Perspectivas de la Comunicación
UNIVERSIDAD DE LA FRONTERA
ISSN 0718-4867

Article

SMARTPHONES: OPPORTUNITIES AND RISKS

DOI: POR ASIGNAR

Dr. Humberto Ortega-Villaseñor
Universidad de Guadalajara, Guadalajara, México
huorvi@gmail.com
ORCID ID: https://orcid.org/0000-0003-3063-9182

Recibido el 2021-12-17
Revisado el 2022-05-05
Aceptado el 2022-04-10
Publicado el 2022-05-11

Abstract

The article looks at smartphones within the framework the ever-growing integration of digital services being offered to users today. It analyzes their typology, limits and scope, their positive and negative aspects, while taking a closer look at the risks and future consequences involved in setting up a system that generates information and personal data on users and stores them in the device itself as well as on computer platforms (the so-called *clouds*). This intimate information is subject to interpretation by personal-data mining (an advanced field of knowledge that focuses on data extraction, processing, and interpretation). This massive data set represents a source of information that has not been fully exploited to improve public health, facilitate human interaction, and enhance users' learning. On the other hand, different corporations have made use of it for purposes of industrial spying; commercial, political, or ideological surveillance of citizens; or direct interventions to manipulate behavior and control certain segments of the population.

Keywords: smartphone, digital convergence, digital vulnerability, wearables technologies, privacy paradox.

Artículo

TELÉFONOS INTELIGENTES: OPORTUNIDADES Y RIESGOS

Resumen

El artículo aborda el estudio de la llamada telefonía inteligente móvil ubicándola en el marco de la integración creciente de servicios digitales que se ofrecen al usuario de nuestros días. Analiza su tipología, límites y alcances, aspectos positivos y negativos, ahondando en los riesgos y consecuencias a futuro que implica constituir un sistema generador de información y datos personales de los usuarios, que son almacenados en el propio dispositivo y en las plataformas de cómputo (las llamadas *nubes*). Esa información íntima es susceptible de ser interpretada a través de la llamada minería de datos personales (campo de conocimiento avanzado en técnicas específicas de extracción, procesamiento e interpretación de datos). Constituye un acervo o fuente de información que ha sido desaprovechada en muchos casos para mejorar la salud, interacción humana y el aprendizaje de los usuarios. Y, muy por el contrario, ha sido utilizado por diversas corporaciones para prestar servicios de espionaje industrial, vigilancia comercial, vigilancia política o ideológica de la ciudadanía, o de intervención directa para manipular la conducta y mantener el control de consumo de segmentos específicos de la población.

Palabras clave: smartphone, convergencia digital, vulnerabilidad digital, tecnologías wearables, paradoja de la privacidad.

1. Introduction

The latest scientific and technological developments in the fields of satellite communications, electronics, computer systems and telephony; the emergence of numerous internet service providers; the increase in personal data storage capacity, as well as improvements in the capability of informatics programs to obtain data and process them to extract information, give rise to the notion that we have put ourselves in an unprecedented human scenario, one that allows great freedom of movement whether people are static or moving, and that is technologically capable of generating strategies for intercepting information in either of the two cases (*Cfr*. Serra-Cristóbal, 2015).

For this reason, some search engines on the web have had to come up with *privacy policies* to head off any potential suspicion as users come to realize that their data can be used to offer them personalized content and to filter ads based on their interests, tastes, and preferences. This information is obtained from the searches that users make, the videos they look at or the messages they have sent over the internet. In other words, having achieved the ability to perform increasingly sophisticated analyses and measurements of what users look for and communicate on the web, search engines have been forced to assure users of their intention to *protect* the proper use of this information and avoid misappropriation. Under no circumstances is it their intention to control, manipulate, market, or exploit this information.

In this way, even if these information control and compilation systems are reliable overall and less and less selective in terms of targets, the fact is that they carry out monitoring processes that, given the new scenario of possibilities, need to be scrutinized as they can jeopardize our intimacy, our freedom of expression and free access to the information of millions of human beings. Why? Because, as Rosario Serra (2015) states, today “endless amounts of personal data and communications are being collected and the technical capacity is there to evaluate and interpret them. This seems to be occurring on a global scale”. (p. 75)

From this perspective, albeit with a more limited scope, this article focuses exclusively on smartphones as its object of analysis. I have two substantial reasons for this decision: the smartphone is a device that has made a signal contribution to the transformation of communication in today’s world, plus I fear that its future development could lead to more insidious psychic and social conditioning for humankind. There is no denying that the technology allows its *owners* to caress the screen tenderly to communicate with any part of

the planet (ICT), to obtain the information they need or to receive unsolicited information, but it seems to come to know them more and more intimately, and to anticipate their decisions. The technology quickly proves its usefulness, but at the same time, it ensnares and subjugates, becomes overly absorbing and demanding, as it accompanies its owners, who now number in the billions, wherever they go physically and wherever they navigate on the web, day after day. As Ana Luz Ruelas (2010) points out, this device "is undoubtedly one of the artifacts that has attained worldwide popularity" (p. 153).

As Sekara (2021) observes:

> The sensing capabilities of modern-day smartphones, together with our seemingly symbiotic relationship to them, render mobile devices good tools for tracking and studying human behavior. Mobile phones are ubiquitous and have permeated nearly every human society. In 2018 there were 107 mobile-cellular subscriptions per 100 inhabitants, and globally smartphones account for 60 % of all mobile phones. Smartphones have transformed the way people access the internet; today most of the traffic to web pages stems from mobile devices rather than from desktop computers, making advertisers target mobile phones to a higher degree (p. 1).

2. Methodology

The ubiquity of the mobile phone has changed public behavior, altered the concepts of public and private space, human relations, customs, ways of communicating, among other social phenomena (Castro-Rojas, 2012). The author writes:

> The mobile phone modifies individuals' presence and absence in social space, the social configuration of space and time (Fortunati). Distance and place do not disappear, but they are reconceptualized and restructured, leading to a new sense of belonging in our web of relationships. The possibility of connection makes others virtually present. Cell phone users can be near and far at the same time, they can be available at any moment without needing to be present, they can meet across great distances and be connected, i.e., absent but present in a virtual communication space. "Mobile phones have the peculiarity of bestowing a certain degree of presence on those who are absent, of embodying the virtual presence of those whose numbers are on our list of contacts, of those who call us or send SMS messages[1], whose presence can be invoked any time we have our mobile phone with us" (p. 93).

1 Short Message Service, or Simple Message Service, better known as SMS, is a mobile phone service that allows users to send short written messages, "text messages," to other mobile phones.

For this reason, the way to approach such a dynamic and complex object of study must be polyhedral and cross-sectional, since it is almost impossible to confine its study to a specific field, or to the analytical tools afforded by two or three disciplines (such as anthropology, social psychology, communication sciences, etc.). An approach that can systematize effective results depends precisely on this kind of pliability in the research methodology and in the disciplines that can be called upon or brought to bear (medicine, commerce, marketing, advertising, etc.). It is important to keep in mind that the resources offered by mobile devices are extremely varied and touch on multiple aspects of our lives and our individual, family, and social behavior.

Moreover, it must not be overlooked that the mosaic of communications is uneven. While mobile telephone access rose from less than 10 % of the world's population in the year 2000 to over 70 % in 2017, and it was second-generation technology that accounted for most of the overall expansion in mobile telephone access, conditions vary significantly from region to region, and from country to country. For example, in Latin America the consolidation of market penetration higher than 80 % has only been reached among the population of the wealthiest countries, since "there are major access gaps in some countries and quality gaps in terms of 4G coverage and connection speeds throughout the region" (D'Almeida & Margot, 2018).

In all humility, another element to consider and to bring explicitly to the reader's attention is the relative and partial nature of the bibliography that was consulted for this article: it was made up primarily of European, North American, and Latin American authors. Contributions by Asian and African scholars are noticeably lacking, despite the enormous technological strides made in Africa, and the successful commercialization of Chinese cell phones in societies that might seem backward at first glance.

The Finnish researcher Pasi Mäenpää recently stated that "in *mobile culture* one always has one foot in the future [...] Places and times somehow fade away: they are not fixed or planned of time; people simply decide (or act spontaneously, without prior notification). People call 'when they get there'... It thus becomes possible to organize one's day on the fly, in response to whatever happens to occur" (Castro-Rojas, 2012, p. 93).

In this article I set out to address only certain aspects of so-called smart telephony and its consequences for the future (particularly those aspects that relate to the euphemism of

freedom of movement in conditions of political, ideological, and social control). The linking of the topics is therefore quire rigorous, and the methodology used is interdisciplinary. I make every attempt to use accessible language when offering explanatory analyses of technical aspects and nomenclature, to facilitate understanding and effectively gauge their significance for the social sciences and humanities.

3. The importance of context and interpretation

The mobile phone has become an omnipresent medium. It offers the possibility of connecting and being always connected, regardless of the caller and callee's physical location (Höflich & Rössler, 2002). The habitual use of mobile phones confirms what Misa Matsuda calls "full-time intimate community" (quoted by Castells *et al.*, 2006, p. 150). To use Fortunati's formulation, we have turned into snails: "we carry our relational house on our back" (quoted by Castro-Rojas, 2012, p. 93).

This marks a significant difference with respect to previous generations. For example, the so-called generation Z, "which has grown up with videogames and mobile phones, has enhanced certain brain functions having to do with speed and automatic behavior, at the expense of other functions such as reasoning and self-control… The problem concerns health professionals. These practices have a neurological impact comparable to alcohol or cocaine dependency, according to a recent study carried out by a mental health research center in Shanghai that looked at brain data of young *technoaddicts*." In fact, a specialization now exists for getting young people "unhooked" from this digital opium (La Jornada, 2015).

> The dependency is harder to detect with smartphones because you don't have to sit down at a desk (to access a computer). So, it is harder to realize that someone has a problem, explains the psychiatrist Takashi Sumioka. The number of cases that this specialist treated tripled from 2007 to 2013. Sumioka offers patients a digital detox program. He asks them to keep a diary to see how hooked they are on their smartphone and internet connection. They need about six months to kick the habit, he says. This type of obsession is driven by a fear of being left behind, or even harassed in a group if one does not answer messages fast enough, warns Sumioka (La Jornada, 2015, p. 2).

As Howard Rheingold (2004) states, microprocessors, with their versatility and portability, have become "smart intercommunication gadgets" (p. 18), and instruments for broadening and strengthening the technological platform in the networked society, a society whose structure and social practices are being organized around microelectronic information and communication networks. "Mobile communication devices make e-business possible, along

with the mobile office, the mobile worker, and the decentralization of production and management in the business world. They allow a direct connection between public servants and users" (Castro-Rojas, 2012, p. 93). And yet, the picture is not entirely rosy. Dizzying qualitative changes have taken place in terms of the evolution of the mobile device itself, making it imperative to take a careful look at these differences.

3.1. Typology of mobile phones

According to Sebastián Ramiro Castro Rojas, there are currently four categories or models of cell phones: the devices[2] that come with each of them are different. Basic telephones allow voice communication and text messaging and come with low-resolution cameras and a rudimentary capacity to reproduce audio files. The so-called feature phones have the capacity to reproduce MP3 files and come with high-resolution cameras that adjust improve the shots. Social phones have multiple messaging functions, a QWERTY keyboard, or a touchscreen. Without being smartphones, they accept the use of apps such as mail, instant messaging (*Messenger*, *Yahoo*, *WhatsApp*) and different social networks (such as *Facebook* and *Twitter*). And finally, smartphones come with their own operating systems with the capacity to download new apps, enabling the user to carry out a greater variety of tasks than any of the previously mentioned categories of phones (Castro-Rojas, 2012, p. 93).

Smartphones bring together or epitomize the notions of device, because:

> When we talk about convergence, we mean that a mobile device enables us to make voice calls, send text messages, integrate other press media including video, cinema, TV, Internet, audio, and a wide range of services such as mail, advertising, market information, bank transactions, data management, electronic leisure, weather, and traffic updates. The mobile phone is characterized by the convergent integration of formats and services, i.e., it is a digital communication and access meta device (Aguado & Martinez, 2009, p. 319).

2 Technological devices do not encompass only the physical, tangible, malleable apparatus that makes it possible to establish the communications link; they also entail other symbolic representations that make themselves present. Following Foucault's lead, "The device is actually the network that is established among all of these elements" (23). Moreover, "the device is anything that somehow has the capacity to capture, orient, determine, intercept, model, control and assure gestures, behaviors, opinions and discourses, navigation, computers, cell phones, and why not? language itself, which is perhaps the oldest device of all" (Castro Rojas, 2012, p. 94).

Full digital convergence assumes access to information in real time and the possibility of intercommunication wherever individuals happen to be, by way of text messages, graphics, videos, or audio. In Castro's words, "mobile devices have permeated the social fabric, with technology that cuts across all sociocultural segments" (Castro-Rojas, 2012, p. 94). For this reason, they have become a meta device, conquering users with different characteristics but with a manifest objective of communicating among themselves. This has radically increased forms of interaction, and therefore, of resistance. As Rheingold (2004) says, "the beneficial effects also involve pernicious consequences" (p. 24). As we will see, smartphones can be used as artifacts for control, which explains why systems engineering, for example, is one of the scientific-technological areas that have made the greatest effort to diversify the uses of smartphones and portable devices.

3.2. The smartphone as an information generator

It is important now to start with a careful literature review of the state of the art of this field of knowledge, and with a taxonomic description of basic principles and mechanisms, plus a review of performance assessment criteria and empirical evidence of this kind of device (Habib-ur-Rehman *et al.*, 2015, p. 4430).

Skyrocketing use of smartphones has given rise to the generation of user-specific personal data on a massive scale. What does this mean? According to Muhammad Habib-ur-Rehman *et al.* (2015), at the global level billions of user-specific data points are produced by the personal sensing devices (PSDs) installed in portable devices, particularly smartphones, known in the jargon of systems engineering as remote-control systems (RCSs).

This is information that can be handled, interpreted, and processed, and according to the *MIT Technology Review* 99.5 per cent of this information *goes to waste*, i.e., has yet to be analyzed, even though in recent years enormous technical and methodological advances have been made that enable people to study and handle them effectively. In other words, the tools are there to *exploit* this personal data mining (PerDM). Personal data mining (PerDM) (a.k.a. Personal Analytics and Quantified-Self) is a relatively new concept that is based on data mining techniques used for mining the personal data of users to fulfill their personal needs.

From this perspective, as Muhammad Habib-ur-Rehman *et al.* (2015), put it,

> Technological advances in smart telephony represent an opportunity to quantify every second of human life, allowing the information obtained through the analysis of our bodies' data and our day-to-day activities to be exploited by means of data-mining algorithms to discover hidden patterns of knowledge that can be derived from frequent activities, the classification of physiological data, and patterns of users' movements and mobile trajectories (p. 4431).

The potential released by the emergence of PerDM is a double-edged sword in much as it seeks to maximize the benefits obtained from personal data to create healthy, well-managed (*sic*) lifestyles, while respecting privacy and data security. And yet, while we see rapid growth in data-mining technologies and algorithms, as evidenced by Kevin Kelly's self-quantified movement and Stephen Wolfram's personal analysis (Choe *et al.*, 2014, p. 1143), at the same time serious concerns have arisen regarding the preservation of privacy and security, given the public nature of users' personal data on different search sites and trajectories.

At present, computer power and memory volume continue to expand, which suggests that PerDM will become more accessible and manageable and will certainly command the attention of researchers before long. As Vedran Sekara *et al.* (2021) points out:

> Tracking behavior is a fundamental part of the big-data economy, allowing companies and organizations to segment, profile and understand their users in increasingly greater detail. Modeling context and interests of users has proven to have various commercial advantages: products can be designed to better fit customer needs; content can be adapted; and advertising can be made more relevant. Efficient user modeling requires the collection of large-scale datasets of human behavior, which has led to a growing proportion of human activities to be recorded and stored. Today, most of our interactions with computers are stored in a database, whether it is an e-mail, phone call, credit-card transaction, Facebook like, or online search, and the rate of information growth is expected to accelerate even further in the future. These rich digital traces can be compiled into detailed representations of human behavior and can revolutionize how we organize our societies, fight diseases, and perform research; however, they also raise serious privacy concerns (p. 1).

These developments have led many countries to legislate the use of such data.

4. Discussion

If we take an overall perspective, we can see that a body of norms has been developed to regulate public transparency and the right of access to information. These legal ordinances are often not binding on States, but they have been developed over time and are based on the recognition of access to public information as a fundamental human right. To cite but of

few of them, there is the Universal Declaration of Human Rights of 1948: article 19 states that "Everyone has the right to freedom of opinion and expression; this right includes freedom 56 to hold opinions without interference and to seek, receive and impart information and ideas." Other documents set forth rights along these same lines: the International Covenant on Civil and Political Rights (article 19), the American Declaration of the Rights and Duties of Man of 1948, the American Convention on Human Rights of 1969 (article 13), the Inter American Declaration of Principles on Freedom of Expression of the year 2000, among others.

The General Assembly of the United Nations has also issued a number of instruments and resolutions, for example, the Resolution on Access to Public Information and the Protection of Personal Information AG/RES. 2661 (XLI-O/11) or the Model Inter-American Law on Access to Public Information of 2010, which ruled that "access to information is a fundamental human right and an essential condition for all democratic societies" and that "right of access to information applies broadly to all information in possession of public authorities, including all information which is held or recorded in any format or medium" (apud. Palomares-Herrera, 2017, pp. 133-135).

However, the reception or transfer of this legal framework to the legislation of the different States is not as simple as it seems. It depends on the complexity of the constitutional legislative norms and procedures of each legal system. For this reason, it could be argued that there are not enough norms at the regional level (in Europe, Asia, Africa, or Latin America) or in national legal statutes to sufficiently safeguard or protect privacy in the handling of users' data, even more so if we consider the dynamism of technological changes and the dizzying emergence of new apps, especially when it comes to smart phones. As Palomares-Herrera (2017) rightly points out:

> If at the end of the 20th century there were only thirteen countries that had such a Law, now there are over eighty, and close to twenty are in the process of formulating and approving one. Nevertheless, mention must also be made of countries that show the other side of the coin, such as the Moorish countries or India, which although it has had a law since 2005 with very detailed mechanisms for guaranteeing transparency, in practice it gives evidence of a very different reality because many people have been killed for defending this law. This global mainstreaming trend of approving norms to guarantee access to public information got its start in the Scandinavian countries (p. 125).

With respect to Ibero-America, Catalina Ruiz-Rico (2019) considers that its legislation "ratifies its category as a fundamental right for all constitutional effects (guarantees). Among others, there is Mexico's General Law for Transparency and Access to Public Information, promulgated on May 4, 2015, which asserts that it is a question of constitutional development and public order (article 1)".

Of course, within this mosaic, mobile phone companies and manufacturers take a somewhat divergent stance, suggesting that

For a data privacy law to be successful, it must effectively protect people and, at the same time, give organizations the freedom to operate, innovate and fulfill the regulatory framework in a way that is reasonable for their business while ensuring positive results for society. The law should be governed by principles that assign the responsibility for identifying and mitigating risks to the organizations, maintaining flexibility and neutrality with respect to technologies and sectors, and allowing data to circulate across borders easily. (GSMA, 2019, p. 3)

4.1. Facilities and limitations

Computer, communication, and storage resources that are available to users in smartphones aim to create a system known as the personal ecosystem. There, personal sensing devices (PSDs) are attached to the system. And they are not only growing more and more ingenious and smart, but they also provide a host of API applications to maximize the efficiency of the integrated sensors and the data from the resident device (Habib-ur-Rehman *et al.*, 2015).

This provides a constant source of information generated by the incorporated sensors, the user's interaction instruments, and the presence of mechanisms or tools already embedded in the mobile device (or that can be downloaded or incorporated later).

The spectrum is quite wide. Some devices have physiological sensors that monitor the user's pulse rate, blood-sugar levels, and physical activity (if the device has an accelerometer). Other sensors measure environmental factors: temperature, humidity, and atmospheric pressure. Others are for navigation—GPS locators, compasses, and movement recorders. As a rule, smartphones also have intercommunication tools for working with text, visual and audio data (such as keyboards, microphones, and cameras for sending text, audio and pictures or video), as well as integrated software to facilitate communication (integrated

search engines, *Google*, *Yahoo*, etc., *scanner, Bluetooth* and *Wi-Fi*, call trackers, contact lists and SMS data (Habib-ur-Rehman *et al.*, 2015).

Even though smartphones include these functional features, when it comes to mobility, real-time data processing, and continuous monitoring and recording of the user's activities, as Muhammed Habib-ur-Rehman *et al.* (2015) point out, "they still have technological restrictions in terms of computing power, energy consumption, memory capacity and screen size, despite the huge growth in micro and nanotechnologies. Likewise, storage capacity and bandwidth continue to represent limitations on PSDs". (p. 4433)

Nevertheless, personal sensing devices (PSDs) are being seen as high-priority research objectives in order not only to overcome the above-mentioned technological limitations, but also to set the direction of future development of data processing systems, given their transcendence in terms of the information they generate. They can play a key role for corporations and public agencies by enabling the detection of hidden patterns in users' daily activities and specific information. One of the main goals of the study done by Muhammad Habib ur Rehman *et al.* is to identify opportunities for maximizing the social benefits pursued by certain public agencies[3] (Habib-ur-Rehman *et al.*, 2015).

Smartphone users' trend younger and younger, and intercommunication options have varied greatly in recent years. The impact of Instagram on social networks serves as an illustrative example.

3 Although these researchers make no mention of the dangers implied in the development and proliferation of smartphones and their embedded personal sensing devices (PSDs), they conclude their study in the following terms: "with a focus on users, the personalization of big data is a concept that offers a wide range of applications for health care, tourism, education, electronic government and smart cities, among others. It has huge personalization potential to offer better attention for patients, travelers, customers, students and citizens. For example, in the case of personalized medicine, the idea is to provide the right treatment at the exact dose, and the right medicine the moment it is needed. Therefore, the success of personalized medicine depends on accurate diagnoses leading to directed treatments. PerDM in RCEs shows great potential for taking advantage of these opportunities by monitoring users' physiology and diagnosing irregularities in patients' daily indicators. The combination of personal data from PSD-based systems and big health data creates the opportunity to personalize large sets of patient-centered data gathered on devices or tools that these patients use (Muhammad Habib ur Rehman et al., 2015: 4461).

> This is a social network that has evolved tremendously since its creation in 2011. It started out as an alternative app for sharing and editing photos but has morphed into a more "visual" or "artistic" social network than Facebook or Twitter, becoming a 'monster' that has effectively mediatized what used to be considered people's 'private life.' Today it serves to tell the world what you're having for breakfast and where, how you exercise, how you dress, how you comb your hair, what you drank at the bar last night, what your spiritual beliefs are and what yoga studio you frequent… All within a framework of creating a concept of your life and showing it off to others by way of visual elements. This is the logic behind the influencers who look for ways to 'sell' this concept of their life and get big companies to sponsor them to push the corporations' products in virtual show windows. Some influencers earn millions from fashion brands (like Chiara Ferragni, o Kim Kardashian). Gamers do the same on platforms like Youtube, inspiring younger generations by simply playing videogames and recording themselves as they provide commentary; for this they earn thousands of dollars in Youtube royalties based on the number of views they attract (El Rubius, Vegeta 777) (Galindo, 2021, p. 2).

4.2. How sensors and PSDs work

Unlocking the information that can be obtained from personal sensing devices (PSDs) inserted in smartphones is very simple. It is called the knowledge discovery process (KDP) and includes three basic stages: **1.** pre-processing of data; **2.** application of algorithm mining to the data stream to discover hidden patterns; and detection or identification of interesting orderly knowledge patterns after evaluating these patterns.

In the first step, the pre-processing tasks include strategies for merging and channeling data, locating atypical values, detecting anomalies, reducing the dimension of the information, along with extraction techniques. In the second step, data or data-flow mining algorithms are applied to the pre-processed data to obtain knowledge patterns by classifying, grouping, and obtaining frequency patterns. The choice between data mining and data-flow mining depends solely on the requirements of the application and the need to analyze the data online (dataflow) or offline (data mining). Finally, in the third step, the discovered patterns are evaluated with different measurements depending on the degrees of interest and the decision of which patterns to store and which to discard (Habib-ur-Rehman *et al.*, 2015).

Next comes the knowledge management… These knowledge patterns are added, summarized, and integrated for later use. Then, these data sets are sent to local storage, i.e., to storage spaces in the smartphone itself and/or to extractable SD cards that are normally used in PSDs for local storage. In the event of insufficient local storage space, the data sets are sent to external environments for their permanent storage. These external environments

include remote data processing systems in clouds, matrices or on the internet (Habib-ur-Rehman *et al.*, 2015).

The application of data mining and automated machine-learning techniques are relatively new fields in PSDs that focus specifically on user personalization. Some recent examples of personalized public-health technologies can be found in activity recognition and smartphone-based systems (Kranz *et al.*, 2013; See also Asif & Krogstie, 2013, p. 1)[4]. As far as we know, however, there is no significant scientific research being conducted to effectively and collectively protect or cover privacy, security and the personalization of the large information flows that run in a generalized environment. Exploration of this area of research thus takes on a certain urgency. As Habib-ur-Rehman *et al.* (2015) put it, "the rapid development of PerDM algorithms and users' adoption of fine-grade PSDs are key pieces of

4 Great care has been taken with the evaluation of user-personalized devices. According to a study by M. Asif and J. Krogstie (2013), the overall effectiveness of user-centered personalization on PSDs is based on 10 constructs: 1. User satisfaction, i.e., the strong connection between user satisfaction and user intention with regard to PSD use. Thus, an effective personalization strategy can increase user satisfaction. 2. Perception of the information load: The overwhelming amount of data makes the information load on PSDs excessive, causing dissatisfaction and reluctance to use them. Personalized services based on pertinent information can reduce the information load and increase overall PSD use. 3. Perception of relevance and accuracy: Personalization based on user profiles and contextual information can help to present relevant and accurate information. Relevance and accuracy, therefore, relate directly to the system's overall effectiveness. 4. Perceived effort: The amount of effort needed to make use of personalized content is directly associated with user satisfaction, because any increment in the labor required to explore relevant results reduces the overall effectiveness of PSDs. 5. Perception of security and privacy: The availability of personal information, such as financial and health data, the requirements of a high-security system that protects privacy. Thus, privacy and security affect user satisfaction. 6. User's perception of control: The sensitivity of personal data and the need for personalization are the key factors that cause users to lose control of their personal information. Therefore, personalized systems that provide users with sufficient control over their personal information improve user satisfaction in general. 7. Perceived reliability: Users produce and exchange different kinds of information. An effective mechanism from the service provider for acquiring, processing, storing and sharing users' personal information improves users' confidence in personalized systems. 8. Perception of goal attainment: Personalized systems are needed to meet users' functional and entertainment needs. Goal attainment is directly linked to users' satisfaction and to their intention to use personalized systems in the future. 9. Perceived adaptability of the device: Personalized systems should be able to adapt to users' preferences in multi-PSD environments. Users' interaction with each device should provide the same level of service. The device's adaptation capability thus directly affects user satisfaction. 10. Perceived overall effectiveness: The main construct of personalized systems is to measure overall effectiveness in improving productivity, attaining goals quickly, and improving users' efficiency in general. Overall efficiency encompasses a system's ease of use, level of personalization and effectiveness. (See Asif & Krogstie, 2013, p. 1).

evidence justifying the proposal of a hypothesis for personalizing big-data ecosystems privately, securely and profitably" (p. 4459). (*See* also Wiese et al., 2017, p. 447–510).

4.3. Positive aspects

Before continuing, allow me to touch on certain positive and negative aspects of mobile phones that respected researchers have identified. Beginning with the positive aspects, below are the generic observations of Juan Miguel Aguado and Inmaculada Martínez:

The mobile phone has permeated the social fabric in unexpected ways, becoming a highly personal object: mobile devices accompany people wherever they go. There is an unbreakable bond between the telephone and its owner. Bearing in mind the evolution of the device together with the progress made in the technological standards governing digital networks, we can recognize the mobile phone as the epitome of digital convergence. The mobile phone is a device that encompasses other digital devices: a single terminal hosts a wide array of applications, functions and services that enable users to undertake multiple tasks (2009, p. 158).

As Ruelas (2010) puts it, it is evident on the one hand that the cell phone has acquired a privileged status for individuals, not just because of "the immanence of its change of status… in a novel format that has conferred greater visibility on technology: the enormous growth in the number of users –adults, young people and children—both high and low-income," but also because "culture is more and more influenced by the enhancement of sophisticated information and communication technologies that expand a person's capabilities" (p. 153).

What advantages have smartphones and social mobile devices brought to the collective dimension of societies and to education? Howard Rheingold (2004) had predicted it as early as 2004: "the mobile 'smart multitudes' are emerging, not from institutional elites but from the peripheral practices of amateurs who decide to change their way of socializing, of working, of 'buying, selling, governing and creating'" (p. 19).

According to Tu *et al.*, (2012), researchers from Arizona State and Northern Arizona Universities, mobile learning environments are human networks that offer the chance to participate in joint creative undertakings, in the construction of social networks, in protests, in the organization and reorganization of social content, and in the call for social actions anywhere and at any time, by way of mobile technologies.

These are social acts that nourish identities, raise awareness, ensure connections, and promote interactions that are necessary for resistance and for shared interactive learning. The study done by these researchers aims at looking deeper into mobile social presence, analyzing how it impacts social interaction and how it relates to online and networked social presences.

Mobile social presence is defined as the degree of enriching social context-awareness; managing location-based communication, personalized multi-layered interactivity, and optimized digital and social identities to other intellectuals through digital mobile technologies (Tu, *et al.*, 2012, p. 247). [...] Mobile technology as an emerging technology holds promise to enhance human interaction and learning. Mobile technology may be instant on, ubiquitous, convenient, easy, fast, and powerful; however, if we take mobile technology to replicate what we interact, mobile interaction would be always a second best to FTF interaction. It would be just like using a computer as a typewriter or using mobile devices to respond to email as our convenience. In such a case, the emerging technology may well become inferior in comparing it to the traditional ones (Tu *et al.*, 2012, p. 260).

These researchers reach the conclusion that mobile social presence somehow resembles virtual social presence, and yet it differs from online and networked social presences in the aspects of personalized control and free-access digital interaction (Tu *et al.,* 2012). Consider, for example, the role played by social networks (*Facebook* and *Instagram* primarily) as promotion-facilitating platforms for commerce between individuals. Then there are the sites for the large-scale purchase-sale of products, such as *Amazon* or *Mercado Libre*, which have seen dizzying growth since the start of the pandemic in March 2020 and throughout 2021. These sites let users make purchases without having any contact with other people, and the products are delivered to their door.

The use of algorithms to determine the advertising that appears on the sites that users visit is directly linked to products sold online, and these are selected to appear in ads as a function of each user's profile as a potential buyer. This constitutes an invasion of users' privacy with respect to the websites they visit, the places they go (their smartphone tracks them via GPS) or even the things they say (by way of the smartphone's activated microphone and the programs that operate with it, whether the user wants to use them or not, such as Siri and Alexa). We should not overlook the fact that thanks to this boom, the founder and owner of *Amazon*, Jeff Bezos, has amassed one the largest fortunes in the world.

One example is the augmented reality system as a mobile app. (*See* the interesting analysis by Vida Davidavičienė, *et al.* (2021).

4.4. Negative aspects

With respect to negative aspects, Virginie Bueno points to smartphones and the time wasted on internet communication and contends that more and more people are clearly having trouble disconnecting.

Their online activities gradually infiltrate their lives at the expense of their sociability, their work, and their studies. But, she wonders, when does this dependency cross the line into disease? She avers that the scientific community has been unable to reach a consensus about whether such dependency can be called pathological or not. "In 2008 internet dependency disorder was excluded from the fifth edition of the American Psychiatry Association's diagnoses and from the Diagnostic and Statistical Manual of Mental Disorders (DSM) for lack of convincing evidence." The debate, however, continues, and the World Health Organization has yet to decide whether it will include this obsession in the 2017 edition of the International Classification of Diseases.

If we limit our consideration of addiction to strictly neuroscientific terms, we unnecessarily constrict the scope of research and possible solutions. So far excessive use has been discussed in social, cultural, and political terms, but there is no international consensus about the phenomenon. The United States and China, for example, accept the possibility that this kind of dependency is a neurological disease, but they differ as to the best way to treat it. The US has set up a competitive private system that depends on insurance companies, while China has opened military-style training camps where patients who "acknowledge their disease" are confined. France and Canada (Quebec) for their part favor a holistic psycho-social approach and case-by-case assessment. Japan has begun to finance treatment centers, recognizing the potential scope of this particular "social problem" (Bueno, 2015).

As for mobile phones, Lin *et al.* (2015) argue that they have become the leading communication device as cellular mobile telephony has reached 96 % of the population (International Telecommunication Union, 2014). People consciously use mobile phones with varying levels of dependency (Carbonell *et al.*, 2013), and users to a great extent display disparate pathological symptoms of mobile phone addiction and maladaptive behavior.

Instead of railing against mobile phone addiction, T.C. Lin *et al.* looked at dependency as a continuum, defining it as a relationship in which individuals attain goals such as social connectivity through confident use of mobile devices (Lin *et al.*, 2015).

Despite the social alarm caused by the fact that young people are prone to losing self-control in their use of smartphones (Igarashi *et al.*, 2008; Leung, 2007), little research has been done into these users' actual dependency on this type of mobile device. It is quite likely that users' attachment to their smartphone will increase as its functions multiply. This leads us to believe that it makes sense to compare smartphones with phones that are not smart to understand the symptoms that signal dependency in each case. Filling this research gap, the study by Trisha T. C. Lin, *et.al.* mentioned earlier looked at the differences between symptoms of dependency on smartphones and ordinary mobile phones, as well as their relationship with the phenomenon of sociability and mobile dependency (Lin *et al.*, 2015).

The researchers used a stratified sampling method to recruit 551 university students in Singapore. The results showed that young smartphone users tended to experience greater dependency and display more alarming symptoms than users of non-smart cell phones. "We found that utilizing mobile Internet and text messaging were both positively associated with smartphone users' dependency. Regardless of phone type used, the level of sociability of mobile phone users was positively associated with mobile dependency and symptoms of feeling anxious and lost, and withdrawal/escape" (Lin *et al.*, 2015, p. 1209). The combination of these elements leads these same researchers to warn the following:

> This indicates an urgent need to increase young people's awareness of overdependence on smartphone activities. The results showed that mobile dependency symptoms were associated with phone activities. Regardless of phone type, using mobile Internet was positively related to all four mobile dependency symptoms (i.e., inability to control craving, feeling anxious and lost, withdrawal/escape, and productivity loss.) (Lin *et al.*, 2015, p. 1213).

Addiction to SMS (Igarashi *et al.*, 2008; Perry & Lee, 2007) and MIM (Hong *et al.*, 2012; Sultan, 2014) among young people resulted from excessive use of these cheap or free connectivity features. Moreover, the results revealed that smartphone users who use SMS and mobile internet tend to develop greater dependency on their mobile device, while these same activities on non-smart phones did not have a significant impact on mobile dependency among their users (Lin *et al.*, 2015).

Nevertheless, as the study by Ubaldo Cuesta Cambra *et al.* (2020) of the Universidad Complutense de Madrid points out:

> The smartphone is seen as an attractive tool that facilitates socialization and communication, even as certain drawbacks are recognized, such as lack of privacy, changes in the forms of social relations, isolation, and deterioration in social relations. Young people are aware that the phone's accessibility and availability has made it a device that they use every day, even in settings where its use is prohibited; they acknowledge their own anxiety at the prospect of not being able to use it. This attitude is also recognized by their parents, but they do not see this as a problem, which shows that it has become normalized. This only underscores the importance of the role played by both parents and educators in getting young people to make healthy use of their phones, although there are certain challenges given the gap in familiarity and use strategies between adults and young people, as our results from the group discussions and in-depth interviews have shown (p. 376).

4.5. Anonymous surveillance

It is noteworthy that in all these research reports, there is no study about the relationship between mobile phones and mechanisms of social control, normalization, and resistance. According to Felipe Corredor, Francisco Tirado and Lupicinio Íñiguez (2010), these aspects "point in a different direction from the overly optimistic or catastrophic positions, toward an understanding of the mobile phone as a hybrid, assembled entity that like any other everyday technology is capable of redefining the functioning of our immediate social setting". (p. 61)

Nevertheless, in the words of David Talbot (2014), a researcher from Harvard University, "the documents released a few years back by E. Snowden, former contractor with the U.S. National Security Agency, indicate that this agency is capable of collecting enormous amounts of information from data-storage computer platforms (the so-called *clouds*, as they are known in popular language), as well as from wireless telephony service providers and the calls that ordinary people make and receive" (p. 35). This same researcher suggests that

> It's not only the government that might be watching you; it's also certain websites, advertisers, marketers and even retailers who try to follow your movements in stores. Modern smartphones, and the apps that run on them, are designed to gather and disseminate huge amounts of data, such as the user's location, her navigation history and routes on the web, the contents and terms of her searches, and her list of contacts. (Talbot, 2014, p. 35)

This shows that the so-called *black phones*, which are sold in the United States for about 629 dollars (with subscriptions to privacy-protection services included), represent just one of the many measures taken by specialized technicians to protect data privacy. One of these efforts entails a higher level of encryption of the traffic or navigation route that a user undertakes on ordinary websites. Stephen Farrell, a computer scientist at Trinity College in Dublin who heads up the Internet Engineering Task Force that seeks to devise impenetrable mobile phones, states that "a telephone that encrypts communication and stanches data leaks is a crucial part of the strategy". (Quoted by Talbot, 2014, p. 35)

> When I joined the group and learned more about mobile phones, I realized how digitally naked I was. I took a look at my new iPhone 5S. I opened the *Wi-Fi* settings and saw different networks available, with names like *Barcelona*, *Wi-Fi*, *Cbarc 1*, *Spyder*, among others. Their reliability was unknown to me, but that didn't matter. After all, I wasn't connected to any of them. However, it turns out that my telephone's automatic search for these signals meant that it was notifying different routers of my telephone's ID. That's when I understood just how that information was being exploited by those retailers who use *Wi-Fi* signals to track customers' habits. And since the information from apps is combined with data from web navigators, shopping sites and other sources, dozens of companies could use that ID number to keep an eye on me (Stephen Farrell, quoted by Talbot, 2014, p. 35)

It recently came to light that in Mexico the State acquired a nationwide communication tapping system from an Italian company registered as Hacking Team, which since it was founded in 2003 has perfected spying technology and skills using Remote Control Systems (RCSs). "With their latest version –Galileo- customers can even infect an 'objective' by bugging it with an 'agent' that extracts data from the machine under orders from its operators. According to an internal company document, a package of 10 'agents' costs 50 thousand euros. A 200- 'agent' package can be had for 400 thousand euros" (Carrasco-Araizaga & Tourliere, 2015, p. 9).

> From a cellphone it can harvest data from *WhatsApp* and other chat systems, call registers, the agenda, e-mails and messages, passwords, geographic location, and the same as with computers, it can take control of the camera and microphone. And not only that: the program's semi-intelligence allows the operator to activate certain functions according to pre-defined factors. For instance, it can turn on the microphone every time the "objective" enters a certain area or register each phone call instantaneously. It can also sound out the interactions that the "objective" has with other people through his social network sites, his use of his cell phone or the places he visits (Carrasco-Araizaga & Tourliere, 2017).

Citizen Lab, a part of the Munsk School of Global Affairs at the University of Toronto, published a wide-ranging technical research study that blows the whistle on 21 government-customers of Hacking Team (including Mexico's government) (*Cfr*. Tourliere, 2015).

The Italian thinker Gianni Vattimo, a philosopher of post-modernism and professor of Aesthetics at the University of Turin, believes that we should not be the least bit surprised because today market freedom is more of an enemy than a value. The British sociologists Vian Bakir *et al.* (2019) stake out a similar position, arguing that organized persuasive communication is essential today for exercising power at the national and worldwide levels not only in the political context but also in public relations, advertising, and propaganda (p. 311).

In today's world, which is rushing headlong into integration and where there are formidable international controls, communications are routinely intercepted. "That is the direction technology is going in; it requires a disciplined, communicating, intercepted world, where authorities know everything… Under conservative European governments capitalist control over labor has grown; consequently, trade-union rights have been withering. And things will not change until there is a social reaction, political resistance –naturally from the left- that is not oriented and dominated by the design of economic development" (Vattimo, quoted by Amador, 2015, p. 64-65).

The study done by the Scandinavian researchers Sekara *et al.* (2021) shows the capacity for identification that the fingerprints from the cell phones of millions of inhabitants have provided to transnational information storage systems. "Smartphone behavior is different from credit card traces and mobility data due to the ease and scale with which behavioral data can be collected, as any app can request permission to access your app history. The economic imperative and the ease of collecting and trading this data at global scale without the users' knowledge raises serious concerns, especially since this practice has been demonstrated to be in violation of users' expectations and knowledge" (Sekara *et al.* 2021, p. 6)

On this note, Rheingold (2004) had long ago called for conscious reflection on the upcoming new stage in the refinement of social networks by smart phones. As these virtual, social, and physical worlds begin to converge and mix, the "espionage machinery" grows apace, with panoptical social implications that point simultaneously to a new social reordering of

existence that begins to take shape (p. 25) […], risks that entail the loss of privacy within this immense spider web being woven around us (p. 27). At the same time, it should be noted that when it comes to privacy, the internet produces a very peculiar paradox, as Sarabia Sánchez *et al.* (2021) explain:

> The privacy paradox expresses the contradiction implicit in the fact that users value their privacy highly, but at the same time they are willing to surrender it in exchange for trifles (2021, p. 7). […] One possible explanation is that emotional barriers to opting out (isolation, the costs of starting up on a new network, loss of popularity, the need to learn a new application or to make oneself known) generate 'captive' users of apps and social networks. This captivity is a psychological anchor that, in line with the ideas proposed by Fox and Moreland (2015), can induce users to remain active on social networks due to social pressure. In other words, remaining on a social network or using an app could be motivated more by a psychosocial dependence than by the user's autonomous, conscious, and free decision. (p. 8)

Another explanation could be what Edgar Galindo calls "the tendency to the merely digital," which points to a high degree of dependence on the mobile device when the user requires any of the data. (See the study by the Italian researchers Gregorio Serra, Lucia Lo Scalzo, Mario Giuffrè, Pietro Ferrara and Giovanni Corsello (2021)).

> The pandemic has been the main factor that has driven us to move our activities to digital devices such as smartphones. Online classes or virtual meetings are especially notorious aspects. Nevertheless, other factors such as finance have followed this trend. The new plastic cards that banks are issuing to their account holders no longer indicate any information (not even the card number), on the premise of protecting the accounts from fraud or identity theft; this information has been moved to smartphone apps, which makes it impossible to consult the information except through the bank's app. Add to this the fact that the information—card number, CVV—is no longer fixed, but changes every few minutes to keep it from being used again for these crimes (Galindo, 2021, p. 1).

For her part, the Harvard professor Shoshana Zuboff (2019) highlights the limitations and futility implicit in any effort to try to regulate things with legal instruments. She observes, with a certain degree of sarcasm:

> In our time, surveillance capitalism repeats capitalism's "original sin" of primitive accumulation. It revives Karl Marx's old image of capitalism as a vampire that feeds on labor, but with an unexpected turn. Instead of claiming work (or land, or wealth) for the market dynamic as industrial capitalism once did, surveillance capitalism audaciously lays claim to private experience for translation into fungible commodities that are rapidly swept up into the exhilarating life of the market. Invented at Google and elaborated at Facebook in the online milieu of targeted advertising, surveillance capitalism embodies a new logic of accumulation. Like an invasive species with no natural predators, its financial prowess

> quickly overwhelmed the networked sphere, grossly disfiguring the earlier dream of digital technology as an empowering and emancipatory force. Surveillance capitalism can no longer be identified with individual companies or even with the behemoth information sector. This mutation quickly spread from Silicon Valley to every economic sector, as its success birthed a burgeoning surveillance-based economic order that now extends across a vast and varied range of products and services. (Zuboff, 2019)

5. Conclusions

As we have seen, smartphones are physical, tangible, and malleable devices that not only enable users to establish communicative connections; they also produce a digital convergence that offers access to information in real time as well as the possibility of intercommunication among individuals. The enormous growth in the use of these cell phones has given rise to an avalanche of personal data from each user that are susceptible to being collected and stored on computer platforms (the so-called *clouds*) and later studied, systemized, or exploited for a variety of purposes by the users themselves or other industrial, commercial, or political agents, using the process known as personal data mining (PerDM).

Personal metadata— digital information about users' whereabouts and movements, phone call registers, web searches– undoubtedly constitute today the engine that drives intensive scientific inquiry (personal data mining) and studies of the online economy.

High-dimension metadata allow different applications to provide users with smart services and personalized experiences. From Google searches to Netflix, from Pandora to Amazon, metadata are used by commercial algorithms to help users connect better, be more productive, and find a surfeit of ways to entertain themselves. There are scientific fields in which high-dimension metadata are used to quantify, for example, the impact of human mobility on the spread of malaria or the relationship between social isolation and economic development (Montjoye *et al.*, 2014). Furthermore, as we have seen, metadata are used for all manner of political purposes, to control, repress or spy on political enemies in the name of State security or corporate profits.

As Muhammad Habib ur Rehman states, as far as we know, no practical user data personalization system has yet been created that is based on personal sensing devices (PSDs) on smartphones. He therefore suggests that it would be plausible and ideal to move personal data mining services from personal ecosystems (PEs) toward large, personalized data systems that safeguard privacy and offer a high level of security. This wish can be achieved

by improving the processing capacity of current PerDM systems, focusing on data mining execution models and algorithms (Habib-ur-Rehman *et al.*, 2015).

> The execution model can be optimized for cost and computation reduction by enabling maximum data processing inside PSDs and extending it to cloud-enabled data mining systems. Similarly, data mining algorithms should be designed to be scalable from small-scale, lightweight computations inside PSDs to computer-intensive tasks in cloud environments. Another important aspect is the enablement of privacy-preserving and personalized data processing in integrated processing modes to fully leverage heterogeneous computing devices uniformly. (Habib-ur-Rehman *et al.,* 2015, p. 4461)

It is important that we become aware of the enormous potential that metadata offer. These are data that are collected and stored by hundreds of different services and companies today. This fragmentation means that metadata are often inaccessible to innovators, researchers, even to the person who generated them in the first place. On the one hand, individuals' lack of control over their own metadata is fueling suspicions, and makes it difficult, if not impossible, for people to grasp and manage the risks involved. On the other hand, privacy and inherent legal concerns inhibit the possibility of checking or reconciling metadata. In fact, they keep them from being widely available, primarily due to concerns about the risk of re-identification (Montjoye *et al.*, 2014).

Montjoye *et al.* (2014) from MIT and Harvard present a hopeful option that they call *openPDS* and *SafeAnswers,* which lets users compile, store, and give third parties detailed access to its metadata, protecting the privacy of the metadata by way of a system of questions and answers. (p. 1)

Despite this latest initiative, I share the asseverations of Gianni Vattimo and the MIT researchers. My perspective is one of resistance and non-support for the direction taken by research that uses metadata generated by smartphones today from the censors and apparently innocuous services that they offer. In other words, I do not agree that we should simply resign ourselves to an inevitable future of constant surveillance, wiretaps, and international corporate control as the only road to fulfillment.

Nonetheless, we have seen how the system itself has generated a privacy paradox, which has led some researchers to propose the possibility of a user-centered open innovation paradigm that would avoid manipulation as far as possible.

Financiamiento
Esta investigación no recibió financiamiento externo.

Conflicto de interés
El autor declara que no existe conflicto de interés.

Referencias Bibliográficas

AGUADO, J. M. & MARTÍNEZ, I. (2009). De la Web social al Móvil 2.0; el paradigma 2.0 en el proceso. *El profesional de la información, 18*(2), pp. 155-161. https://doi.org/10.3145/epi.2009.mar.05

AMADOR, J. (2015, OCTOBER 4). El mundo será socialista o no será: Gianni Vattimo. *Proceso*. https://publicacionesdigitales.proceso.com.mx/publication/index.html?title=proceso-2031

ASIF, M. & KROGSTIE, J. (2013, JUNE 24-27). *Mobile client-side personalization* [Conference session]. 2013 International Conference on Privacy and Security in Mobile Systems (PRISMS). United States. DOI: 10.1109/PRISMS.2013.6927183.

BAKIR, V., HERRING, E., MILLER, D., & ROBINSON, P. (2019). Organized Persuasive Communication: A new conceptual framework for research on public relations, propaganda, and promotional culture. *Critical Sociology*, *45*(3), pp. 311-328. https://doi.org/10.1177/0896920518764586

BUENO, V. (2015, JULY). Only Disconnect. *Le Monde Diplomatique*. https://mondediplo.com/2015/07/16disconnect

CARBONELL, X., OBERST, U., & BERANUY, M. (2013). The cell phone in the twenty-first century: A risk for addiction or a necessary tool? In Miller, P. (Ed.), *Principles of addiction: Comprehensive addictive behaviors and disorders Vol. 1* (pp. 901-909). Academic Press. https://doi.org/10.1016/B978-0-12-398336-7.00091-7

CARRASCO-ARAIZAGA, J. & TOURLIERE, M. (2015, JULY 11). Los mexicanos espiados hasta la cocina. *Proceso*. https://www.proceso.com.mx/reportajes/2015/7/11/los-mexicanos-espiados-hasta-en-la-cocina-149620.html

_____ (2017, June 20). Así se negocia para que nos Vigilen. *Proceso*. https://www.proceso.com.mx/reportajes/2017/6/20/asi-negocia-el-gobierno-de-pena-nieto-para-que-nos-vigilen-186411.html

CASTELLS, M., FERNÁNDEZ-ARDEVOL, M., LINCHUAN-QIU, J. & SEI, A. (2006). *Comunicación Móvil y Sociedad. Una perspectiva global*. Ariel.

CASTRO-ROJAS, S. R. (2012). Ubicuidad y comunicación: los Smartphones. *Chasqui, Revista Latinoamericana de Comunicación, 118*, pp. 91-95. https://revistachasqui.org/index.php/chasqui/article/view/197/206

CHOE, E. K., LEE, N. B., LEE, B., PRATT, W. & KIENTZ, J. A. (2014, APRIL). *Understanding Quantified-Selfer's Practices in Collecting and Exploring Personal Data* [Conference session]. CHI '14: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. United States. https://doi.org/10.1145/2556288.2557372

CORREDOR-ÁLVAREZ, F. A., TIRADO-SERRANO, F. & IÑIGUEZ-RUEDA, L. (2010). ¿Bajo las riendas del teléfono móvil? Control social, normalización y resistencia. *Psicologia & Sociedade*, *22*(1), pp. 60-69. https://doi.org/10.1590/S0102-71822010000100008

CUESTA-CAMBRA, U., CUESTA-DÍAZ, V., MARTÍNEZ-MARTÍNEZ, L. & NIÑO-GONZÁLEZ, J. I. (2020). Smartphone: en Comunicación, algo más que una adicción. *Revista Latina de Comunicación Social*, *75*, pp. 367-381. https://www.doi.org/10.4185/RLCS-2020-1431

D'ALMEIDA, F. & MARGOT, D. (2018). La evolución de las telecomunicaciones móviles en América Latina y el Caribe. *Serie de Desarrollo a través del Sector Privado*, (4), pp. 1-54. https://www.idbinvest.org/sites/default/files/2018-09/tn4_spa_la_evolucion_de_las_telecomunicaciones_moviles_2018.pdf

DAVIDAVIČIENĖ, V., RAUDELIŪNIENĖ, J., & VIRŠILAITĖ, R. (2021). Evaluation of User Experience in Augmented Reality Mobile Applications. *Journal of Business Economics and Management*, *22*(2), pp. 467–481. https://doi.org/10.3846/jbem.2020.13999

GALINDO, E. M. (2021, AUGUST 20). Personal interview with the university student. [Personal interview].

GSMA (2019). *Leyes inteligentes de privacidad de datos. Cómo lograr los resultados deseados en la era digital.* https://www.gsma.com/latinamerica/wp-content/uploads/2019/10/GSMA_Leyes-inteligentes-de-privacidad-de-datos_junio-2019.pdf

HABIB-UR-REHMAN, M., SUN-LIEW, C., YING-WAH, T., SHUJA, J., & DAGHIGHI, B. (2015). Mining Personal Data Using Smartphones and Wearable Devices: A Survey. *Sensors*, *15*(2), pp. 4430-4469. https://doi.org/10.3390/s150204430

HÖFLICH, J. & RÖSSLER P. (2002). El teléfono móvil y el uso del SMS por parte de los adolescentes alemanes. *Revista de Estudios de Juventud*, *57*, pp. 79-93.

HONG, F. Y., CHIU, S. I., & HUANG, D. H. (2012). A model of the relationship between psychological characteristics, mobile phone addiction and use of mobile phones by Taiwanese university female students. *Computers in Human Behavior*, *28*, pp. 2152–2159. https://doi.org/10.1016/j.chb.2012.06.020

IGARASHI, T., MOTOYOSHI, T., TAKAI, J., & YOSHIDA, T. (2008). No mobile, no life: Self-perception and text-message dependency among Japanese high school students. *Computers in Human Behavior*, *24*, pp. 2311–2324. https://doi.org/10.1016/j.chb.2007.12.001

INTERNATIONAL TELECOMMUNICATION UNION (2014). *The world in 2014: ICT facts and figures.* https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf

KRANZ, M., MÖLLER, A., HAMMERLA, N., DIEWALD, S., PLÖTZ, T., OLIVIER, P., & ROALTER, L. (2013). The mobile fitness coach: Towards individualized skill assessment using personalized mobile devices. *Pervasive and Mobile Computing*, *9*(2), pp. 203–215. https://doi.org/10.1016/j.pmcj.2012.06.002

LA JORNADA (2015, FEBRUARY 12). La generación Z, con un "tren cerebral de alta velocidad que va del ojo al pulgar". https://www.jornada.com.mx/2015/02/12/ciencias/a02n1cie

LEUNG, L. (2007). Unwillingness-to-communicate and college students' motives in SMS mobile messaging". *Telematics and Informatics*, *24*(2), pp. 115–129. https://doi.org/10.1016/j.tele.2006.01.002

LIN, T., CHIANG, Y. H. & QIAOLEI, J. (2015). Sociable People Beware? Investigating Smartphone versus Nonsmartphone Dependency Symptoms among Young Singaporeans. *Social Behavior and Personality: an international journal*, *43*(7), pp. 1209–1216. https://doi.org/10.2224/sbp.2015.43.7.1209

MONTJOYE, Y.A., SHMUELI, E., WANG, S., & PENTLAND, A. S. (2014). openPDS: Protecting the Privacy of Metadata through SafeAnswers. *PLoS ONE*, *9*(7), pp. 1-9. https://doi.org/10.1371/journal.pone.0098790

PALOMARES-HERRERA, M. (2017). Estudio comparado sobre transparencia y Derecho de acceso en el ámbito internacional y su influencia en España. *Ius Humani: Revista de Derecho,* (6), pp. 123-153. https://dialnet.unirioja.es/descarga/articulo/5877166.pdf

PERRY, S. D. & LEE, K. C. (2007). Mobile phone text messaging overuse among developing world university students. *South Africa Journal for Communication Theory and Research, 33*, pp. 63–79. https://doi.org/10.1080/02500160701685417

RHEINGOLD, H. (2004). *Multitudes inteligentes. La próxima revolución social*. Gedisa.

RUELAS, A. L. (2010). El teléfono celular y las aproximaciones para su estudio. *Comunicación y Sociedad*, (14), pp. 143-167.

RUIZ-RICO, C. (2019). Análisis comparativo de la legislación iberoamericana en materia de transparencia y derecho de acceso a la información. *Boletín mexicano de derecho comparado*, *52*(154), pp. 255-283. https://doi.org/10.22201/iij.24484873e.2019.154.14144

SARABIA-SÁNCHEZ, F. J., AGUADO, J. M., & MARTÍNEZ-MARTÍNEZ, I. J. (2019). Privacy paradox in the mobile environment: The influence of the emotions. *El profesional de la información*, *28*(2), pp. 1-11. https://doi.org/10.3145/epi.2019.mar.12

SEKARA, V., ALESSANDRETTI, L., MONES, E., & JONSSON, H. (2021). Temporal and cultural limits of privacy in smartphone app usage. *Scientific Reports*, *11*(3861), p. 1-9. https://doi.org/10.1038/s41598-021-82294-1.pag

SERRA, G., LO-SCALZO, L., GIUFFRÈ, M., FERRARA, P., & CORSELLO, G. (2021). Smartphone use and addiction during the coronavirus disease 2019 (COVID-19) pandemic: cohort study on 184 Italian children and adolescents. *Italian Journal of Pediatrics*, *47*(150), pp. 1-10. https://doi.org/10.1186/s13052-021-01102-8

SERRA-CRISTÓBAL, R. (2015). La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y Seguridad nacional. *Revista de Derecho Político*, *92*, pp. 73-118. https://doi.org/10.5944/rdp.92.2015.14422

SULTAN, A. J. (2014). Addiction to mobile text messaging applications is nothing to "lol" about. *The Social Science Journal*, *51*, pp. 57–69. https://doi.org/10.1016/j.soscij.2013.09.003

TALBOT, D. (2014). Ultraprivate Smartphones. *MIT Technology Review*, *117*(3), pp. 35-37. https://www.technologyreview.com/technology/ultraprivate-smartphones/

TOURLIERE, M. (2015, JULY 12). Citizen Lab exhibe a la empresa de espionaje favorita del peñismo. *Proceso*. https://www.proceso.com.mx/reportajes/2015/7/15/citizen-lab-exhibe-la-empresa-de-espionaje-favorita-del-penismo-149750.html

TU, C.H., MCISAAC, M., SUJO-MONTES, L., & ARMFIELD, S. (2012). Is there a mobile social presence? *Educational Media International*, *49*(4), pp. 247–261. https://doi.org/10.1080/09523987.2012.741195

WIESE, J., DAS, S., HONG, J. I., & ZIMMERMAN, J. (2017). Evolving the Ecosystem of Personal Behavioral Data. *Human–Computer Interaction*, *32*, pp. 447–510. https://doi.org/10.1080/07370024.2017.1295857

ZUBOFF, S. (2019). Surveillance Capitalism and the Challenge of Collective Action. *New Labor Forum 2019, 28*(1) pp. 10–29. https://journals.sagepub.com/doi/full/10.1177/1095796018819461

ANEXO 1

Glossary. Abbreviations and Technical Terms

App	Software application installed in mobile phones to help users with specific tasks
BSN	Body Sensors Network
DSPS	Data Stream Processing Systems
GPS	Global Positioning System, a satellite-based navigation system
ID	Integration Device
PE	Personal Ecosystem
PerDM	Personal Data Mining
PSDs	Personal Sensing Devices
RCE	Remote Component Environment
RCS	Remote Control Systems
SMS	Short Message Service
OMM	Open Mobile Miner
WhatsApp	Mobile-phone app for exchanging written messages, icons, photos, videos, and voice messages over the internet

Source: Own elaboration