

Volume 38  
issue 2 / 2019

Contracampo e-ISSN 2238-2577  
Niterói (RJ), 38 (2)  
aug/2019-nov/2019

Contracampo – Brazilian Journal of Communication is a quarterly publication of the Graduate Programme in Communication Studies (PPGCOM) at Fluminense Federal University (UFF). It aims to contribute to critical reflection within the field of Media Studies, being a space for dissemination of research and scientific thought.

## 14 FRAGMENTS OF A FACE: facial recognition and visibility negotiations in sociotechnical networks

RAFAEL RODRIGUES DA COSTA

Doctorate degree in linguistics, Federal University of Ceará (UFC). Adjunct Professor of the Social Communication/Journalism School of Federal University of Ceará. Member in PráxisJor research group. Fortaleza, Ceará, Brasil. For this paper contributed with the theoretical foundation, data analysis and the segments of introduction and conclusion.  
E-mail: rafaelrg@ufc.br.  
ORCID: <http://orcid.org/0000-0001-8566-1112>.

NAIANA RODRIGUES DA SILVA

Master's degree in Communication, Federal University of Ceará (UFC) and Doctorate student in Communication, University of São Paulo (USP). Assistant Professor of the Social Communication/Journalism School of Federal University of Ceará. Member in PráxisJor research group. Fortaleza, Ceará, Brasil. For this paper contributed with the theoretical foundation, methodological decisions, data analysis and the segments of conclusion.  
E-mail: naianarodrigues@gmail.com.  
ORCID: <http://orcid.org/0000-0003-1966-3616>.

TO REFERENCE THIS ARTICLE, PLEASE USE THE FOLLOWING CITATION:

COSTA, Rafael Rodrigues da; SILVA, Naiana Rodrigues da. 14 FRAGMENTS OF A FACE: facial recognition and visibility negotiations in sociotechnical networks. *Contracampo*, Niterói, v. 38, n.2, p. XXX-YYY, Ago./Nov. 2019.

Submitted on: 04/10/2019 / Accepted on: 07/29/2019

DOI – <http://dx.doi.org/10.22409/contracampo.v38i2.28477>

## Abstract

The use of recognition techniques from body attributes dates back to the adoption of the first police intelligence databases. Nowadays, facial recognition is seen as a surveillance instrument pertinent to the forensic sciences, but also capable of provoking discussions about subjectivation regimes. This research discusses how the negotiation of visibilities in sociotechnical networks is triggered from the processes of facial recognition in Facebook. This is an exploratory study, in which a questionnaire was applied with 152 users of that platform. The results indicate that the visibility provided by the facial recognition is not adopted by this group of users due to privacy reasons, although they have acted as managers of the visibility of other users by means of manual tagging in photographs.

### Keywords

Facial recognition; Sociotechnical networks; Visibility; Identities.

## Introduction

Brazil, 5th March, 2019. During Salvador's Carnival festivities, Marcos Vinicius Neri had his face recognized by a camera - made by the Chinese company Huawei - connected to a database of outlaws and wanted criminals in Bahia. Neri was a homicide suspect and the police had been trying to track him down ever since 2018. The man was arrested (Távora, Araújo & Sousa, 2019). The device that captured his face was one of the 42 cameras installed in strategic places designated according to the police operation in Salvador, in order to ensure people's safety while partying at the Carnival (Câmeras de Reconhecimento, 2019).

United States of America, 6th March, 2019. Mark Zuckerberg, founder and CEO at the social media platform Facebook, published a post announcing changes in his main services - Facebook, Messenger, Instagram, WhatsApp - as an attempt to establish, according to him, a more intimate environment to conversations people have. Zuckerberg emphasizes, along his text, privacy as a central value that should be the basis to all of his companies services, and platforms integration as a way to make interactions closer and out of an indiscriminate public reach. "For a service to feel private, there must never be any doubt about who you are communicating with. We've worked hard to build privacy into all our products, including those for public sharing" (Zuckerberg, 2019).

Marcos and Mark portray, in different perspectives, the ambivalence that surrounds the extensive production, storage and data analytic process, where the most diverse practices are effectuated - from police investigations to simple conversations in smartphones. On one side, there are claims for security and privacy, defined in consonance with examples of escaping from crowds, data protection or absence in public spaces. On the other hand, there is a search for a clairvoyance expressed by the idea that it is necessary to identify, know or certify who they are interacting with, under the sentence of putting in risk the credibility of these interactions.

In both cases, what seems to be the delimitation factor is the physical presence or, more precisely, the human face, represented by a profile avatar of a social network, an image in a database, as a guarantee source of an identity that establishes itself as different and unique, coming from the premise that no face is entirely equal to another one. In the boundaries of this capsule wrapped by eyes, hair, skin, mouth and ears, rests not only the borders of access to a mysterious life, a delimitation of who you are and who you are not, but also the last border to be investigated by surveillance and control tactics, functioning conforming the capital accumulation, where individuals are entrepreneur unities (Dartot & Laval, 2013).

Therefore, the popularization of face recognition techniques (Woodward Jr. et al., 2003; Okabe & Carro, 2014; Braga, 2013; Indrawan et al., 2013; Oh et al., 2016; Yan et al., 2017) makes us question, by looking at the previously mentioned ambivalence, how the individuals visibility is articulated contemporaneously, in a platform society (Van Dijck, 2017; Helmond, 2015), where algorithmic governance (Castro, 2017) and submissions to a performance regime (Han, 2015) are operated simultaneously.

Based on this inquiry, we will discuss in this research how visibility negotiation in sociotechnical networks is triggered from the processes of facial recognition in Facebook. Initially, we will review the concept of visibility (Thompson, 2018; Sibilia, 2015) considering its application in contemporary contexts. Subsequently, it will be approached technical and conceptual assumptions about face recognition, as an attempt to understand what sort of appropriation of this activity is applied by Facebook. Finally, the methodological decisions in this study will be presented, followed by results and discussion.

## Seeing and being in the contemporary age

When facing communication scenarios, people tend to use as much individual resources as material ones to define who they are to themselves and to others. This second aspect consists exactly in

acknowledgement and identification of a person by everyone else. Therefore, identity comprises a double movement, from what is particular of the self to an assumed social script that will be interpreted by others.

Identity used to be considered singular, as a stable marker and a showcase of the most essential traits that people would carry from birth to death, capable of giving someone the power of certainty. However, realizing that modernity did not follow a linear path, the modern man found himself obligated to rethink himself (Giddens, 1991). The very own idea of identity is reviewed, changing from the concept of something unique, that remains the same, to a multiple and plural notion. Someone who lives in a late modernity (Giddens, 1996) or in a postmodernity is able to hold multiple identities (Hall, 2003) or express different identity constructions along their psychosocial existence (Ribeiro, 2014).

This background favors the emergency of studies that consider identity as a result of a dialogic relationship with alterity. According to Kathryn Woodward, Stuart Hall and Tomaz Tadeu da Silva (2000), identity is not a subjective composite that comes from the inside out. It takes form through subjectivity, social roles and the recognition of another different being. Both configuration of subjectivity and identity experience the process of acknowledgment. And to be acknowledged, in contemporary age, implies to be seen, taking the action of seeing not only a physical perception of forms, colors and material, but also the symbolic discernment of individuals. Acknowledgement relies on visibility, on how someone stands out in the crowd, which is represented, in the context of a network society (Castells, 1999), by communicational spaces such as social networks platforms.

These highly symbolic environments are places where subjectivities and identities are performed aiming to be acknowledged by others. In order to accomplish this goal, individuals use a great variety of codes (visual, sonorous, verbal, etc.) that make them visible among numerous connected people. Thompson (2018) compares the changes around visibility with the transformations that happened due to interactions and communicative mediations.

In face-to-face interaction, visibility is tied to the spatial and temporal properties of the interaction situation and is reciprocal in character: each participant in the interaction is visible to everyone else. (...) In the case of mediated quasi-interaction, visibility is no longer reciprocal in character. The medium changes what I call the directionality of vision: TV viewers can see the distant others who appear on their screens but the distant others cannot see them. In the case of online mediated interaction, the directionality of vision is different again because many participants in the interaction may have means at their disposal to make individuals, actions and events visible to distant others. (Thompson, 2018, p. 287).

The author states that the changes in visibility regime that occurred due to online communication modifies diverse social instances such as the political power - a phenomenon that both Brazil and the United States of America face constantly as a result of controversies presented in Twitter interactions between their respective presidents and their audience. These examples reinforce Paula Sibilia (2015) thesis, to whom the manner we connect to ourselves and the others was significantly modified in the transition from the 20th century to the 21st thanks to the performatic way of being in the world (Sibilia, 2015, p.356).

The author suggests that the existence of individuals is tied to their performances visibility. The everyday life performed in sociotechnical networks becomes not only a public spectacle accompanied by followers, friends and visitors, but also a dispute subject, competed among individuals because, as Sibilia affirms (2015, p.357), each person fights to “stand out in a outer appearance market more and more competitive” and, in order to succeed, they build representations from communicational and interactive possibilities provided by the platform.

It is possible to observe that the comparison proposed by the author between subjectivity construction and commerce is not simply metaphorical. The craving for visibility performances is part of the neoliberal logic, the neoliberal reason in contemporary times. According to Dardot and Laval (2013),

the contemporary rationality revolves around the construction of subjectivity based on enterprises management styles, stating competence as the main behavior rule that should be followed by individuals or the front (Goffman, 2013) that they flaunt publically and to themselves. For that matter, social acknowledgement of individuals is only possible thanks to visibility performances. Nevertheless, only communication elements are able to build visible, memorable and knowable performances due to the competitiveness resulted from the high density of individuals present on the sociotechnical networks. The competent and competitive individual is the one that searches the best way to maximize their human capital in all of their domains, not only projecting themselves to the future and calculating their profits and expenses, like the old economic man, but also pursuing, above all, improvement on themselves, looking for transformation and refinement, becoming each day more efficient (Dardot & Laval, 2013).

As the authors indicated, the impression management of the self is not limited to the field of business or to work issues, it spreads to the most various scenarios that exist while living in society. Masters of their own choices, the entrepreneurial men are the only ones responsible for their success or failures. Philosophe Byung Chul-Han (2015) reminds us all that the contemporary society lost the discipline appeal because the social acceptance is no longer tied to an obedience to power institutions.

The role model citizen is productive and delivers high quality performances (at work, communication and physically). It is the performance individual. Han (2015) states that unlimited power is the positive modal verb of the neoliberal society of performance and quotes the affirmation “Yes, we can”, which precisely expresses the positivity trait in a neoliberal society of performance. The author also highlights that, instead of prohibition, commands or law, there is project, proactivity and motivation. While the discipline society is still dominated by negativity, creating insane and delinquent people, the service-oriented society produces losers and depressed individuals.

In this service-oriented society, identities are forged based on visibility, which can be reached through likes, comments and shares. The loss of followers in sociotechnical networks is an indication of failure to the service-oriented individual. Therefore, invisibility is a symbolical death of the entrepreneurial men, who feels impotent and devoid of identity, because he is only another ordinary profile in the artificial chain of algorithmic selection.

## Tactics and ambivalences of face recognition

The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others.<sup>16</sup> Under our system of government, he can never be compelled to express them (except when upon the witness stand); and even if he has chosen to give them expression, he generally retains the power to fix the limits of the publicity which shall be given them. (Warren & Brandeis, 1890, p. 198.)

This is a quote from “The Right to Privacy”, an 1890 article considered the first affirmation on the right to privacy, in the scope of USA legal system. In this text, jurists Louis Brandeis and Samuel Warren argue that privacy is, in essence, the right “to be left alone” (p. 205). Subsequently, they ponder if the legal guarantees related to this right can be extended beyond the cases where an expression or media had been used to enter the private space of an individual. It was an attempt to consolidate a general right to privacy regarding thoughts, feelings and emotions - to the point where even conversations face-to-face and facial expressions would be considered in the scope of such protections.

Still during the 19th century, the Parisian police initiated the utilization of databases containing suspects measures and body informations, in order to elucidate various incidents such as homicides, paternity determination and prisoners identification (Jain et al., 2004). However, the use of evidences or material proofs in this background dates back to the beginning of the human civilization, where there was

already an effort to establish an “incipient judicial system structure” (Calazans & Calazans, 2005) capable of conciliate distinct interests and/or opposites (Capez, 2005).

These efforts have been subsidized by a notable technological development that took place specially in the last 100 years, that provided new tools and techniques to criminal investigation routines. It is precisely at this technological support that rests the forensic science peculiarity, defined by Fachone & Velho (2007, p. 153) as the classification given to the efforts of generating technology and science in order to clarify related questions in the field of public and criminal justice system. Phonetics, ballistics, spelling and fingerprinting exams, genetic testing and document background checks are some of the areas covered by forensic science, with criminal law specialists and knowledges from many different subjects.

Beyond the legal and police world, the human body singularities, specially the face traits, have been used to distinguish people from one another since remote times. The face can be understood as a territory susceptible to regulamentation as well as to become a storable and interpretable data, while submitting itself to the will of a neoliberal governmentality (Foucault, 2008), distinguished by an individual body discipline as well as by social control, designed thanks to the accumulation of measurable informations about people’s grouping.

Castro (2017) describes the rise of these large databases as a reconfiguration of the biopolitics proposed by Foucault, originally delimited in a social body management through disciplinary institutions. In its place, emerges an algorithmic governance, relying in big data and in algorithmic data process. The probabilistic analysis, that already appeared as an institutional control facilitator during the 19th century, is colonized by a capitalist logic. In this analysis, the proliferation of metrics projects outlines of the market, socially, and it is equivalent to a sort of risk management - the goal is no longer neutralize it, as in the State of well-being, but live with it (Castro, 2017, p. 4).

The technical developments in the fields of computer sciences, artificial intelligence and information technology along the 20<sup>th</sup> and 21<sup>st</sup> century provide a more consistent concept to this kind of existences management. Face recognition processes - improved thanks to electronic and digital tools - are commonly associated to biometrics, understood as “any automatically measurable, robust and distinctive physical characteristic or personal trait that can be used to identify an individual or verify the claimed identity of an individual” (Woodward Jr. et al, 2003, p. 1).

In a sociotechnical network platform such as Facebook, our face is perceived as the assurance acknowledgement factor, with purposes that vary between safeguarding publications authenticity to the social capital approachability and negotiation (Facebook Privacy Basics, 2019). Although the face is less valuable regarding its robustness and distinction when compared to other body parts, it was not randomly designated to Mark Zuckerberg’s platform name. It appears like a commodity from which users perform their identities, as debated in the previous topic.

The profile personal image on Facebook is one of the mandatory public elements to be provided by users, suggesting the importance of this content unity to the platform’s functioning. From a corpus with 7200 profile images from Facebook, collected in 30 cities around the world, Rueda & Giraldo (2016) reported that the human figure represents the typical profile image (p.127). From another perspective, Baert (2018) observes that individuals with profile pictures considered the most beneficial ones on Facebook - face pictures classified as the most attractive during previous evaluation tests - received approximately 38% more invitations to job interviews when compared to candidates with images considered the least beneficial. It is possible to assume, from the notes of these two authors, that the face registration in audiovisual devices meets a strategic role to potentialize claims from the previously mentioned service-oriented society.

Images that feature the human face, even if only partially, provide enough elements to the success of face recognition systems. This sort of automated system can register the spatial geometry of distinctive face traits (Woodward Jr. et al, 2003) in a similar way to the human perceptual system. A number of



researches have reported various types of face recognition techniques, but all of them rely on the main face attributes, the so called nodal points (Okabe & Carro, 2014). Examples of nodal points are the distance between the eyes, the nose length, the orbit cavity, the bones on the side of the face, etc. Systems such as FaceIt, developed by Visionics, a company located in the US, require at least 14 nodal points in order to succeed in face detection and assign a face signature as a numeric code in a database.

The stages of recognition may include face detection in a static image or in motion, storage of features, and identification/recognition originated from a database search for matches (Braga, 2013; Indrawan et al, 2013). An essential problem in these processes is the accuracy of face detection and its later association to a database.

Oh et al. (2016) enumerate four dimensions capable of disturbing an individual identification in a face recognition system: the number of labeled heads, the type of face obfuscation or obstruction, the quantity of obfuscation or obstruction and the domain displacement (images where an individual intentionally appears might have been registered at a same or various events). This study approaches more directly the fragility of privacy limits, by suggesting, for example, that obfuscation techniques, such as distortion, have a restrained effectiveness in preventing individuals detection. Application of metadata in order to catalog images, usually in sociotechnical networks platforms, is another procedure that puts privacy in risk.

On the other hand, Yang et al. (2017) present what is considered to be the benefits of overseeing face attributes located in specific parts, such as mouth or nose, in natural networks. The authors develop a faceness<sup>1</sup> scale, based on the mentioned attributes, used to train the face detector for working under adverse conditions, like severe occlusion and indiscriminate pose variations found in photographs. In addition to describing how face recognition systems operate, these researches illustrate how governance tactics rely on institution and legitimation of databases, surrounded by protocols of companies interference that explore these systems.

## Methodology

The methodological approach taken in this study is a qualitative and exploratory investigation. As noted by Deslauriers and Kerisit (2008), qualitative outlines attempt to handle social actors concerns in a way that a study based only in quantitative techniques would not be able to cover. Beyond looking for reality transformation, qualitative researches can be more concerned in developing a deeper knowledge of a social phenomenon, be it because of its transience or complexity.

Given the above, we decided to execute a qualitative study, exploratory in nature, since we align contemporary discussions related to society and the daily use of technology, based on our literature review, as an attempt to instigate reflections about an emerging social and technological phenomenon: face recognition in digital platforms. The theoretical framework relies on various schools of thoughts, from the most classical debate on identity to the concepts found in the computer sciences, that explain the functioning of this face recognition in platforms.

In order to avoid an essayistic path, we opted to develop an empiric research based on questionnaire applications to a wide and heterogeneous audience found in social networks platforms. This questionnaire was designed and applied as an indirect form of access to the researched phenomenon. Thiollent (1982) suggests that, as a technique of indirect data collect, questionnaires should be planned and properly applied to capture the individuals judgmental systems about socially debated subjects or themes.

In this study, we came up with questionings elaborated to capture Facebook users perception

---

<sup>1</sup> In this study, "faceness" assumes a more instrumental sense rather than the one attributed by Deleuze and Guattari (1996), which would be a device that merges significance and subjectivation process.

about face recognition tools in this particular platform and still inquire these same users about their use and photo posting motivations. For that matter, our questionnaire was built upon 20 questions, with 4 of these being open-ended questions, while the other 16 were multiple choice or subjected to straight answers. Thiollent (1982) notes that the prevalence of close-ended questions has better chances to reach a higher number of informers. That is the reason why we chose to this kind of structure, since our expectation was to gather an embracing sample of informers in qualitative terms, although non-probabilistic.

The target-audience to our questionnaire consisted of Facebook users who were willing to cooperate and did not face any obstacles to do so, such as language barrier or literacy absence to answer the questions hosted in Google platform. That all being said, the questionnaire application was launched in social networks Facebook, Instagram and WhatsApp through the authors personal profiles. In order to broaden the sample to an audience that was not in the range of our personal contacts, we adopted the snowball sampling.

The snowball sampling is a chain-referral technique applied to subjects networks, to create informers groups (Baldin & Munhoz, 2011). Therefore, it seemed only logical the usage of this technique in this study, because it is about individuals behaviors in gregarious ambiences of network organization. Particularly in this research, the purpose on this sampling strategy was not to reach the global users universe on Facebook in Brazil, estimated in 127 million people (Oliveira, 2018), and about whom it is not exposed more precise data. The goal was to build a random informers network, able to offer a great variety of information (Baldin & Munhoz, 2011, p. 332). Overall, 152 users answered the questionnaire applied between 20th and 31st March of 2019.

This study is also based on interface observation technique of the social network platform Facebook, occurred during previous login by the authors of this research, who joined the network under similar conditions to other users of this platform. Along the months February and March of 2019, we logged into the platform with no specific frequency, through mobile devices (smartphone) and laptop. In addition, bibliographic and documental research techniques were used to accomplish the already mentioned conceptual discussions and applied so that they could allow a proper analysis on the proposed theme - face recognition -, as well as comprehend guidelines and terms of use related to this technique on Facebook - which was done by accessing the recommendations and warnings given by the platform itself.

## Data analysis

The exploratory nature of this study allows the data analysis to comprise available documents about face recognition, provided by Facebook, Zuckerberg's manifest and the questionnaire results. Overall, the empiric research obtained answers mostly from individuals aged from 25 to 34 years old (38.2%). Among the participants, 7.5% (equivalent to 11 informers) identified themselves as college professors, while university and high school students summed a total of 9 individuals, which is equivalent to 6% of the sample. Considering that these were the most common professional categories in the poll, it is possible to assume that there was a great diversity of professional identities.

It is important to highlight that 98% of informers use Facebook for over a year, while 36.2% access the platform daily and stay connected for over an hour. This constant and prolonged frequency might be related to the fact that 63.3% of informers use Facebook as a work tool. Furthermore, it is possible to add to this information the ubiquity and mobility of the access through mobile devices, after all, 71.2% of the respondents log in to the network through their smartphones.

After presenting the participants social profile and their Facebook usage habits, we will now describe the regulations of face recognition on the platform. It is fundamental to highlight that to access these face recognition regulations, the user must access their profile settings and select the option "Face Recognition". They will then be directed to a new screen and be questioned if they want Facebook to be



able to recognize them in photos and videos. In that case, the platform only offers the options "yes" or "no", establishing the users choice to extreme situations. There are no choices that could mean negotiations between the platform and the user, such as recognition only in photos or only in videos, or execute this type of recognition exclusively in posts from friends, family or other social groups posts that can be built in the network.

This closed choice has a strong effect on the individual visibility and its attributes, such as recognition and social capital. The subject is seen, but may come across unscathed to others recognition, specially those who are not part of their primary connections network. Face recognition of an individual in a photo, for example, expand the published image visibility, since the actors connected to the subject whose face is tagged on the photo can also visualize this image on their timelines. Consequently, the referred photography may attract more likes and comments, promoting more visibility to the actor who posted the image and to all of those whose faces were tagged.

In practice, the platform compares machine intelligence capable of executing this task to the human users ability to do the same. This grant, when allowed, highlights subtleties such as deliberate management of social capital or the attention flow in networks where a user is present. To the users, photo and post tags have a quantitative value expressed, for example, in decisions such as accepting certain tags and rejecting others.

"I think it is interesting to have an option to approve or disapprove a tag in photos from other people", says one of the respondents in our poll, answering the closing question from the questionnaire, where users could freely express their opinions about face recognition. Another respondent affirms that it "makes it easier the task of tagging one person at a time". These statements acknowledge a logistic support to visibility management present in the referred tool, while assuming to have context rules to attribute relevance to a certain tagging - approving would be an endorsement to the value of that publication.

However, an accurate evaluation of this value attribution does not seem to be in the algorithm reach, which can be understood from users findings that the platform performs a type of inquisitive indexicality, based on unwanted tagging, out of context or simply unfounded. When asked if they had ever been tagged in photos where they were not present, more than half of the participants answered "yes".

When the users choose to not have their faces recognized by the platform, they lose the possibility to expand their visibility to friends of friends, for example. Therefore, this option sets a closure to relationship branches and visibilities possible at the platform and can be read as a way found by Facebook to pressure its users to accept the conditions of face recognition, due to the visibility loss and having to afford the price of this decision in a symbolic trade market.

Face recognition regulations can be accessed through a link, still in the user settings, that leads to another web page where it is possible to find a face recognition usage description and its importance to users in a screen entitled "Facebook Privacy Basics". Through an interactive infographic, Facebook presents reasons to accept the terms and conditions related to face recognition, allowing us to list the following classification:

- *instrumental*: "let you tag people quickly and easily". In other words, the platform executes a task for the user, revealing the action automatism.
- *security*: "help protect you from strangers using a photo of you as their profile picture". The platform then demonstrates a regulatory power, being capable of acting as a judge or another law professional by defining, through face recognition, the veracity or falsehood of a profile, taking care of the user identity.
- *accessibility*: "help people with visual impairments by telling them who's in a photo or video". In that case, the acknowledgement action transforms into a democratization act of the platform contents to users with visual impairments. It is possible to understand this justification for face recognition use as a way of stating that people who do not activate this

tool are not being empathetic with disabled people or limiting Facebook usage to those with special needs. It is a moral perspective that puts the platform as an inclusion agent and the users who do not accept the recognition tool as social exclusion agents.

- *visibility*: “and let you know when you might appear in photos or videos, but haven't been tagged”. In this topic, the platforms reveals once more its surveillance and regulation mark, since it is capable of not only identifying an user presence in images, but also naming them, enabling them enjoy the benefits of visibility and recognition, while protecting their identities. (Facebook Privacy Basics, 2019).

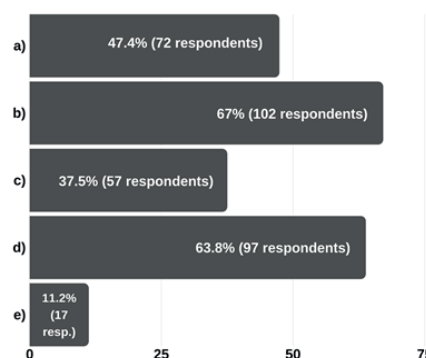
Still in Privacy Basics, the platform explains, in a simplistic way, that recognition is made from photographs comparisons and videos posted by the user himself, such as profile picture and images that they have been tagged in. Afterwards, it is explained that the user can “control face recognition in your settings” (Facebook Privacy Basics, 2019). This secrecy of techniques, modes of action, rather than considering that the user is unable to understand algorithmic logic, can be interpreted as a platform opacity, a protection decision against the competition (trade secret) or even a precaution regarding the law, security politics and privacy State and/or Governments.

Besides, the highlighted excerpt also brings an idea of control and regulatory power granted to the user. However, this idea is illusory, when we realize that this power is not extendable to knowledge of recognition operation mode and it is limited to the ability of choosing "yes" or "no". This Facebook stance tends to perpetuate in case explanations about its operation modes are not requested. Nevertheless, our empirical research revealed that 60% of 152 respondents do not know the face recognition settings on the platform, implying the thought that many users are not willing to get to know Facebook's *modus operandi*.

When interrogated about face recognition senses, in a question that allowed more than one answer, 102 respondents, equivalent to 67% of the total, declared to agree with the sentence "Face recognition may violate my privacy when tagging unwanted or unsolicited photographs". In the following Figure 1, this alternative corresponds to item b). Other affirmations presented to the users, and their respective accordance rate were:

- a) Face recognition prevents other people from using my photos without my consent (72 respondents, or 47.4%);
- c) Face recognition helps me to connect with other users, since it can tag me in their pictures (57 respondents, or 37.5%);
- d) Facebook's system of face recognition stores my data, and this is not always safe (97 respondents, or 63.8%);
- e) Face recognition helps to increase the number of followers, likes and other interactions in my profile (17 respondents, or 11.2%). y).

Figure 1: Percentage of participants accordance regarding affirmations on face recognition.



Source: designed by the authors of this research.

Among the majority of users who declared to agree with affirmative b), the ones that do know the platform privacy terms seem to be suspicious or cynical regarding Facebook's security justification about its privacy settings. It is still quantitatively relevant the accordance with item d), which suggests the users preoccupation with data analytics at the platform and also a certain uniformity, in the inquired universe, regarding privacy threats, which in this case are potentialized by big data.

It is interesting to observe that, among the participants, only 11% associated face recognition with visibility, by realizing that this tool can increase the number of followers, likes and other interactions. This result is tied to the fact that only 7.9% of informers consider very important being tagged in a Facebook photo. Likewise, only 10% of the respondents believe it is very important to tag people in photographs posted on the platform. These indications are intriguing because they reveal that privacy concern is quite ahead in the dispute with visibility.

Some contextual facts can justify this tendency, such as misinformation propagation in the form of fake news in various platforms, data leaking as in the Cambridge Analytica scandal and the very own manifest written by Facebook's CEO, Mark Zuckerberg, in which privacy concern is put as the main reason to make changes in the platforms under his watch.

I understand that many people don't think Facebook can or would even want to build this kind of privacy-focused platform -- because frankly we don't currently have a strong reputation for building privacy protective services, and we've historically focused on tools for more open sharing. But we've repeatedly shown that we can evolve to build the services that people really want, including in private messaging and stories (Zuckerberg, 2019).

In these situations, the spontaneous performance of machine intelligence appears to users as an alert, because it highlights the platform autonomy and the human control disadvantage due to an algorithmic control. Therefore, face recognition does not seem to be an indispensable factor to visibility promotion and identity construction in sociotechnical ambiance, although 84.9% of the 152 informers had already used this tool to tag a friend in a photo.

This controversy between using face recognition and not considering it quite important may lead us to think about a certain users automatism regarding the tools available in the platform's interface, making them rely on the instrumental dimension of face recognition and, therefore, execute actions which implications to their identitary performances cannot be measured. However, there are users who problematize the privacy sense in a more structural form, questioning not only the visibility dynamic and the platform's recognition, but also pondering over data value in Facebook's traffic. "The use of these data is a matter of concern. Facebook is not for free. We are the merchandise, but we never know exactly to what or to whom we are being sold. Even though we are aware of this, we still use it and expose ourselves a lot". This participant's concern, expressed in the questionnaire session designed to free comments, indicates clarity regarding the society dynamics of productivity and subjectivity featured by the entrepreneurial man, questioning the platform's role while being a private entity and dealing with so many individuals informations given by the users themselves in exchange for visibility.

The caution in self-presentations on Facebook is also pointed out by the low update frequency of profile pictures. The following Figure 2 summarizes data obtained about this matter, indicating a great majority of users (94.1% or 143 respondents) who declare to update their profile picture less than once a month, while only 9 users affirm to do it more frequently, usually on a week basis.

Figure 2: Profile picture updating frequency.



Source: designed by the authors of this research.

When questioned about their motivations to update the profile pictures, some users indicated a need to approximate the profile picture to their current appearance, which may change in case of new haircuts, beard growth or natural aging. These ponderations seem to confirm the profiles utility as a space where the origin of individual identities is ensured. Equally relevant is the percentage of respondents who declare to publish pictures on their feeds less than once a month (69.7% or 106 respondents), a data that is in consonance with the perception of privacy and integrity risks, already noted in other answers of the questionnaire.

## Conclusion

This study aimed to investigate visibility negotiations between users and sociotechnical networks through regulations and uses of face recognition on Facebook. By analyzing the empiric research with 152 participants, the regulation documents on face recognition available at the platform and Facebook's CEO manifest it is possible to notice in this users group, how visibility negotiation at the platform through face recognition is a cognitive work extremely human. This way, the platform function especially as a decision auxiliary and less frequently as protagonist. This happens because by attributing this role to an algorithm would increase the risks of data monitoring, loss of privacy and deleterious effects of the "self institution" logic.

It is also possible to highlight that even though visibility loses in the strength dispute against privacy, this fear of privacy exposure does not push users out of the platform, because they have already built identity and recognition ties in there, after all, it is also a workplace, making them prefer to invest on visibility through other means, such as profile picture updating. This investment on a photo as a self manifestation shows identity management through this designation and identification tool provided by the platform and depends on user's action and will in order to be executed.

These negotiations made by users are results of a symbolic preservation instinct, a ontological security update extremely expensive to the modern man and resonate to Zuckerberg's speech. Whether it is a result of individual convictions or a fear instigated by dystopian fictions, it is a fact that the insecurity that boosts these negotiations do not modify deeper structures related to face recognition and algorithmic governance. It barely scratches the platform's surface, ensuring that Facebook continues to manage the wealth exploitation of network society: data.

## References

- Baert, S. (2018). Facebook profile picture appearance affects recruiters' first hiring decisions. *new media & society*, v. 20, n. 3, p. 1220-1239.
- Baldin, N.; Munhoz, E. M. B.. (2011). Snowball (bola de neve): uma técnica metodológica para pesquisa em educação ambiental comunitária. *X Congresso Nacional de Educação (EDUCERE)*. Pontifícia Universidade Católica do Paraná: Curitiba, 7 a 10 de novembro de 2011.
- Braga, L. F. Z.. (2013). *Sistemas de reconhecimento facial*. Monografia (Graduação em Engenharia Elétrica com ênfase em Eletrônica): Escola de Engenharia de São Carlos da Universidade de São Paulo, São Carlos, 2013.
- Calazans, C. H.; Calazans, S. M. P. B.. (2005). Ciência Forense: das Origens à Ciência Forense Computacional. In: XV Seminário Regional de Informática, 2005, Santo Ângelo. *Anais do 15º Seminário Regional de Informática*. Santo Ângelo: Universidade Regional Integrada do Alto Uruguai e das Missões.
- CÂMERAS DE RECONHECIMENTO facial vão ajudar a identificar criminosos no Carnaval. *Correio da Bahia*, Salvador, 26 fev. 2019. Retrieved March 20th 2019 from: <<https://www.correio24horas.com.br/noticia/nid/cameras-de-reconhecimento-facial-vaio-ajudar-a-identificar-criminosos-no-carnaval/>>.
- Capez, F.. (2005). *Curso de processo penal*. 12ª ed., São Paulo: Saraiva.
- Castells, M.. (1999). *A Sociedade em Rede: a era da informação, economia, sociedade e cultura*. Vol. 1 [The Information Age: Economy, Society and Culture, Vol.1]. São Paulo: Paz e Terra, 2. ed.
- Castro, J. C. L.. (2017). Redes sociais como modelo de governança algorítmica. XXVI Encontro Anual da Compós. *Anais...* São Paulo.
- Dartot, P.; Laval, C.. (2013). *La nueva razón del mundo*. Ensayo sobre la sociedad neoliberal. Barcelona: Editora Gedisa. Versão kindle.
- Delleuze, G.; Guattari, F.. (1996). *Mil Platôs - capitalismo e esquizofrenia*. Rio de Janeiro: Editora 34.
- Deslauriers, J.; Kérisit, M.. (2008). O delineamento de pesquisa qualitativa. In POUPART, Jean et al. *A pesquisa qualitativa*. Enfoques epistemológicos e metodológicos. Translated by Ana Cristina Nasser. Petrópolis: Vozes.
- FACEBOOK PRIVACY Basics. *Facebook*. Retrieved March 26th 2019 from: <<https://www.facebook.com/about/basics/manage-your-privacy/face-recognition>>.
- Fachone, P.; Velho, L.. (2007). Ciência forense: interseção justiça, ciência e tecnologia. *Revista Tecnologia e Sociedade*; 3(4). p. 139-161.
- Foucault, M.. (2008). *O nascimento da biopolítica* [The Birth of Biopolitics]. São Paulo: Martins Fontes.
- Giddens, A.. (1991). *As conseqüências da modernidade* [The Consequences of Modernity]. São Paulo: Ed. Unesp.
- Goffman, E.. (2013). *A representação do eu na vida cotidiana* [The Presentation of Self in Everyday Life]. Trad Maria Célia Santos Raposo. 19ª ed. Petrópolis: Vozes.
- Hall, S.. (2006). *A identidade cultural na pós-modernidade*. 11. Ed. Rio de Janeiro: DP&A Editora, 2006.
- Han, B.. (2015). *Sociedade do Cansaço* [The Burnout Society]. Translated by Ênio Paulo Giachini, Petrópolis, RJ: Vozes.
- Helmond, A.. (2015). The Platformization of the Web: Making Web Data Platform Ready. *Social Media + Society*.

Indrawan, P. et al. (2013). Face recognition for social media with mobile cloud computing. *International Journal on Cloud Computing: Services and Architecture*, v. 3, n. 1, p. 23-35.

Jain, A. K. et al. (2004). An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, v. 14, n. 1.

Oh, S. J. et al. (2016). Faceless person recognition: Privacy implications in social media. In: *European Conference on Computer Vision*. Springer, Cham. p. 19-35.

Okabe, R. K.; Carro, S. A.. (2014). Reconhecimento Facial em Imagens capturadas por Câmeras Digitais de Rede. In: *Colloquium Exactarum*..

Oliveira, F. (2018). Facebook chega a 127 milhões de usuários mensais no Brasil. *Folha de S. Paulo*, São Paulo, 18 de julho de 2018. Retrieved March 29th 2019 from: <<https://www1.folha.uol.com.br/tec/2018/07/facebook-chega-a-127-milhoes-de-usuarios-mensais-no-brasil.shtml>>.

Ribeiro, M.A.. (2014). *Carreiras: Novo olhar socioconstrucionista para um mundo flexibilizado*. Curitiba: Juruá.

Rueda, R.; Giraldo, D. (2016). La imagen de perfil en Facebook: identidad y representación en esta red social. *Folios*, n. 43, p. 119.135-119.135.

Sibilia, P. (2015). Autenticidade e performance: a construção de si como personagem visível. In *Revista Fronteiras – estudos midiáticos*. Vol. 17. Nº 3. Porto Alegre: Unisinos, September/December.

Távora, F.; Araújo, G.; Sousa, J. (2019). Scanner facial abre alas e ninguém mais se perde no Carnaval (e fora dele). *UOL TAB*, Rio de Janeiro, 11th March. Retrieved March 20th 2019 from:<<https://tab.uol.com.br/noticias/redacao/2019/03/11/carnaval-abre-alas-para-o-escaner-facial-reconhece-milhoes-e-prende-seis.htm>>.

Thompson, J. B. (2018). *Social Media and the Public Sphere: An interview with John B. Thompson*. Universidad Nacional de Rosario (UNR) y Centro de Investigaciones en Mediatizaciones (CIM), Argentina. jun.

Tomaz, T. da S.(org). (2000). *Identidade e diferença*. Rio de Janeiro: Editora Vozes.

Thiollent, M. J. M. (1982). *Crítica metodológica, investigação social e enquete operária*. 3. ed. São Paulo: Editora Poli.

Van Dijck, J.. (2017). Faces da conectividade: Plataformas, Influência e Usuários. São Paulo: *Parágrafo*, jan/jun, v. 5, n. 1, p. 172-175.

Warren, S. D.; Brandeis, L. D. (1890). Right to privacy. *Harvard Law Review*, v.4, p. 193.

Woodward Jr, J. D. et al. (2003). *Biometrics: A look at facial recognition*. RAND CORP SANTA MONICA CA.

Yang, S. et al. (2018). Faceness-net: Face detection through deep facial part responses. *IEEE transactions on pattern analysis and machine intelligence*, v. 40, n. 8, p. 1845-1859.

Zuckerberg, M.. (2019). A Privacy-Focused Vision for Social Network. *Facebook*, 6 March. 2019. Retrieved March 20th 2019 from: <<https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/>>.