Public Civil Action IDEC vs. ViaQuatro

IRIS' opinion

INSTITUTE
FOR RESEARCH
ON INTERNET
AND SOCIETY

AUTHORS
Davi Teofilo
Lahis Kurtz
Odélio Porto Jr.
Victor Barbieri Rodrigues Vieira

SCIENTIFIC ADVISOR
Bruno Bioni

TRANSLATION
Florência Lorenzo
Lahis Kurtz

REVISION
Luíza Couto Chaves Brandão

EDITORIAL DESIGN, COVER AND LAYOUT
Felipe Duarte

EDITORIAL PRODUCTION
Institute for Research on Internet and Society

FINALIZATION
Felipe Duarte

INSTITUTE
FOR RESEARCH
ON INTERNET
AND SOCIETY

Summary

I. About the Institute for Research on Internet and Society - IRIS

The Institute for Research on Internet and Society - IRIS, according to its statute consolidated on April 28th of 2017, is constituted as a non-profit civil association of scientific nature and policy formulation in the areas of law and technology, internet and innovation. Its activities seek to serve as an independent study platform, centered on the articulation between theory and practice. The Institute seeks to consolidate itself as a reference in the national context, cooperating with governmental, business, civil society and academia organizations, in Brazil and abroad, in topics related to its areas of expertise. Among the objectives of the Institute are the development and full participation in public advocacy projects, with relationship in judicial and extrajudicial processes of high impact on issues of public and collective interest, in areas related to IRIS topics. Among its activities, IRIS has been accepted as amicus curiae[1] of the Federal Supreme Court to act in Direct Constitutionality Action No. 51/2017, which refers to extraterritorial access to data by the Brazilian authorities. In addition, it also offered representation to the Public Prosecution Service of Minas Gerais in processes related to the collection and use of consumer CPFs in drugstore chains operating in the state.

II. Case summary and topics covered

The present case is a Public Civil Action (ACP) in which the plaintiffs and defendant are, respectively, the Brazilian Institute of Consumer Protection - IDEC - and the concessionaire of the São Paulo S.A. subway line 4 - ViaQuatro. The purpose is to terminate the activities of the Digital Interactive Doors system, implemented by the latter in its activities along the subway line that operates, as well as to convict ViaQuatro for collective damages, related to the violation of the rights of users who use the subway network's system.

This request is based on ViaQuatro's violation of consumer and personal data legislation, identified by IDEC due to the operation of this system, which, through cameras and software, has the functionality to recognize the presence of human faces and identify the the number of people who transit in its area, as well as detect their emotions, gender and age. In the complaint, the following abusive practices are reported: i) there was no clear and adequate information to consumers regarding the operation of Digital Interactive Doors; ii) the passengers' right to choose their data collection was not respected by this system; and iii) not even its operation is detailed, which may involve facial recognition and individualized treatment of data to form consumption profiles.

1 IRIS. Request for ingress as Amicus Curiae in ADC 51. Available at: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=729220092&prcID=5320379#>. Accessed on 07/05/2019. IRIS. Memorial presented to STF as Amicus Curiae on ADC 51. Available at: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=747870981&prcID=5320379#>. Accessed on 07/05/2019. G1. Drogaria Araújo é multada em mais de R$ 7 milhões por condicionar descontos a fornecimento de CPF. 05th December 2018. Disponível em: <https://g1.globo.com/mg/minas-gerais/noticia/2018/12/05/drogaria-araujo-e-multada-em-mais-de-r7-milhoes-por-condicionar-descontos-a-fornecimento-de-cpf.ghtml>. O Estado de Minas. Drogaria Araújo é multada em quase R$ 8 milhões por pedir CPF de clientes. 06th December 2018. Disponível em: <https://www.em.com.br/app/noticia/economia/2018/12/06/internas_economia,1011120/drogaria-araujo-e-multada-em-quase-r-8-milhoes-por-pedir-cpf-de-clien.shtml>.

Summoned, ViaQuatro presented defense based on the distinction between recognition and facial detection, reporting that: i) it only performs the latter, which does not imply the formation of individual consumption profiles, but only a demographic survey on the general public; ii) it would not store passenger data, as individualized information would be deleted immediately upon collection and aggregation to the database; and iii) the data stored in aggregate form would be anonymized, and therefore would not process personal data protected by law, given that its database would be of statistical purpose.

The Public Defender's Office of the State of São Paulo also manifested, considering that ViaQuatro is a public transport service concessionaire; the Public Prosecution Service, taking into account the protection of collective rights; and Instituto Alana, an institution that operates in programs that seek to guarantee conditions for the full experience of childhood, as amicus curiae, considering that the system also collects information about underage passengers.

Considering the performance of the Institute for Research on Internet and Society - IRIS - and its research themes, this opinion will address clarifications in several points of the process: in particular, those that are permeated by frontier issues between law and technology. To this end, we will analyze: i) the most relevant concepts related to the processing of personal data, as well as the description of their phases, based on the operation of the technology involved; (ii) the essential elements for checking that appropriate anonymization techniques have been used; iii) the international discussion on facial detection; iv) the technical considerations presented by ViaQuatro in the ACP framework; and v) effects derived from information asymmetry between the concessionaire and consumers.

III. What can be understood as "personal data processing" in producing information about groups of people?

At first, it is important to consider the main element underpinning rules for the protection of personal data in the various legal systems of the world, and which is intrinsically related to the present case: automated processing.

European legislation on the protection of personal data, for example, since the 1980s, is based on concern about the risks arising from the rapid technological development of automated data processing, which allows various information about citizens to be easily accessed and used, increasing therefore the risks of violation of fundamental rights and freedoms[2]. This consideration is made clear when regarding that the material scope of European law (the former Data Protection Directive 96/45/EC and the current General Regulation on Personal Data Protection 2016/679 [GDPR]) is established as "the processing of personal data wholly or partly by automatic means"[3]. These legislations were also based on Law No. 13,709 / 2018 and other laws, resolutions and sectoral regulations on the protection of Brazilian personal

2 EUROPEAN UNION. Article 29 Working Party. Opinion 4/2007 on the Concept of Personal Data - 01248/07/EN. p. 5. Available at: <https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf>. Access in: 06/04/2019.

3 Article 3 of Directive 95/46/EC and Article 2 of Regulation 2016/679.

data (about 40 in total), as per art. 43 of Law No. 8.078 / 2018. 90 regarding consumer databases.

This underscores the importance of the present case for the future of Brazilian personal data protection scenario, as the use of AdMobilize Artificial Intelligence (AI) algorithms enables the quantitative and qualitative processing of thousands of faces of people who use the yellow subway line daily. This processing takes place at a low cost and on a scale unmatched by any team of humans, as shown in the information ViaQuatro attached to the process. The advances observed in data processing capacity have a direct influence on the legal interpretation of the rules that regulate these technologies, as lawyer and juridical writer Marcel Leonardi clarifies: "[...] a quantitative difference brought about by technology generates a qualitative difference in the way of interpreting the legal norms".[4]

Throughout the present proceeding both parties, based on both national law and the best interpretations coming from the European Union, have defined personal data broadly as any information related to the identified or identifiable natural person. It is this feature, in fact, that allows law to accompany technological development, for if the concept were too restrictive - or associated only with certain technologies - its legal utility would quickly be lost in the face of advancing technology.

The processing of any personal data should be understood as a chain of procedures, which should be in line with the Brazilian legal system and its sparse laws on personal data protection[5]. In relation to the present public civil action, two approaches can be used on the operation of the personal data processing chain of subway users, so as to better understand the case.

From the perspective of (i) the chain as a whole, raw personal data (face image) are collected to extract information on the reaction to the advertising offered, which in turn will be used later to optimize new advertisements on the subway[6]. In this sense, data processing is not a process that occurs "in a vacuum" - unpretentiously. The consumer is both the origin and the final recipient of the treatment chain, since it is the source of the information that has the ultimate objective to influence its own consumption behavior.

4 LEONARDI, Marcel. Tutela e privacidade na internet. São Paulo: Saraiva, 2011. p. 365.

5 Article. 11 of Brazilian Law 12.965/2014 (Internet Bill of Rights): "In any operation of collection, storage, safekeeping and processing of records, personal data or communications through internet providers and internet application where at least one of these acts takes place in the national territory, the Brazilian law and the rights to privacy, the protection of personal data and the confidentiality of private communications and records shall be applicable. "

6 According to Bruno Ricardo Bioni, data mining involves the capture of raw data (input) for further processing and output of information. This information, in turn, is reverted to a decision, such as advertising targeting. The issue, therefore, is not just about data or databases, but about a whole dynamics of an information system that allows a wealth of raw data to be structured, organized and managed to produce knowledge that can be employed to a specific end. BIONI. Bruno Ricardo. Proteção de dados pessoais: A função e os limites do consentimento. Rio de Janeiro: Forense, 2018. p. 35-39.

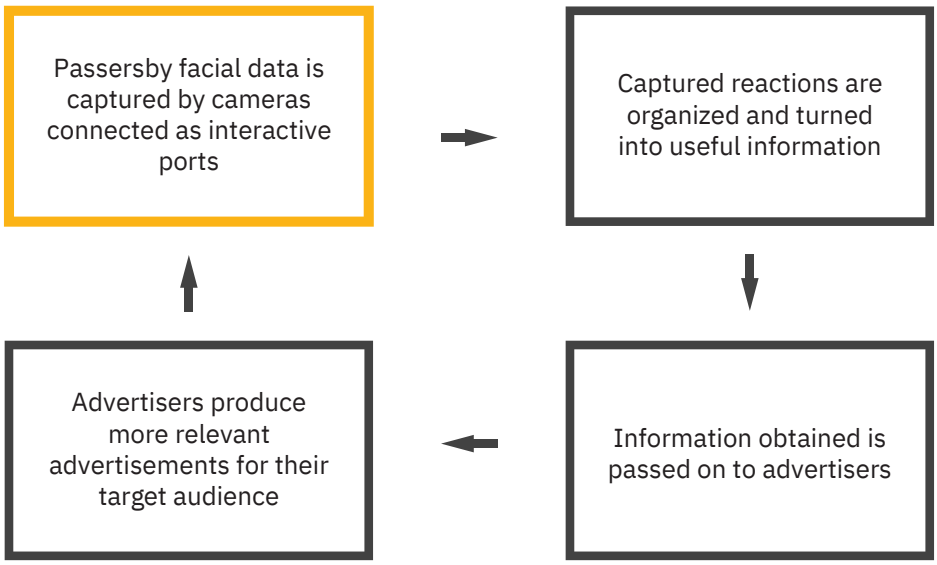


Image 1: Overview of the personal data processing chain of interactive doors.

A second look at users' personal data processing chain focuses on explaining (ii) what occurs technically and legally from the moment of image capture to the production of extracted information. This specific view of the treatment chain can be divided into 3 phases.

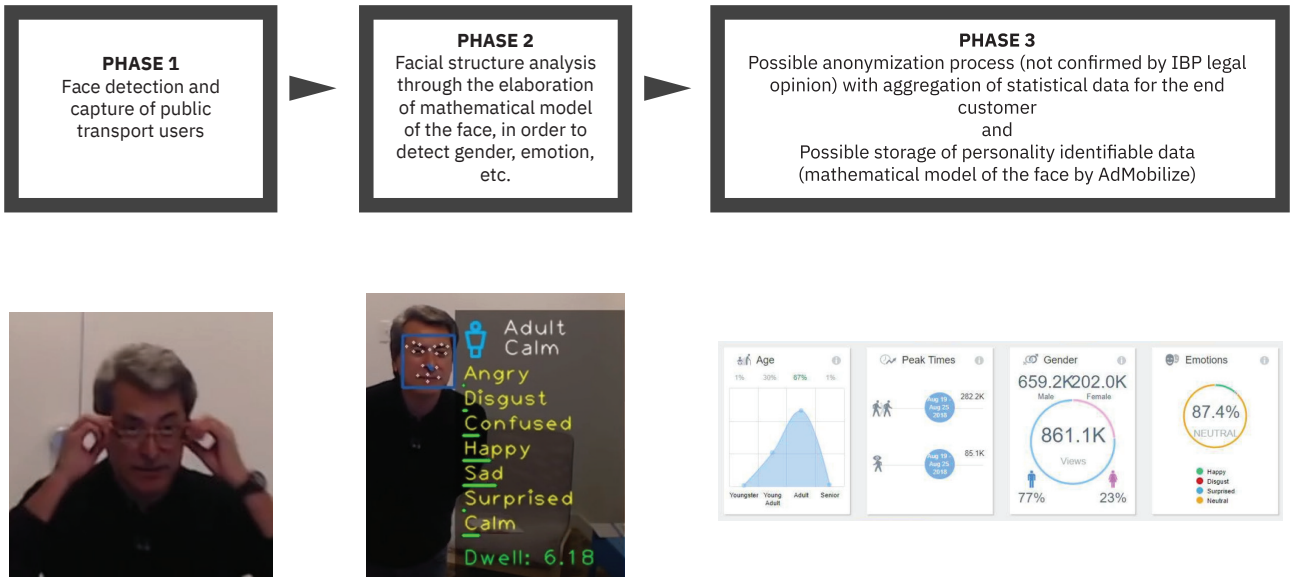


Image 2: Flow of processing of facial data, from its collection to the supposed anonymization process. Source: Authors. Images: taken from the institutional video and the technical opinion of IBP, p. 437 and 442

Although it is still unclear whether or not there is an anonymization process and adequate aggregation of data in the final stage of treatment (phase 3), due to the superficiality of the evidence produced by ViaQuatro in the process (topic that will be properly developed at a later section of this document), special attention to phases 1 and 2 is important.

In phase 1, the first action related to data processing in this case is the filming done by cameras owned by ViaQuatro, which provides the raw material for AdMobilize's artificial intelligence algorithm. In this process, the capture of a person's face image is undoubtedly characterized as a treatment of personal data, even if it is considered to last only a few fractions of a second and the image is discarded at a later stage of treatment.

It cannot be argued that the picture of a face is an anonymous data ab initio, as ViaQuatro seeks to argue, because it is intrinsic to the nature of a person's face to be characterized as personal data. If it were not for the face to be an intrinsically personal element, there would be no need, for example, for the use of photos in identification documents - including official ones, assigned by the state.

In addition, given the intent of protecting individuals from automated techniques made possible by technological development, data protection laws in Europe and Brazil, as well as in other parts of the world, do not impose any minimum processing time between the capture and anonymization[7]. This means that even if processing takes place in milliseconds, there is still processing of personal data, subject to the duties and guarantees provided by law.

In phase 2, the image is analyzed using an AI algorithm which produces a mathematical model of the person's face, so that one can later make the inference about the emotion felt at the moment of the image capture, besides allowing the identification of gender, age group, etc[8]. This analysis uses face reference points to identify physical characteristics associated with emotions, such as mouth position (for detection of a smile, for example) or eyebrow position (for indication of surprise, disapproval, etc[9]). This process is also described by AdMobilize, clarifying that its product "works by algorithms that detect about 80 (eighty) points on a person's face and, upon detection, convert them to binary numbers" on pages 426 of the case.

7 The concern with automated data processing is reflected in the historical absence of legal provision regarding the duration of processing in the legislative design on the subject. For an introduction to the historical background, see IRIS. GDPR and its effects on the Brazilian Law: First impressions and a comparative analysis. Available at: http://irisbh.com.br/wp-content/uploads/2018/06/GDPR_ENG-1.pdf . Access: 09/04/2018.

8 Normally, facial expression recognition is performed by a three-step approach. The first step is the detection of faces within an image (face detection). The second step is to obtain a numerical representation of the facial structure (facial expression data extraction). Face characteristics are extracted to reduce the large amount of image data and to obtain an abstract representation of image content. Finally, in the third step, facial expression is determined from this data extracted in the second step, usually though a classificator (facial expression classification). PANTIC, Maja e ROTHKRANTZ, Leon J.M. Automatic Analysis of Facial Expressions: The State of the Art. Institute of Electrical and Electronics Engineers (IEEE) Transactions on Pattern Analysis and Machine Intelligence. Vol. 22, nº 12. 2001. p. 1.424. Available at: <https://www.researchgate.net/publication/3193199_Automatic_Analysis_of_Facial_Expressions_The_State_of_the_ArtvVT>. Access: 10/04/2019. The above description, although published a considerable time ago, is in line with that presented on the technology company Norton's website on its website. NORTON. How does facial recognition work? Available at: <https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html>. Access: 31/05/2019.

9 *Ibid.*

Thus, the mathematical representation of a face is clearly a sensitive personal data, representing the unique biometric characteristics that allow the identification of an individual. The same logic is used in the collection of fingerprints by the state, because it is the singular positioning of the papillae of the finger pulps, inherently biometric data, that allows the identification of the individual. The risk of using biometric data is considerable, as they represent unique and virtually unchanging identifiers, accompanying holders throughout their lives. Considering these aspects, the capture of the facial structures contained in the images demands special caution in the analysis of the case by judicial power.

There is a risk that data on the distance between facial elements of a face will be crossed with other information, such as date and time of image collection, or even the Single Ticket database[10]. If this happens, it may be possible to identify the proprietor and use his profiling data based on his inferred preferences through reaction to the exposed advertisements. Thus, in phase 2 of the treatment there is also the processing of personal data, which is even more sensitive in nature because it is biometric information of the faces of individuals.

It is instructive to quote the following explanation of biometric data from the European Article 29 Working Party (WP 29)[11] [12] - International Data Protection Reference:

> [...]These data may be defined as biological properties, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability. Typical examples of such biometric data are provided by fingerprints, retinal patterns, **facial structure**, voices, but also hand geometry, vein patterns or even some deeply ingrained skill or other behavioural characteristic (such as handwritten signature, keystrokes, particular way to walk or to speak, etc...)[...]**As such, they can work as "identifiers". Indeed, because of their unique link to a specific individual, biometric data may be used to identify the individual.**[13] (our highlight)

It would only be at a third stage of treatment (phase 3), as shown in Figure 2, that anonymous data could be referred to if it had been proven that AdMobilize does not store any images and/or mathematical models of subway users' faces individualized, together with the inferences made about them.

In order explain what is an appropriate anonymization process, it must be

10 The criticisms and risks related to the Single Ticket in the city of São Paulo revolve around users' databases and potential sale of these data to third parties. These and other concerns are pointed out by experts in : <https://www.vice.com/pt_br/article/panq7n/mudancas-no-bilhete-unico-acendem-alerta-sobre-coleta-indevida-de-dados>. Access: 08/04/2019.

11 The Working Group on Article 29 (acronym in English, WP 29) is the independent European working group that dealt with issues related to the protection of personal data and privacy in the previous scenario to the validity of the European Regulation on Data Protection (General Data Protection Regulation No. 2016/679). It gathers highly qualified opinions on personal data protection and privacy, which are made available on the site.: <https://edpb.europa.eu/our-work-tools/article-29-working-party_pt>.

12 With the entry into force of GDPR, this working group became the European Data Protection Board.

13 EUROPEAN UNION. Article 29 Working Party. Opinion 4/2007 on the Concept of Personal Data - 01248/07/EN. p.8. Available at: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>. Access: 06/04/2019.

assumed that anonymization can only occur if there is as raw material a set of personal data that will be anonymized, as the report on anonymization techniques of the European Article 29 Working Party:

> First, **anonymisation is a technique applied to personal data** in order to achieve irreversible de-identification. Therefore, **the starting assumption is that the personal data must have been collected and processed in compliance with the applicable legislation on the retention of data in an identifiable format.**
>
> In this context, the anonymisation process, meaning the processing of such personal data to achieve their anonymisation, **is an instance of "further processing"**. [14] (our highlight)

This understanding is comparable to the "poisonous tree fruit" doctrine[15], because if the initial processing of personal data - in this case facial detection - violates the applicable law, even if appropriate anonymization techniques are used at a later time, all other processing phases also end up violating the legal system. The reasoning is the same, for example, where evidence obtained illegally contaminates subsequent evidence, rendering it invalid, even if the latter was lawfully obtained from the former.

Thus, the processing of personal data in the present case would have been "contaminated" initially by an unlawfulness in its capture and later mathematical modeling, considering the rules of consumer protection, the rights of public transport users and, in particular, the rights of privacy and image as detailed below.

For the collection of the face image, mathematical modeling of the face and analysis of the emotions, a legal basis would be necessary to allow the treatment, such as the consent of the subway user, according to art. 7, VII and IX, of Law No. 12,965/2014. For consent to be valid, it is also a prerequisite that clear information is passed on to ensure the consumer's right to information - arts. 6, III, and 31, among others, of the Consumer Protection Code - as will be developed at a later section.

Furthermore, it should be considered, according to the current state of the art, that enhancement of artificial intelligence (AI) algorithms for facial detection would benefit from storing data resulting from facial analyzes (mathematical model of the face and the characteristics detected as emotion, gender, etc.). This is because it is possible to use this data to verify the efficiency of these algorithms, as well as to improve their accuracy[16]. It should be recalled that AI algorithms, such as machine learning and neural networks, function primarily through access to large data

14 EUROPEAN UNION. Article 29 Working Party. Opinion 05/2014 on Anonymisation Techniques - 0829/14/EN. p. 7. Available at: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>. Access: 06/04/2019.

15 Robert M. Pitler. The Fruit of the Poisonous Tree Revisited and Shepardized, 56 Cal. L. Rev. 579 (1968). Available at: <http://scholarship.law.berkeley.edu/californialawreview/vol56/iss3/2>. Access: 09/04/2019

16 "Automated facial expression recognition systems face a number of characteristic challenges. Firstly, obtaining natural training data is difficult, especially for facial configurations expressing emotions like sadness or fear. Therefore, publicly available databases consist of acted facial expressions and are biased by the authors' design decisions[...]". MAYER, C, EGGERs, M, e RADIG B. Cross-Database Evaluation for Facial Expression Recognition. Pattern Recognition and Image Analysis. Vol. 24, nº 1. p.1. Available at: <https://link.springer.com/article/10.1134/S1054661814010106>.

sets through which they can detect patterns and subsequently apply this acquired knowledge in the analysis of new data sets[17] .

Thus, technically, it can be said that the more data used to train an AI algorithm, the better its accuracy. It would therefore be in AdMobilize's interest to store the personal data processed in the present case (mathematical model of the face and the corresponding emotions detected) so that the company can better evaluate the efficiency of its AI algorithm and train it for facial detection. According to our analysis of the IBP's technical opinion, presented later in this text (item VII), it does not clarify which data is stored by AdMobilize.

IV. What does "anonymization of personal data" mean?

Anonymization techniques refer to data processing in order to avoid the identification of the data subject. It is important that when conducting anonymization processes, companies can ensure that once anonymized, there is no reasonable chance of reidentifying the data. As the Article 29 Working Party opined, "[a] nonymised data would therefore be anonymous data that previously referred to an identifiable person, but where that identification is no longer possible"[18].

For this reason, the anonymization techniques used should be clearly described so that they can be verified for compliance with current best practices. It is not possible to observe in the documents submitted by ViaQuatro any description or naming of the anonymization technique supposedly used, which would ensure that no user of the subway exposed to the technology would be identified or identifiable. Explanations of what anonymization procedures are used are fundamental in stating that a technology does not process personal data.

Compared to European law, the data anonymisation process was initially conceptualized by Directive 95/46/EC on the processing of personal data. The European experience, beyond any exercise of comparative law, is an international reference on data protection, since the standardization of the subject has been on the community agenda since the 1980s[19]. According to this directive, anonymization is a technique data processing whereby a natural person is detached from the ownership of any given data. This means that after anonymization, a natural person, initially identifiable by means of a given data, will no longer be associated with that data. Therefore, since anonymised data imply non-application of personal data protection rules, it is even more important that the duty of transparency be observed by the controller.

17 RUSSELL, Stuart J.; NORVIG, Peter. Artificial intelligence: a modern approach. Malaysia; Pearson Education Limited, 2016, p.26.

18 WP29. Opinion 05/2014 on Anonymisation Techniques. 10/04/2014. p.8. Available at: <https://www.pdpjournals.com/docs/88197.pdf>.

19 For more information on the evolution of this matter in the European Union, as well as its doctrinal and legislative influence on the Brazilian order, see: IRIS. GDPR and its effects on the Brazilian Law: First impressions and a comparative analysis. Available at: http://irisbh.com.br/wp-content/uploads/2018/06/GDPR_ENG-1.pdf . Access is: 09/04/2018.

This definition of data anonymization in the Directive has been virtually reiterated in the final text of the recent General Regulation on Personal Data Protection (GDPR), which replaces the 1990s Directive. The regulation, adopted in 2016, which came into force in 2018, undeniably influenced the Brazilian General Data Protection Act (Law No. 13.709 / 2018), whose article 5, III and XI states:

> "Article 5
>
> For the purposes of this Law, the following shall be considered:
>
> III - anonymized data: data relating to the holder that cannot be identified, considering the use of reasonable technical means available at the time of processing;
>
> [...]
>
> XI - anonymization: the use of reasonable technical means available at the time of treatment, whereby a data loses the possibility of direct or indirect association with an individual."

Importantly, the ability to identify an individual by a data is not limited to information such as name, social security number or other personal information that is too obvious.

Identifying a natural person, especially with the advent of the internet and mass data processing, can be done by employing much more vague information - called metadata. These are data that provide information about other data. Metadata may be considered, for example, according to Brazilian law: "Art. 5th - VIII - Internet application access records: the set of information regarding the date and time of use of a particular internet application from a given IP address"[20]. Metadata such as geolocation and time of data generation, IP address, source logical port, among others, can also be employed, individually or together, to identify a natural person accurately.

Thus, it is evident that there is automated processing of personal data, and that there is no proof or mention of the anonymization procedure performed in this procedure.

V. Importance of Proper Anonymization

There is no specific technique for data anonymization. Thus, when establishing a service that involves this technique, you can choose one or more available options from a range of possibilities.

In practice, the necessary technique should be presented and justified on a case by case basis. For this reason, it is also reinforced the need for presenting the used techniques to this Court, in order to prove that the technology present in

20 BRASIL. Lei 12.965/ 2014. Internet Bill of Rights.

the "interactive doors" does not involve the use or the possibility of using, with the advancement of technology, personal data. The Article 29 Working Group, in one of its publications[21], lists some practices available for data anonymization, as well as recommendations for the use of each, possible vulnerabilities and specific cases in which it was possible to revert the anonymity promoted by each technique.

In such cases, the implementation of these measures is not merely a consequence of a legal obligation arising from the application of personal data protection. Moreover, due anonymization of the data represents a condition for not qualifying as personal data - reiterating that, as shown in Figure 2, the moment of collection (phase 1) and subsequent elaboration of the mathematical model of the face for analysis of emotions (phase 2) are characterized as processing of personal data. The anonymization of these data (phase 3, shown in Figure 2), therefore, is imperative so that such processing is not subject to the legal regime provided for personal data in the Internet Bill of Rights (Law No. 12.965/2014) and, in the future, in General Data Protection Law, as the defense manifests.

It is important to emphasize that, due to the precautionary principle in force for the protection of the Brazilian consumer, when using a technology, the company that provides services (including public services) has the obligation to know holistically the processing involved and to be able to provide complete clarifications regarding technology, especially in court.

The adoption of organizational measures and proper anonymization techniques are fundamental elements to verify whether or not a particular treatment involves personal data. At no time in this process were presented what would be the possible techniques adopted by ViaQuatro. The agreement between the parties, which could contain clauses requiring the proper use of anonymization techniques, was not even annexed, nor was AdMobilize contractually required not to treat subway users' personal data, nor to seek to re-identify them in case it treats the data that was supposed to be anonymized in phase 3 of the treatment.

In a report indicating best practices to ensure consumer privacy, the US Federal Trade Commision recommends that companies that handle anonymized data - in order to mitigate the risks of re-identification by correlation processes. - take the following precautions:

> a company's data would not be reasonably linkable to a particular consumer or device to the extent that the company implements three significant protections for that data [...](1) the company must take reasonable measures to ensure that the data is de-identified [...] (2) a company must publicly commit to maintain and use the data in a de-identified fashion, and not to attempt to re-identify the data. [...] (3) company makes such de-identified data available to other companies – whether service providers or other third parties – it should contractually prohibit such entities from attempting to re-identify the data. [22]

21 EUROPEAN UNION. Article 29 Working Party. Opinion 05/2014 on Anonymisation Techniques - 0829/14/EN. Available at: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>

22 FEDERAL TRADE COMMISSION. Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers. 2012. p.20-21. Available at: <https://www.ftc.gov/reports/protecting-

Such clauses would be an important incentive to avoid any violation of the sparse personal data protection laws of the Brazilian order, and to ensure the safety of users of the ViaQuatro subway. The presentation of these clauses would be a demonstration that ViaQuatro, at least with regards to the protection of consumer data, conducts interactive port activities with some degree of good faith.

It should be pointed out, however, that the demonstration of contractual provisions in this sense does not nullify any irregularity in ViaQuatro's activity that may be proven in the course of the ongoing judicial process, nor would it satisfy the duty to inform and the requirement of consent inherent in the right of users as consumers.

As a result, there is a situation in which information about the actual data processing method employed in interactive ports is a "black box". It remains for the users of the São Paulo subway - as well as the present Court and third parties - to believe, in full confidence, in the discourse reiterated by the yellow line 4 concessionaire, without further question, despite the well-founded fear already expressed by experts, including the Institute. Consumer Protection Institute and the Alana Institute, and even by the Public Prosecution Service itself and the Public Defender's Office of the State of São Paulo in the case file.

Concerning the arguments presented in court and which, allegedly, would be sufficient to clarify any controversial points regarding the technology used in interactive doors, a separate topic is pertinent (item VII). In particular, an analysis of the opinion commissioned by ViaQuatro will be carried out.

VI. Implications of a possible lack of proper anonymization of data

One of the possibilities for phase 3 of the data processing performed by the Interactive Digital Doors would be, if there is no adequate anonymization, the formation of profiles for each passenger, containing details about their behavior, such as when they are usually at a particular station, their mood , their physical characteristics and their age.

Considering this hypothesis, there are some risks that this practice imposes on the consumer and the way the government has been acting in order to avoid violations. For this, analysis will be performed in parallel with another case, similar to the profiling hypothesis considered here.

In its institutional activities, the Institute for Research on Internet and Society (IRIS) offered a formal complaint to the Public Prosecution Service of Minas Gerais, in which case pharmacies incur practices with similar effects to the case in question.

consumer-privacy-era-rapid-change-recommendations-businesses-policymakers>

In Belo Horizonte and other Brazilian cities, it has been common practice for establishments to request the number of the National Register of Individuals - CPF - from customers when making any purchase. The case is related to this fact in some aspects: i) the use and collection of consumers' personal data without free, express and informed consent (Internet Bill of Rights, art. 7, §VII); ii) breach of the duty to inform consumers about their participation in databases, even if they are demographic in nature; iii) the possibility of using data aiming at profiling. In the case of CPF registration, the risk was immediate, whereas in the present case, it is a possibility and may also result from a security breach in the camera systems or secondary function of the system that produces demographic data; and iv) the lack of privacy policies that contain clear information about the use, collection, objectives and security levels of the processed data.

In the case of drugstores, after the administrative procedure No. 0024.18.002027-3, instituted by the Public Prosecutor of Minas Gerais (MPMG), was verified the irregularity of the practice by signing the Conduct Adjustment Agreement (TAC) between the drugstore and the MPMG[23]. The administrative proceeding resulted in a precedent of corrective determinations regarding registration and consumer participation in commercial withdrawals. Consumer information and self-determination as data subjects were highlighted in the prosecution's conclusion on the practice.

The case is important to illustrate that even if the General Data Protection Law - which will be vigent in 2020 - is not yet in force, sparse legal devices can be bases for actions seeking to protect the use of personal data in Brazil. Thus, the legal basis of both cases are similar in that they deal with the same objective in similar circumstances: the absence of information, consent and consumer safety, in order to conduct market analysis and influence the consumer. If in this case the emotions, age, gender and other data are used to optimize advertising and encourage consumption, in the other the use of medical-pharmaceutical consumption patterns were used to allocate discounts related to customers' individualized habits, also encouraging consumption.

In addition to working as a way to manipulate consumer behavior by individually targeting advertising based on massively collected data, profiling techniques focus on other corners of social life, enabling the discrimination of a person. It should be taken into account, in the scenario of lack of proper anonymization, that there are companies interested in acquiring and marketing databases - the so-called data brokers[24]. This business model is based on the purchase and provision of personal databases to third parties who may use them to evaluate health insurance, life insurance, admission to employment, and other selection processes.

23 MPMG. **Acordo com o MPMG prevê que drogaria Araújo cesse captação de CPF dos consumidores**. Available at: https://www.mpmg.mp.br/areas-de-atuacao/defesa-do-cidadao/consumidor/noticias/acordo-com-o-mpmg-preve-que-drogaria-araujo-cesse-captacao-de-cpf-dos-consumidores.htm. Access: 09/04/2019.

24 Vermont was the first state in the US to approve, as early as 2018, a specific law to regulate the performance of data brokers. The law defines what data brokers are, the obligation of companies to register with state authorities, the duty of transparency to consumers about the processing of their data, when is it possible to withdraw from processing, and the duty to inform those affected in case of data leakage. COLDEWEY, Devin. Vermont passes first law to crack down on data brokers. Techcrunch. 27/05/2018. Access: 04/06/2018. Available at: <https://techcrunch.com/2018/05/27/vermont-passes-first-first-law-to-crack-down-on-data-brokers/>

Thus, the administrative decision in the case of pharmacies is important for the recognition of the need, by society and its representatives, to protect information that may involve consumers' freedom of choice, especially information that may refer to health or physical characteristics issues. It is noted that, under current legislation, the use and processing of such personal data does not constitute illegality, provided that the limits and guarantees established by the consumer and personal data protection system are respected. As in the present case there is a behavioral analysis of consumers, they must respect the limits established by the consumer protection system in order to protect their self-determination, privacy and transparency in business relations.

VII. Considerations on the technical opinion presented

Taking the risks of a possible profiling practice into consideration, it is pertinent to analyze the document submitted by ViaQuatro in order to corroborate the allegations that it does not collect identified or identifiable data.

The technical opinion presented by the respectable Brazilian Institute of Experts (IBP) on pages 427 of the records, regarding the data collected through the Interactive Digital Doors, is not sufficient to demonstrate the absence of processing of personal data. It should not, therefore - with all respect to the IBP - be regarded as technical evidence in this regard as it is not completely sustainable from a technical point of view.

The resources analyzed by the technical opinion are not sufficient to demonstrate precisely what data are collected and sent over the internet to the software owner, AdMobilize, although ViaQuatro claims only to have access to the aggregated results, because the analysis was restricted to: i) the mere image of a data flow diagram (pages 433); ii) the dashboard information book for the contracted solution (pages 433-441); iii) the data package with the final result of the treatment performed by AdMobilize ("forensic container") and emailed to ViaQuatro (pages 438-440); and iv) the publicity[25] video about the operation of the AdMobilize solution (pages 441-446). These items are insufficient to demonstrate that neither ViaQuatro nor AdMobilize would store the characteristic points of faces with their respective emotions detected and/or camera images (which are connected to the internet, as found in questions and answers), at pages 1,132 and 1,133).

The image of a data flow diagram and advertising video, both authored by AdMobilize itself, cannot support a technical conclusion, since they carry the same weight as a statement and do not actually prove that the claim corresponds to reality. While the dashboard and forensic container, although indicative, do not technically demonstrate to which data AdMobilize has access and stores it after the identification of emotions (phase 3).

From the above, the employed techniques do not reflect the current notions for the explanation of the software functioning[26] and the necessity of the proper use of

25 Available at:<https://www.youtube.com/watch?v=_zj_51eU-kU>

26 SAMUELSON, Pamela; SCOTCHMER, Suzanne. **The law and economics of reverse engineering**. Yale Law Journal. 111.7, p.1575-1663, May. 2002. p.1608

methods, such as reverse engineering, to elucidate the case in question, concerning the use of complex technology, which employs artificial intelligence. Technically, it should be noted, reverse engineering enables auditing of the software without exposing the source code[27].

It should also be highlighted that the information security measures adopted were not made explicit, which is serious considering the danger of exposing sensitive[28] (biometric) data from thousands of users of the yellow subway line.

By way of illustration, consider the well-known case involving Facebook and Cambridge Analytica. The case gained notoriety when, on March 17, 2018, The New York Times[29] and The Guardian[30] reported that Cambridge Analytica used personal information from millions of profiles to direct political campaigning.

Keeping in mind the proportions and specificities of the case, it is interesting to consider the elaboration of a more detailed technical explanation of the case - the simple descriptive presentation of the dashboard, an institutional video, and an image of the data stream provided by Facebook would not suffice. the experts found a sharing of personal data without authorization from the holders. Therefore, if the objective is to understand the flow of the data used, one should use reverse engineering tools, network traffic analysis tools to which they are connected and analysis of the application's databases and servers.

That is, the technical clarifications about software, to be conclusive, require a process to discover the technological principles and the operation of a device, object or system, through the analysis of its structure, function and operation. These elements are not found in the opinion submitted by ViaQuatro, which broadly only analyzed the final data processing product that is provided to ViaQuatro, without further consideration of AdMobilize's role.

This is not to say that the opinion comes to untrue conclusions, but that, in order to demonstrate unequivocally how it has been reached, it should clarify which materials technically prove the inexistence of image storage and/or information about the biometric configuration of faces together with the detected emotions, as well as the lack of individualization of the data collected from each user.

By looking at the product generated by the system, the technical opinion intends to conclude whether, to arrive at that information, there would be individualized treatment of biometric data or not - as a "reverse engineering" tactic. It should be noted that reverse engineering is the process by which knowledge or design models can be extracted from anything man-made[31]. Thus, it consists in understanding the

27 Idem.

28 On the risks of using artificial intelligence without clarifying their mechanisms, especially for the authorities, see: O'NEILL, Cathy. **Weapons of math destruction: How big data increases inequality and threatens democracy**. Nueva York, NY: Crown Publishing Group, 2016.

29 THE NEW YORK TIMES. **How Trump Consultants Exploited the Facebook Data of Millions**. 17, March, 2018. Available at: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>.

30 THE GUARDIAN. **Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach**. 17, March, 2018. Available at: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

31 EILAM, Eldad. **Reversing:** Secrets of Reverse Engineering. Indianapolis: Wiley Publishing Inc. 2005. p. 3-4.

functioning of something through the analysis of its structure and behavior.

Unlike corporeal objects - which can be observed "physically" - software reverse engineering is through a variety of computer programs that allow even non-intrusively closed-source (proprietary) software analysis, by analyzing the instructions issued by the analyzed software to the processor[32]. In other words, there are software reverse engineering techniques that enable the program to be inspected without direct access to its source code, avoiding infringements of Intellectual Property rights and business secrets.

Thus, in order to provide conclusive information about the analyzed software, the technical advice should have been to verify whether any data anonymization process was actually used, and to analyze what information is passed on to AdMobilize in order to make it clear what data is processed all along the chain. The absence of such explanations is even more serious when considering the fundamental role that a technical opinion should play facing the complexity of Artificial Intelligence software.

By way of example, one cannot access all the data that a software such as Google's search engine or Facebook social network has from a particular user only by logging in to that user's login and account. In fact, it is well known that there is much more information in their database than is available in a reduced control panel provided to the user, or even to companies that buy advertising on these tools.

Thus, statements like that of pages 444-445, analyzing AdMobilize's own video advertising about how the software would work in theory, lacks robust technical foundation. By checking the excerpt "the square changes color, thus indicating that the software does not store personal information, because even though the software has previously detected this person, it generates new anonymized data, as if it were actually someone else", it appears that the reasoning of the opinion is based on an element of null technical value, the mere color of the picture placed in the advertising video. It is unclear from the technical advice how video is true to what the software actually does, or even what the colors and squares mean for the source code that operates the AdMobilize system.

Graphical representations that appear on the dashboard and advertising video may not be the only information generated by the software, and it is possible to process and store information that generates background-only databases that can be accessed by users with administrative access to the system, such as AdMobilize developers. By way of example, in the Google Docs system itself, where you can write collaboratively, each time the same logged in user opens the file in their browser, it gets a different color. This does not mean that the system did not recognize him or that she is anonymous.

Thus, the technical opinion cannot be considered conclusive, since it does not present technical parameters of the algorithm operation about the data flow between the cameras, AdMobilize and ViaQuatro, or the possible storage or not of a unique identifier of users of the subway service.

32 Idem. p. 8-9.

Thus, it is noteworthy that the technical opinion limited itself, in its conclusions (i) to (vii) of fls. 447, to make statements about the final result of processing made available to the customer (data in csv format), as well as to make inconclusive statements such as "no evidence has been identified", which does not mean that it has been sufficiently demonstrated whether or not personal data are treated.

As for point (viii) of the conclusions, in which the technical opinion concludes that 'ADMobilize software has no memory', there is no way of knowing how this supposed conclusion was reached, since at no time do these reviewers claim have had access to the raw data - images that the cameras record - or the package they send to the AdMobilize solution for later delivery to the control panel. Access only to an interactive control panel solution for ViaQuatro, as well as email sent by the software after data processing, does not allow us to determine whether the software has memory or not, as these products do not clearly demonstrate the origin of the information they present.

Finally, according to the best doctrine, the technical opinion aims to bring clarity to the process[33], helping the judgment regarding the specific techniques and knowledge involved in the case to be considered. In this sense, the technical advice offered in the present case should clarify how the technology in question works, and not be limited to the visual analysis of the software control panels made available to the end customer.

The purpose of bringing more technical clarity to the process is related to the presentation and significant explanation of the technology in question. The elements analyzed in the opinion submitted by ViaQuatro cannot be configured as sufficient, because such elements do not demonstrate the more detailed operation of the system, the actual data flow to which AdMobilize has access, and whether, if any, appropriate anonymization techniques were applied.

It should also be added that equally inconclusive is the notarial minute requested to the 26th Notary's Office (pages 486-497). This is because the document in question, as well as the technical opinion of the IBP, refers only to superficial aspects of the technology offered by AdMobilize, plus situational information on the occasion of drawing up the minutes - information that is limited to the description of the interface of the software used in the Interactive Digital Doors - together with the situational detailing on the occasion of the drawing up of the minute, which does not attribute any technical evidential value to the document.

Such notarial minutes, therefore, do not allow knowledge to be obtained about the processes involved in the operation of AdMobilize software, as this would require a technical analysis of the technology backend, as addressed during the analysis of the technical opinion. IBP above. Thus, it is also impossible to make any technically sustainable inference from the notary minutes attached to the case file.

33 THEODORO, Humberto Jr. **Curso de Direito Processual Civil**. Volume 1. 56ª edição. Rio de Janeiro: Editora Forense. 2015. p. 1262.

VIII. International cases with common elements to the made

The use of face detection and/or recognition technologies for commercial purposes through the practice of interactive displays can be found in other countries of the world, offering analysis parameters for the case in point. This trend can be traced back to mid-2012, when Nike began its "Nike Free" advertising campaign, whereby individuals could interact with a tennis shoe by recognizing their facial movements by a webcam[34].

Since then, there has been a gradual increase in the use of these technologies, as well as their accuracy, which has resulted in a recent intensification of the presence of these techniques. Several advertising companies began offering smart ads implementation services - and these, in turn, surpassed the exclusively digital environment and also occupied the physical world, including public spaces.

According to a 2015 study by First Insight[35], 75% of customers claim they would not buy from a store that employs face recognition technologies for commercial purposes. This percentage was reduced to 55% when respondents were asked about the use of face recognition that resulted in beneficial and individualized consideration for clients - in the form of discounts, for example.

Both statistics indicate that acceptance of this type of technology is not peaceful among consumers who travel through their image capture sites. It is also worth mentioning that 70% of respondents did not even know what beacons are, that is, the sensors used in facial reading. This reinforces the information asymmetry between those who implement the technology and those who have their images captured.

The discussion on facial detection in the context of consumer relations also gained evidence in Norway. A case in this country that brings parallels with the present accomplishment concerns a pizzeria in Oslo called Peppe's Pizza. In 2017, a consumer was passing in front of the restaurant and noticed that the store's digital ad had gone through some software glitch that made the desktop of the computer connected to the screen in question visible. The following images represent the information on the screen:

34 NIKE FREE LACE (case study video). Available at: https://vimeo.com/123158970. Access: 09/04/2019.
35 FIRST INSIGHT. Consumer Survey Report. August, 2018. Available at: https://cdn2.hubspot.net/hubfs/160569/First_Insight-In_Store_Experience_Report.pdf. Access: 09/04/2019.

Image 3: Picture of the interactive display in front of Peppe's Pizza. The camera, facing a public space, can be seen above the screen, though barely noticeable to people uninformed about technology. Source: Diinside

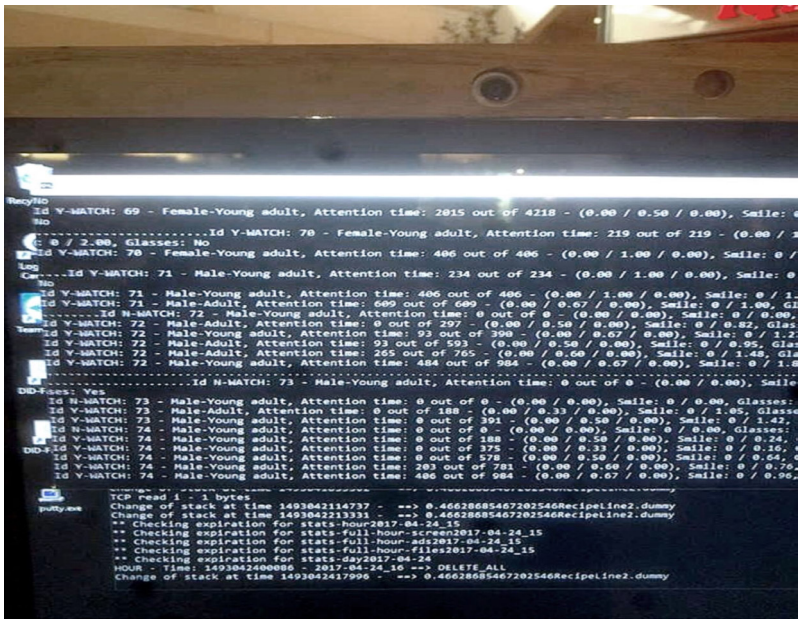


Image 4: Detail of the software that worked in the background on the interactive display, recording information about passers-by. Source: Diinside

The consumer noticed that the on-screen window seemed to be filled with information about himself: his gender, approximate age, wearing glasses, facial hair, his attention span to, and reaction to the content on the screen. After posting the photo on their social networks, it became strongly shared and was a reason for many questions[36], which shows the fear generated among consumers about the use of this technology. The repercussions of the case made it headline news outlets

36 Some examples of forums where this subject was discussed: https://www.reddit.com/r/norge/comments/67jox4/denne_kræsjede_skjermen_på_peppespizza_viser_en/dgrltgl/ e https://linustechtips.com/main/topic/777448-pizzeria-billboard-in-oslo-analyzes-people/

around the world[37]. Fearful of the negative repercussions they had achieved, Peppe's Pizza officials quickly and voluntarily removed the face sensor from the ad, claiming it was just a trial period and that the technology was expected to be removed that same week. Thus, they retreated from the practice and did not provide technical clarifications on the technology, beyond the screenshots that the consumer had released.

It is important to note, however, that when interviewed on the case, the senior advisor to the Norwegian data protection authority, Stian D. Kringlebotn, expressed considerable concern about commercial face detection technology. According to the counselor, as a camera is used to capture and treat consumers' facial structures, the current Norwegian regulation on the use of security cameras would apply to the case in order to preserve the rights of people passing by. In addition, the counselor pointed out that, from this point of view, the practice of Peppe's Pizza would be considered illegal. This is because the use of Norwegian surveillance cameras requires express and justified authorization in order to safeguard the right to image and privacy of the population, which reflects concern about the rights of consumers whose face detection for advertising purposes would not be recognized as a legitimate reason for authorizing the pizzeria to use it.

International experience and societal perspectives, in which facial detection was employed, demonstrate the relevance of the decision of this feat. This is because the present judgment presents a frontier case for law - both nationally and internationally - in the field of technology. Thus, it deals with setting a relevant precedent for the personal data protection scenario in Brazil, in relation to large-scale automated processing in a public place and the use of artificial intelligence technology. Therefore, it is important to consider obligations regarding the transparency, information, safety and caution of those who travel on the Yellow Line of the subway of the largest city in Latin America.

37 Some press repercussion of the case: TURTON, William. **A restaurant used facial recognition to show men ads for pizza and women ads for salad**. The Outline. 2017. Available at: <https://theoutline.com/post/1528/this-pizza-billboard-used-facial-recognition-tech-to-show-women-ads-for-salad?zi=iq3iltht&zd=6>. Access: 09/04/2019; VENTURA, Felipe. **Outdoor de pizzaria usava câmera para escanear e analisar rosto das pessoas.** Tecnoblog. 2017. Available at: https://tecnoblog.net/214548/pizzaria-camera-analise-facial/. Access: 09/04/2019; STOKKE, Ole. **Reklamer på Oslo S med kameraer analyserer fjeset ditt - Reklameskilt ser hvem du er** [Advertise in Oslo with cameras that analyze your face - Advertisement signs see who you are]. Dinside. 2017. Available at: https://www.dinside.no/okonomi/reklameskilt-ser-hvem-du-er/67552025. Access: 09/04/2019; STOKKE, Ole. **Peppes Pizzas overvåkningsreklamer er fjernet** [Peppe's Pizza's surveillance ads removed]. Diniside. 2017. Available at: https://www.dinside.no/okonomi/jeg-synes-det-er-skummelt/67560027. Access: 09/04/2019.

IX. Even if the data is properly anonymised, what are the legal implications of information asymmetry with consumers?

IX.I. The adequacy between means and ends

ViaQuatro, when providing urban transportation services, is a public service concessionaire. Accordingly, it is subject to public service legislation and also to the terms and limits set forth in its concession agreement - Contract No. 4232521201 - Sponsored Concession for the purpose of Operation of Yellow Line 4 Passenger Transport Services of the São Paulo Metro.

The subway is a public service with millions of users[38], who have no alternatives to get to their jobs, homes and other places in the city. Subway users expect from this service the ability to move between points of the urban structure. That is, it is not part of its core business to conduct demographic surveys for market purposes. Nor can this type of data collection, which is done with the compulsory participation of the users of the subway network, be considered essential to the adequate provision of services.

Collecting data on how many people are traveling could be considered useful in calculating timetables, number of trains and the configuration of the wagons on which ViaQuatro is a concessionaire. However, the other information that is being captured by facial detection devices, allegedly anonymous, with data on gender, age, reaction, is not linked to the improvement of transport activity granted by the government.

Compelling users to participate in a survey violates users' rights and fails to comply with concessionaire's duties. And this happens even if they do not even know for sure what kind of information is collected (something that was not fully clarified on the records, because the technical advice was incomplete).

Knowing a posteriori that a machine could detect their faces in order to compute public reactions and characteristics does not make this practice any less intrusive to all users of the subway system. To require that, in order to be able to move around the city, a person must collaborate with market research that is not in any way linked to the provision of the subway service violates the adequacy between means and purposes of the provision of the service, an obligation provided for in art. 5, IV, of Law 13,460 of June 26, 2017. And participation in the research is a requirement imposed on the user of public transport, since it is not a situation in which she has the power not to participate, which directly hurts that legal device.

38 "Linha 4-Amarela transporta mais de 3,5 milhões de passageiros durante o carnaval". Source: <http://www.viaquatro.com.br/imprensa/noticias/linha-4-amarela-transporta-mais-de-3-5-milhoes-de-passageiros?releaseid=31507>.

IX.II. Practices permitted by the concession agreement

Following the analysis of the situation, it is clear that the concession under discussion is a public-private partnership[39], which would make it possible for the concessionaire to use the permissions granted as a provider of this service to make a profit in their exercise. This point is evidenced by the concession agreement presented, which allows, in its clause 10.1.1, the use of the space for commercial exploitation.

It is clear that commercial use has an exclusive character, which is part of the contract in which the only concessionaire is ViaQuatro. Thus, it holds the rights to operate activities in that place under its administration, with respect to subways and stations. This means that only the concessionaire has the legal possibility to cater for third parties ad space, as well as to install equipment such as cameras and screens there.

Thus, the only company that has commercial exploitation rights to ViaQuatro's line and subway space is itself. Therefore, the concessionaire exercises unbalanced power in relation to that market, in which there is no other company able to make the survey made by it, which makes the demographic information collected by it a valuable one for sale to third parties.

Due to this economic value, this face detection activity is part of commercial practice. And in this context, its character is abusive, because a person, when using the public transport service, compulsorily contributes to a market research activity, without the possibility of not doing so. This hurts citizens' freedom of choice. That is, besides obliging its users to integrate compulsory demographic research, ViaQuatro does it exclusively, being the only company that has this power in those spaces, which makes this information collection economically advantageous to ViaQuatro.

This practice is in dissonance with the contractual provision of "restrictions on advertising" in clause 10.1.2 of the concession agreement, which states that activities that violate legislation, morals and customs are prohibited.

It is worth remembering what Cavalieri Filho says in his work on consumer law: "Profit is allowed and paramount in a capitalist economy, but it cannot overflow to abuse, to the exploitation of consumers [...]"[40].

Market activity, to be appropriate to the concession contract, cannot hurt the duty to inform and the free choice of the individual about his actions. Citizens cannot be required to participate in the utility's profit generation. By the time users' presence and emotional reaction is detected by devices that do not require consent or provide opt-out, users are having this freedom violated. In addition, by not publicizing that this collection is made, the concessionaire incurs negligence regarding the duty to inform.

39 Source: <http://www.viaquatro.com.br/a-via-quatro>.
40 CAVALIERI FILHO, Sérgio. Programa de direito do consumidor. 2a. ed. São Paulo: Atlas, 2010. p. 150

IX.III. On the duty to inform

Apart from the broader provisions on transparency and reporting, contained in Articles 4, caput, and 6, III, of the Consumer's Defense Code (CDC), this obligation is also provided for in Articles 46 and 54 of the same law, which states that the provisions of a Consumer contracts - more specifically, adhesion contracts, as is the case under consideration - must be clear to the consumer so that he has an easy understanding of the terms of the relationship with the supplier.

As a service provider in the subscription mode, where subway users do not have the power to negotiate the terms of contracting the transportation service, ViaQuatro has a duty to comply with this standard. It must clearly and comprehensively inform all users of all terms of use of that service.

The concessionaire, as evidenced by the reading of the records, did not keep notices, at its stations and trains, that users were subjected to collecting their reactions to interactive doors. The fact that users of ViaQuatro's subway concession line did not knew that by purchasing a ticket and using the section, they would also be participating in research for commercial purposes, infringes the duty to inform.

This duty is the basis for conscious and motivated consumer's choice as to whether or not to participate in the profit-generating activity of the goods and services provider. The consumer user of subway services, when subjected obscurely to an activity in which their personal data generates information, which is transformed into a product by the concessionaire, is treated as raw material.

In this case, the violation relates to the price charged for the goods and services purchased - since part of the payment for using the public transport service is in the form of personal data obtained directly from the behavior of users. As users participate in such activity, and because it integrates the price of the service provided by the concessionaire, it is the right of these users to know of this cost imposed on them.

An important human characteristic on which our legal system is founded is self-determination, that is, the ability to decide and determine one's own identity, the activities one wants to integrate and which define one's experiences throughout one's life. In cases involving the processing of personal data, the concept of informational self-determination[41], which consists of the idea of the individual's control over his or her data and information, requiring therefore more specifically consent - and, therefore, information - of the holders to enable the use of this data by third parties. To hide that a person participates in a particular situation, especially considering that his activity will generate profit for a third party, is to hurt her self-determination as a subject.

41 Bruno Ricardo Bioni points to the principle of informational self-determination as a fundamental precept of consumer protection today, guaranteed through the data subject's information and consent.

IX.IV. On the consumer's freedom of choice

Just information about collecting data for commercial survey purposes is not enough either; for even if informed, if there is no choice about participating or not, the subject is still violated in his or her self-determination. To give information about rights infringement is not a way to undo this violation.

Users are generating, with their compulsory facial detection, an exclusive profit for the utility - something that is completely beyond commercial exploitation and permitted marketing activity, as no one can be required to engage in profitable activities for a third party providing public service without be aware or choose about it.

In addition to the consumer's freedom regarding in what situations they want to buy goods and services, they have the right to be informed of the extent of the burden (whether payment with cash or other goods and services, such as monetization of information extracted from their data, personal emotions detected when seeing advertising), the citizen has, in the preamble of the Constitution, the right to freedom, enshrined in the set of social and individual rights on which our society is built.

The concessionaire's website states that it is the user's right to "obtain and use the service with freedom of choice, subject to the rules established by the State of São Paulo"[42].

It is pertinent to point out that the relations between the public service concessionaire and its users must be based on good faith, that is, in the words of Cláudia Lima Marques, "reflected performance, thinking about the other, the contractual partner, respecting him, respecting their legitimate interests, their reasonable expectations, their rights, acting loyally, without abuse, without obstruction, without causing injury or excessive disadvantage, cooperating to achieve the proper end of obligations: the fulfillment of the contractual objective and the fulfillment of the interests of the parties "[43].

Commercial exploitation contractually allows for profit-generating activity, however, this activity should be based on the user's freedom to participate or not. The practice of obliging the user to generate profit for the concessionaire through a situation included in another good acquired by him may be, by analogy, equated with the married sale situation.

It could be argued, on the basis of this contractual permission, that the activity of collecting demographic data for commercial purposes is similar to the lawful and already consolidated activity of renting advertising space. That is, third parties would be paying the dealership in exchange for some advantage for themselves, in which the user does not choose whether to see that ad or not.

It turns out that the situation narrated does not match that of offering space for commercials, and this can be summed up for one reason: what is being offered as a

42 Source: <http://www.viaquatro.com.br/guia-do-usuario/direitos-deveres>.
43 MARQUES, Cláudia Lima. Contratos no código de defesa do consumidor. 5a. ed. São Paulo: Revista dos Tribunais, p. 216.

lucrative counterpart comes not from something owned by the dealership, but from its users. That is, instead of charging a value from the third party to offer in return a space held and controlled by the concessionaire on trains or stations, in the situation under consideration, value is charged to deliver in return data obtained from the activity of the transit users by trains and stations[44].

Considering that the users are not commercially linked to the concessionaire beyond the acquisition of the transportation service, they could not be directly participating in the counterpart of this profit generating activity without being able to choose informedly about it.

IX.V. Concerning the hidden price of the service provided - manifestly excessive advantage

That is, if a consumer cannot be obliged to purchase a product attached to another which he does not choose, it is obvious because the price of both is included in the price of the first product and this hurts the duty of transparency and freedom of choice over what you want to acquire. This is what happens to the subway user being forced to generate profit for the concessionaire by capturing their data. Not only does he pay cash to use the service, he pays the concessionaire with his data, in a hidden way and without any choice.

The situation also falls within the event of misleading advertising by omission, whereas the ad fails to say something relevant that would be essential in consumer behavior. By omitting that all users of its transportation system would be required to integrate demographic research through compulsory face detection, the concessionaire omitted an essential factor of what was being purchased by those using the urban transportation provided by it.

By purchasing and using the ViaQuatro subway service, the citizen also provides data with their participation in the demographic survey conducted there, an abusive practice indicated in the hypothesis of art. 39 of the CDC, which points out that the supplier is forbidden to “demand from the consumer a manifestly excessive advantage”. Still, violates the provision of art. 6, CDC, which states, in section IV, that basic consumer rights are protection against “coercive or unfair commercial methods, as well as against unfair practices and clauses”.

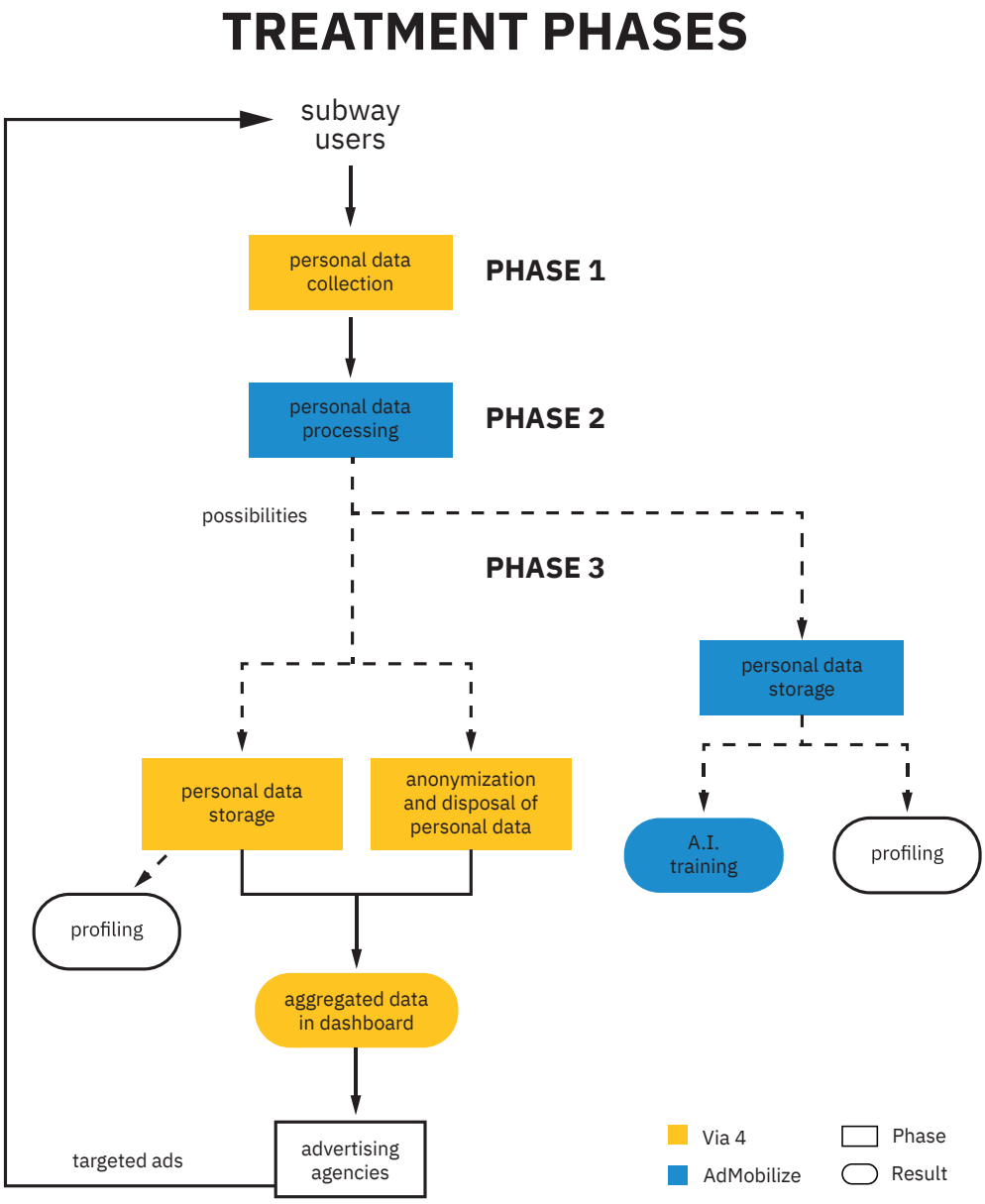
The user remains without freedom to choose what to buy and there is total opacity about the real price of the purchased good, which is masked by an inevitable consume situation.

44 This phenomenon, in which users of a particular service are used as raw materials for their profitable products, is the basis of the model called “surveillance capitalism” by Harvard Business School researcher and professor Shoshana Zuboff. She warns of the risks to freedom and autonomy posed by this production system in ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização da informação. In: **Tecnopolíticas da vigilância**: perspectivas da margem.BRUNO, Fernanda et al (org.). Boitempo, 2018.

X. Concluding remarks

From the material contained in the case, it is verified that the situation analyzed consists of violation of the Federal Constitution, the rights of Consumers and Users of Public Transport, as well as the rights of protection of personal data and rights of consumers by ViaQuatro public transport service concessionaire, through the Interactive Doors service, which captures user reactions to advertisements through cameras at stations.

The procedure consists of three technical phases to be taken into account: 1) collection of images of people's faces through cameras; 2) treatment of these images to elaborate the mathematical model of the face, and subsequent extraction of information on age, gender, and emotion felt when viewing the advertising; and 3) alleged elimination of the images and mathematical model of faces, with the supposed aggregation of information on users' detected emotions by anonymization technique, sent to ViaQuatro.



Source: authors.

There is, in phases 1 and 2, the clear processing of personal data related to the image collected from subway users and the subsequent elaboration of the mathematical model of the face (sensitive personal data), to infer the emotions felt when viewing the algorithm from AI from AdMobilize. In phase 3, the supposedly anonymized data is transferred through aggregation to ViaQuatro. However, ViaQuatro did not demonstrate whether it exists and what anonymization technique would be used at this stage of data processing. Transparency regarding the technique used is important because anonymization is not a process characterized as absolute, but one that allows gradations, according to the state of technology development and the context in which personal data are processed. For more sensitive data, such as biometric and emotion information captured, the use of more robust techniques would be appropriate to avoid the possibility of reversal of anonymization, especially when considering the current easiest crossing of several categories which facilitates reidentification of the data. In addition, anonymization is a measure encompassed by the current sparse regulatory framework for the protection of Brazilian personal data, mainly to ensure the inviolability of information security, as established by Decree No. 8,771/2016. Still in relation to Phase 3, there is also reasonable doubt, regarding AdMobilize, about the actual elimination of individualized records, either from images or from the mathematical model of faces associated with detected emotions.

Therefore, it is essential to consider that the documents gathered by ViaQuatro are not comprehensive, nor scientifically substantial, about the data collection and processing procedure performed through the Interactive Doors. Thus, it is not clear what information is transmitted to the AdMobilize software, by which locations and servers this information is transmitted and whether or not it is stored individually at any of the steps, to verify whether AdMobilize stores personal data, and whether anonymization was appropriate. data sent to ViaQuatro.

Even though anonymization is deemed to have occurred properly for sending data to ViaQuatro and AdMobilize does not store any data, the treatment as a whole has biases in phases 1 and 2 as there is a violation of users' rights regarding duty to inform them about the treatment, as well as the freedom to choose whether or not to participate in this activity (consent to the use of their image). This situation in itself already violates the self-determination that underlies our rights system. Thus the chain of treatment becomes biased due to initial illegality, similar to the theory of the poisonous tree fruits.

Reaffirming, the situation described does not match that of offering space for commercials, and this can be summed up for one reason: instead of giving costly to an advertising company a space owned and controlled by the concessionaire on trains or stations in situation under analysis the profitable offer given by the concessionaire is data obtained from the activity of users, their customers, who travel by trains and stations.

Since ViaQuatro is responsible, as concessionaire, for ensuring that there is no violation of its users' rights, this responsibility also permeates the contracting with third parties. The reasonable doubt about what actually happens to data on phase 3 is based on the economic value that face and emotion recognition software has on the market, and the relevance that a comprehensive database can have for training these artificial intelligence algorithms.

The existence of anonymization and its degree of adequacy does not rule out the violation indicated in the early stages of processing, but must be taken into account by the judiciary regarding the response to the practices of each company. This parameter can avoid the possibility of two unwanted consumer situations: i) that companies enter the legal costs of violations into their opportunity cost and refuse to produce evidence of what is actually made of the data, without knowing the extent of the damage to users, the anonymization and security levels, as well as understanding of the functioning of the chain involving personal data or ii) the upcoming of a strong antagonism between technology companies and the Brazilian legal system, which hinders the progress of technology regulatory projects, influenced by the industry's fear of new situations of instability. These situations can create a scenario of regression to consumer rights and lead to increasingly obscure use that is far from the population's knowledge of technologies that handle their data.

It is crucial that the decision on the case takes into account the pillars of protection against automated treatment and those concerning self-determination, both within the framework of constitutional and consumer rights, and the logic of existing sparse data protection rules, such as the Internet Bill of Rights.

There is no doubt, therefore, that there was damage, since all of the above indicates that the violation of the collective rights related to the consent, information and self-determination of subway users is evident. However, it should be noted that the documents filed by ViaQuatro are not sufficient to exclude the possibility of damage caused by insufficiently anonymized or non-anonymized personal data, which is even more serious. Considering that a possible storage would also lead to further processing of individualized data, which may lead to the re-identification of people and their emotions, would be inherent in this situation all risks linked to the processing of personal data, and, more seriously, of sensitive data, allowing discrimination against such persons and causing moral damage to all subway users.