9 GarcÍA MexÍA PL. Internet Y ProtecciÓN de Datos: Los DesafÍOs de La EvoluciÓN Digital. *Diario La Ley*, *Ano XXXII* 2011; **N**. **7577**: 11–14.

10 Bioni BR. *Proteção de Dados Pessoais: a Função e O Limite do Consentimento*; Forense: Rio de Janeiro, Brazil, 2019, 18.

11 Souza DC de; Amaral F. Cookies e Publicidade Comportamental Estão na Mira da Proteção de Dados. Avaliable online: https://www.conjur.com.br/2020-fev-22/opiniao-cookies-publicidade-mira-protecao-dados (accessed on 30 March 2023).

12 Myshadow. *Org*. Eu e Minha Sombra: Assuma O Controle de Seus Dados. Avaliable online: https://myshadow.org/pt (accessed on 30 March 2023).

13 Vainzof R. Geo-Pricing É Ilegal? Discussão Sobre Livre Iniciativa, Livre ConcorrÊNcia, Proteção de Dados e Defesa do Consumidor. Avaliable online: http://jota. info/colunas/direito-digital/geo-pricing-e-ilegal-

12012017 (accessed on 30 March 2023).

14 FrÍAs AL. *Los Contratos Conexos: EstÚDio de Supuestos Concretos Y Ensayo de Uma ConstrucciÓN Doctrinal*; JosÉ Maria Bosch: Barcelona, Spain, 1994.