DOI: 10.1590/1413-812320182310.15942018

Collective Health and a Sophie's Choice: to defend privacy in cyberspace

Ilara Hämmerli Sozzi de Moraes [1]
Lívia Antunes Prado [1]

Abstract *The world is currently experiencing complex threats to privacy in health (PH) in the context of the growing virtualization of bodies and biographies exposed in social networks. This paper aims to identify the approaches to PH in Brazilian scientific production in the light of Collective Health (CH). This is an exploratory, analytical-descriptive study reviewingpapers from Brazilian Collective Health journals of excellence from 2000 to 2017. Papers employing PH as their object were selected for further analysis. We found that papers are commonly anchored in the perspective that the "professional's fear of punishment" is the borderline inhibiting PH violation actions. However, neither the legal-normative framework nor the technological security apparatus sufficed. In the Unified Health System (SUS), threats escalate in initiatives of the SUS Card, PEP, Regulatory Centers and Telehealth. The results corroborate a hypothetic gap in the production of the subject in Collective Health journals of excellence. The discussion is about institutional omission; adoption of the ICF for the use of individual data; opacity on the revenue of public expenditure in the technological security apparatus. Respect for PH must bethe result of a political-ethical agreement, in which all start to act ethically in defense of privacy by choice and not coercion and fear of penalties.*

Key words *Privacy, Confidentiality, Social networks, Cyberspace*

[1] Escola Nacional de Saúde Pública Sérgio Arouca, Fiocruz. R. Leopoldo Bulhões 1480, Manguinhos. 21041-210 Rio de Janeiro RJ Brasil.
ilara@ensp.fiocruz.br

Introduction

The myriad of positive or disastrous consequences of the Man-Technology relationship impregnates debates on "burning" issues for the very continuity of the human species and a civilizing project for all peoples. One of these matters refers to the current meaning of individual privacy in cyberspace, established by connections in social networks mediated by the technologies of virtualization of the "solid", where "new communities" and new types of relationships are set[1,2]. These interactions are stored in a technological apparatus located somewhere, under the governance of someone unknown, but "trusted" a priori. In trust, mediated by information technology (IT), Men create connections and relationships that ground a space of virtual sociability.

The world currently experiences a political and technological context of threats to privacy and the use of personal and physical data involving complex issues. The same apparatus that virtualizes bodies does so with the financial flow in a globalized capitalist society that advocates privacy violation actions in the name of the "War on Terror". This setting is used as a justification for intensifying the use of cyberspace in agreements such as "The Five Eyes Alliance" (USA, Canada, England, Australia and New Zealand), which spy on the population and exchange data with each other to circumvent/bypass restrictions of the legal-institutional framework of each country concerning population surveillance[3].

Big Data databases, digital social networks and the Internet of Things (IoT) produce an intense online traffic that feeds and strengthens one of the echoes of the Enlightenment project: "faith" in the power of human reason, the trust that technology, science, and technology make us masters and owners of nature, in the words of Descartes. In the rationalism advocated by Voltaire, reason does not expose its limits, insufficiencies, uncertainties and risks. However, from there (18thcentury) to the 21stcentury, the world witnesses an expansion of the limits and risks arising from the Man-Technology relationship, which, to minimize them, must be revealed in their complexity.

This paper focuses on one of these risks: the vulnerability of citizens' privacy concerning "their health" in the increasing virtualization of bodies (public and private healthcare networks) and fragments of biographies exposed by individuals or health professionals (social networks) in cyberspace. A presupposition is implicit: the trust in the security provided by private or collective health managers, such as the Department of Computer Science of the Unified Health System (DATASUS) or owners of the apparatus of social networks, such as Facebook, WhatsApp, Twitter and telecommunication companies. However, neither SUS or health plans[4-6] institutions nor the main social networks[7-9] evidence levels of security that ensure the full preservation of individual privacy.

Nowadays, consciously or unconsciously, everyone who uses the Internet faces a choice almost impossible to make – Sophia's choice – considering that any option has equally disturbing consequences, considering both the social, political and ethical value historically ascribed to privacy and IT penetration in the daily life of human life. Is it possible to choose to stay "out" of cyberspace? Spatial and temporal mobility (GPS in cars and cell phones, for example), bank flow, consumption of goods and services, health examination results, medical records, life cycle (birth to death): everything is traceable.

It is considered that the concerns shown here are one of the problems to which there is not yet a complete solution, as Hobsbawm[10] warns:

The Brief Twentieth Century ended in problems for which no one had, nor said to have solutions. As they groped their way into the third millennium amid the global fog that surrounded them, the fin-de-siècle citizens only knew for sure that an era of history had ended, and very little else.

Given this context, the imperative to further reflect around the complex issue of the defense of privacy in its expression in the health sphere emerges. This concern gives rise to this study and its starting question: In Brazil, how has the field of Collective Health knowledge and practices[11,12] been questioning the theme of privacy in the context of intensified use of virtualization technologies[1] that affects the processes of health care and its meaning in society? Thus, evidence is sought to confirm or refute the hypothesis that there is a gap in the production of knowledge about the issue within Brazilian Collective Health.

Methods

This study on privacy in health (PH) aims to understand the approaches developed on the subject of the privacy of individuals and communities in the Brazilian scientific production in the light of Collective Health references. In this regard, an exploratory study is carried out,

Ciência & Saúde Coletiva, 23(10):3267-3276, 2018

with analytical-descriptive orientation, adopting the assumption that one of the ways to identify the scientific production of a knowledge area is to analyze the material published in journals of excellence considered by the field.

The conceptual design that underpins the research builds on the thought of Paim and Almeida Filho[11,12] for the understanding of Collective Health, and of Pierre Lévy[1,2] for the concepts of cyberspace and virtualization. The latter argues that cyberspace is a "new flood" caused by the technological advances of information technologies:

The term specifies not only the material infrastructure of digital communication but also the oceanic information universe it harbors, as well as the human beings who navigate and nurture this universe[1].

Lévy[2] characterizes the concept of virtualization as the detachment of the fixed and solid, the here and now, where the elements are "nomadic, liquid and dispersed", reinforcing the idea of "deterritorialization" and "timelessness".

When a person, a community, an act, some information becomes virtualized, they become 'non-present', they are deterritorialized. A kind of trip separates them from ordinary physical or geographical space and clock and calendar temporality. It is true that they are not independent of the space-time of reference since they must always insert themselves into physical media and update themselves here or elsewhere, now or later. However, virtualization made them skip out[2].

The formulation of Paim and Almeida Filho[11,12] is used to support the conception of Collective Health as a field of knowledge and scope of practice:

As a field of knowledge, collective health contributes to the study of the health/disease phenomenon in populations as a social process; investigates the production and distribution of diseases in society as processes of social production and reproduction; and analyzes health practices (work process) *in its articulation with other social practices; it seeks to understand, in short, the ways in which society identifies its health needs and problems, seeks its explanation and organizes itself to confront them.* [...] *... collective health privileges... four intervention objects: policies* (power distribution forms); *practices* (behavioral changes, culture, institutions, production of knowledge, institutional, professional and relational practices); *technical* (organization and regulation of resources and productive processes; bodies / environments); *and tools* (means of production of intervention)[11].

With this set of references, a review of the scientific production published in the leading Brazilian journals on Collective Health Knowledge (according to the Table of Coordination for the Improvement of Higher Education Personnel/CAPES) is carried out. We employed CAPES' *Qualis-Periódicos* classification, which is adopted by the representatives of the evaluation areas themselves, to define which Brazilian publications are classified as of excellence. Thus, we established as a source of the study Collective Health journals located in the upper strata, namely, A2, B1 and B2. In the current ranking, no Brazilian journal is rated A1 by the Collective Health Assessment Area.

Papers published from 2000 to August 2017 were selected. The analysis of the literature shows that the second half of the 1990s is characterized by the beginning of the advancement of microelectronics in the Brazilian institutional and business spaces. Several initiatives emerge from the migration of 100% analogical information flow to a health work process with IT-mediated stages. Information and Information Technology in Health Projects (ITIS) are gaining momentum *pari passu*with the consolidation of the economic and political power of Brazilian IT companies[13,14]. The gradual onset of scientific production with analyses on ITIS initiatives occurs in this period. In parallel, in the first half of the 2000s, digital social networks begin their journey – MSN Messenger (1999), MySpace (2003), LinkedIn (2003), Orkut and Facebook (2004) – raising new privacy issues.

Papers were searched in the Medical Literature Analysis and Retrieval System Online (Medline) database via PubMed and the Virtual Health Library Portal (BVS). The descriptors and keywords used in the elaboration of the search strategies (using the Boolean method) were defined based on the consultation of experts from the ENSP/CNPq Information and Health Research Group, and the following were selected: in the Medical Subject Headings (MeSH)[15], used in MEDLINE search: *Privacy*; *Genetic Privacy*, *Confidentiality*. In the Health Sciences Descriptors (DeCS)[16], used in the BVS, we selected the following Portuguese keywords: *Privacidade*, *Confidencialidade*, *EspaçoPessoal*, *Autorrevelação*, *ComunicaçãoPrivilegiada*, *Sigilo*.

The other methodological steps are summarized as follows:

1. Elaboration and implementation of search strategies in databases through various search tests. After successive refinements, nine strategies

with significant results associated with the object of the study were obtained.

2. Addition of titles, abstracts and full-text-papers in the Zotero Free Open Source Reference Manager Software and withdrawal of duplicates.

3. Double-blind reading of titles and abstracts independently and classification according to the following criteria for eligibility of papersconcerning "privacy in health": *Group A* – it is the object of study of the paper; *Group B* – it is addressed as one of the realms of the object of study; *Group C* – it appears in the text without direct connection to its object; and *Group D* – it is present in the publication and is associated with a scope other than health, such as copyright and open access to scientific journals. Any disagreement in the classification of papers was resolved by consensus among the authors of this investigation, based on the understanding adopted on Collective Health.

4. Concerning the defined conceptual design, for the critical reading of full-text papers, the following guiding questions were elaborated for analysis: 1) What object/theme/problem is addressed by the paper? 2) What realm of privacy in health is addressed: informational privacy or physical/bodily/territorial privacy? 3) From which perspective is privacy analyzed? That of the serviced patient or the health professional? 4) What method was adopted? 5) Are papers grounded on the preservation of health privacy and proposal for its guarantee? If so, which ones?

Results

The implementation of the first two stages of the bibliographic review resulted in ninety-six (96) papers distributed in twenty-four (24) journals, highlighting: *Ciência & Saúde Coletiva* (19); *Cadernos de Saúde Pública* (16); *Revista da Associação Médica Brasileira* (10); *Revista Latino-Americana de Enfermagem* (8); *Revista Brasileira de Enfermagem* (7); *Revista de Saúde Pública* (5); *Saúde e Sociedade* (4). Of concern, we can observe that 48 papers were published in the period 2000-2010, a number that is repeated in the period 2011-2017, despite the progress of IT in Health.

Also of concern is the result found after applying the eligibility criteria of the papers (step 3). Only fifteen (15) papers address "privacy in health" as the object of the study, which has been the case for almost two decades, published in journals rated as of excellence by the Collective Health sector (Table 1).

The fifteen papers thus become the primary source for an in-depth examination with the objective of identifying the realms and approaches on the subject of the privacy of individuals and communities studied by the authors. In order to analyze the contributions that researchers add to old and new challenges regarding health privacy, a "dialogue" with them was sought through guiding questions (step 4). The primary results are described below:

Concerning Question 1) What object/theme/problem is addressed by the paper?

Privacy was addressed in a broad spectrum of situations associated with health care (Table 2).

The thematic diversity found can be interpreted as evidence of the complexity of the topic, found in almost all facets of healthcare. Despite the expanded use of social networks geared to Health, only one paper was devoted to studying them concerning PH. In the regional distribution, 86.6% of the works were produced by authors linked to universities in the South and Southeast, 13.4% in the Midwest and none in the North and Northeast.

As a subsidy for the epistemological debate on Collective Health, it should be pointed out that in the "cutting-edge" journals of the Collective Health Knowledge Area (CAPES), a prevalence of Clinical references on the topic PH is observed (60% of the papers).

Concerning Question 2) What realm of privacy in health is addressed: informational privacy or physical/bodily/territorial privacy?

Two categories were established to understand better the approach adopted by the authors, namely: informational privacy, when referred to the content of health information that can be identified by the individual, named in the legal framework as "personal data"; and the serviced subject's bodily privacy and the space that he/she occupies when associated with the face-to-face care provided by the health team, in the procedures that require direct contact. Of the papers selected in this stage, 20% addressed two categories, and 80% were geared to informational privacy.

Concerning Question 3) From which perspective is privacy analyzed? That of the serviced patient or the health professional?

This question was introduced to identify, concerning the health team – subject attended, which end of this binomial has deserved more attention. Studies that analyzed PH from the perspective of the health professional (46.7%) prevailed compared to those who analyzed the lenses

Ciência & Saúde Coletiva, 23(10):3267-3276, 2018

Table 1. Distribution of the selected papers (steps 1, 2 and 3) by eligibility criteria according to the approach of the privacy in health (PH) topic.

Classification by eligibility criteria	Papers (N.)	%
Group A – it is the object of study of the paper	15	15.6
Group B – it is addressed as one of the realms of the object of study	24	25.0
Group C – it is cited in the text without connection to its object	19	19.8
Group D – PH is present in the text and is associated with a scope other than health	38	39.6
Total	**96**	**100.0**

Table 2. Distribution of selected papers in Group A (step 4) by realm associated with health care.

Realms associated with healthcare	N.	%
Care to the HIV patient in the Family Health Program (PSF)	03	20.0
Adolescent care	02	13.3
PSF care, in general	02	13.3
Genetic counseling – sickle cell trait	01	6.7
ICU care	01	6.7
Hospital care	01	6.7
Nursing care	01	6.7
Exhibition of pictures with the identification of patients posted by doctors and dentists on Facebook	01	6.7
Law on access to information and privacy in research	01	6.7
Technological risks from the perspective of health law	01	6.7
Oral Health – Second opinion consultation	01	6.7
Total	**15**	**100.0**

of the serviced subject (26.7%). The remaining 26.7% addressed both perspectives. Consistent with the more significant number of nursing care-related studies, the perspective of the nursing team was the most studied, followed by the PSF team.

Concerning Question 4) What method was adopted?

The descriptive exploratory studies with a qualitative approach predominated (66.6%), varying regarding the techniques and methods adopted (content analysis, focus group, interviews), and 26.7% are theoretical essays, with one ethnographic study (6.7%). One opinion paper does not evidence any method.

Concerning Question 5) Are papers grounded on the preservation of health privacy and proposal for its guarantee? If so, which ones?

The basis for the preservation of PH was the characteristic feature in 100% of the papers. In any given situation, it is assumed that privacy is an ethical value and human right that should be assured by health professionals. Only two papers evidenced a nuance, extending responsibility to the health institution.

PHis worked out as a principle associated with respect, autonomy and dignity. The human rights perspective has provided a clear and robust reference not only for the identification and understanding of socially established situations of vulnerability but also to identify means to help overcome them. References of PH as a human right enlighten different realms that concretely found the ideals of a civilizing project.

The finding that there are failures in the preservation of privacy in health was highlighted in 86% of papers, whether they address studies in public or private services, especially when they involve people with health insurance plans.

A first reading evidences proposals or recommendations that are diverse. However, careful analysis shows that they are anchored in the same rationality: on the one hand, a particular "faith" in the existing legal-institutional-normative framework, and on the other, in behavioral changes of health professionals, under penalty of punish-

ment by their professional regulatory bodies. In this conception of PH proposals, a professional emerges– the community health worker –who is not subject to any regulatory body, who was the subject of search in 20% of the papers and cited in 13.3% as an element "outside this framework" deserving "specific regulations" (same rationality).

The recognition of the existence of inequalities in the care with the privacy of citizens according to the socioeconomic situation, ethnicity or gender is noted in 20% of the papers. One of the papers (6.7%) highlighted the technological apparatus of information security, such as data encryption other than the use of access passwords. Only one paper questions "trust" in the current legal-normative framework, proposing that PH be under public control, with the use of an Informed Consent Form (ICF) for the current and potential uses of the information of the assisted subject, which underpins health databases.

Discussion

The results shown express only a specific realm on how the subject of privacy in health is addressed in light of the Collective Health references. There is a whole universe to be studied. However, the analysis of scientific production in Brazilian journals rated A2, B1 and B2 has proved to be a useful alternative in the search, since in a first approximation, they were well-versed on the questioning developed.

Within the limits of this selection, the study has provided indications about what is being proposed to reduce the vulnerability of individuals and groups, contributing to debates in the area around actions that minimize negative and sometimes overwhelming consequences for a decent life of citizens in the full enjoyment of their rights and for the quality of health care. However, in seventeen years (2000-2017), the endpoint of only fifteen papers classified in Group A evidences the need to further study the determinants for such finding.Considering the value and relevance assigned to the topic within Collective Health knowledge and practices vis-à-vis the evaluation criteria adopted by the Collective Health Knowledge Area/CAPES, as well as the editorial and evaluative lines of journals rated A2, B1 and B2, it is worth emphasizing that this finding does not mean that the issue is not the subject of concerns and research in the field of Brazilian Collective Health, but only expresses those that "were filtered through" the periodicals.

When highlighting informational privacy, the papers examined underlie, to a certain extent, the contemporary uneasiness that Man does not yet have satisfactory answers to deal with the risks arising from the fast and intense virtualization of the most diverse facets of life, among which the violation of PH. Cyberspace is not a "safe place". There are shadows, a deep web, hackers and crackers, institutional surveillance, the war on terror, curiosity, the desire to snoop on the privacy of others. There are sounds, images and texts in an impalpable medium, where time and space are diluted and become fluid[1,2] but allow for symbolic interpersonal interactions from the most varied places in the world, establishing an endless tangle of social networks.

The analysis evidences that the proposals to ensure PH shown in the papers studied are anchored in the perspective that the "fear of punishment" is the borderline to inhibit actions of disrespect to PH, penalties that are foreseen in the legal, institutional and normative framework. This approach may seem necessary and relevant, but will it suffice?

Other areas of knowledge are worth mentioning, such as Biomedical Engineering, Software Engineering, Computing and the thematic field called Health Informatics, which concentrate their "faith" in technological security mechanisms. However, things are not that smooth here either. According to Gartner Consulting, in 2018, global investment in information security is expected to reach US$ 93 billion, which represents a 12% increase over last year, but in the evaluation of UPX Technologies, even with the high figures, the sector is vulnerable and jeopardizes user data, whether or not they are business users. It states that 2017 was marked by major mass attacks that affected the entire world and hijacked data from organizations worldwide[17].

The international literature[18] shows that neither the legal-normative-institutional framework nor the technological security apparatus has been sufficient. Violations of databases with sensitive information related to the privacy of individuals and human communities in the most diverse situations are reported daily. However, the political debate in society can still be considered reduced given the complexity of the issues involved in the fabric of cyberspace. Although it is not within the scope of this paper to answer it, the question prevails: why is that so?

Technological advances, such as the interoperability between large databases (Big Data) in Health composed by nominal bases, facilitate the

Ciência & Saúde Coletiva, 23(10):3267-3276, 2018

tracing of the citizen's journey through health (public or private) services, enhancing risks of invaded privacy, a fundamental ethical principle in the trust relationship of citizens with professionals and health services, and the quality of care. In the SUS, these threats escalate depending on the consequences of some initiatives, such as the National Health Card, e-Health, Electronic Patient Record, Regulatory Centers and Telehealth, which are topics that did not appear in the 96 papers selected in the first steps of this research. These results corroborate the hypothesis of this study: there is a gap in the production of knowledge about the topic in the field of Brazilian Collective Health published in journals of excellence on the subject. A troubling finding to consider is the historical trend evidenced in this research: the number of papers published on the topic in the period 2000-2010 is upheld in the 2011-2017 period.

The previous studies[6,19,20] have shown that the theme of PH involves political, economic, social, scientific, technological, cultural and symbolic interests that weave the structure of cyberspace. Many actions make patient privacy vulnerable. As an example, a case of great international repercussion, reported by the New York Times (https://www.nytimes.com/ on 09/28/2010), occurred at the New York Presbyterian Hospital. Medical data of 6,800 patients were leaked through search engines on the Internet. Information such as name, age, clinical and surgical status and test results were available in cyberspace. According to the New York Times, the mistake was detected in early July 2010, only after reports by relatives of a patient whose information was found on the internet. It is noteworthy that the problem was only made public because of the investigation on the case, generated by a lawsuit filed by the New York Police and The National Institutes of Health, culminating recently with the payment of $ 4.8 million to resolve possible violations of health privacy laws.

Targeting virtual social networking, companies create applications that "help users take care of their health." However, what are the effective assurances of privacy protection? By way of illustration, we mention a study evaluating menstrual control and fertility applications by Consumer Reports[21], which denounced in 2016 the GLOW application for practices that harm the privacy of its female users. However, other apps also evidence vulnerabilities. The information generated through the use of these applications is a capital for the companies that create them, without users' knowledge. Everything that is contained in social networks and applications, including information on the sexual life and reproductive cycle can be monetized, and is profitable not only for the pharmaceutical industry and health plan operators, but also for advertisers who wish to sell their products to women of certain profile, and for those who mediate these processes. Information is shared with third parties, either for publicity purposes or for health research, whose business model of apps' developers is based on the use of these data[22].

Evidence seems to indicate that the vulnerability of the PH occurs not necessarily due to a lack of a legal-institutional-normative framework or security devices. The studies show that in Brazil as in other countries, norms, regulations and security mechanisms are fundamental, but alone have proved insufficient for the preservation of the right to privacy. So, what to do?

Far from pretending to answer this question, one must cling to the statement of philosopher Karl Marx[23]: *Humanity only raises the problems that it is capable of solving, and so, in close observation, it will be found that the problem itself emerged when the conditions for resolving it already existed or were at least in the process of appearing.*

It is, therefore, necessary to face the challenge of uncovering the conditions from which to build action strategies that expand assurances of PH, aligned with the inter and transdisciplinary approach of Collective Health. To this end, some persistent concerns and proposals to be debated and further analyzed in new studies are shown below:

- Concerning the legal-institutional-normative framework, it is imperative to move forward. Brazil does not yet have a general law for the protection of personal data. The issue of data protection on the Internet is a constant challenge, allowing abusive practices by companies that process these data, with an impact on (public or private) health services that computerize their healthcare practices.
- It is worth discussing the different levels of accountability for invasions of privacy. As shown in the Results, the analysis of papers revealed an emphasis on the individual behavior of health professionals, as if no institutional and political responsibility permeates praxis in health services. The higher the burden of duty to preserve PH and punishment (in case of violation) falls on the health professional, abstracting the institutional contextualization in which the risk to PH emerges. The proposals to minimize threats to PH by

substantively prioritizing "behavioral changes" do not face the complexity that currently characterizes PH. The health institutions omit themselves before violations with a discourse alleging an isolated action of a professional. Silence in the face of disrespect to PH is refined in its indignity when it emerges as a result of ethnicity, gender, age or economic situation of the serviced individual who has been harmed. One must incorporate into the institutional culture of the SUS the principle that the information provided by citizens in their contact with the health system belongs to them and not to the institution, the team or the doctor and. Therefore, the subject served should authorize the use of his/her information that feeds both the electronic patient record (PEP) and the so-called health information systems of the SUS. This control must be formalized previously through the informed consent form, which lists the criteria under which citizens authorize the use of their individual, physical and genetic data by science and public and private management.

• About the technological apparatus, an endless path remains to be pursued among the sellers of "information security solutions" and those who enrich themselves by endangering information security, including threats to privacy. Cyberspace has become an arena for disputes between "the fellas" (hackers) and the "bad boys" (crackers), which currently generate one of the highest revenues in the world[24]. How has the area of health, especially public managers, been driving its technological security options? This is an opaque topic in the debate on public policies in Brazil, and especially in the National Health Policy. Who defines and how are the specifications of bidding documents for acquisition of security mechanisms for "SUS Big Data" being decided? Have options fallen on adopting open source or proprietary "security solutions"? Who has participated in this debate? What is the social control over these issues that involve millions of Reals from the SUS public budget? These are themes of a public policy agenda related to the incorporation of ITIS into the praxis of the health sector in its relation with the citizen who, in general, is not considered as "The Player" in this decision-making process. The existing institutional culture drives away citizens (in the Health Councils: user representatives) from this debate because it is a "technical", "experts" issue[25]. It is technocratic rationality to politically exclude citizens from the debate of a public policy that focuses on how individuals and communities want to preserve the PH.

• It is observed that, depending on the area of knowledge, the perspective of actions aimed at ensuring the PH rests now on continuous advances in the juridical-institutional-normative framework, anchored in the rationale of fear of being caught red-handed and its consequent punishment, sometimes in the continuous development of the technological apparatus of information security. However, violations persist in all countries of the globalized world. In the scope of this work, despite different traditions of analysis that structure distinct areas of knowledge, we try to highlight the relevance of the two strands, which are the faces of the same coin and require a further study that impregnates each other. One complements the other if, and only if both discuss the theme of PH in a complementary and respectful way in the search for interdisciplinary dialogue, in mutual writing. Trails being built to this end[4,26-28] deserve to be widely debated, since they contribute to the establishment of a virtuous communicative circle of knowledge, such as the sociotechnical approach of ITIS.

Final considerations

It can be seen that, without a set of political, ethical and technological initiatives aimed at respecting citizens' privacy, the conditions of a "risk environment" for the project of a country that preserves the value of life are extended. The challenge is to inscribe respect for human dignity in the praxis of healthcare as a gain to society: expression of a broad Ethical and Political Agreement guided by responsibility towards one's neighbor and the community, based on rationality other than that of the "fear of punishment".

Respect for privacy must become a result of the will and the understanding and express itself in a broad and capillary political-ethical coalition, in which all the subjects involved (managers, professionals and serviced individuals and groups) participate fully in the exercise of citizenship in the construction of "new institutional cultures".

An agreement based on understanding differs from the doctrine of man's duties, from the fear of penalties, where the individual acts/performs something by command and not by free, autonomous decision. Insofar as the imperative of duty becomes a citizen and professional option, PH is assured by understanding and no longer by external compulsion. In this case, the construction of this understanding adopts what Spinoza[29] calls *rational ethics* as a matrix.

Ciência & Saúde Coletiva, 23(10):3267-3276, 2018

The defense of privacy in health, based on the rational ethics of Spinoza, becomes an expression of an act of the will of citizens, counselors, professionals and health managers around the understanding of the severe consequences of breaking the built trust, throughout history, in the relationship between the health system and the patient, and their impact on the quality of care. Everyone begins to act ethically in defense of privacy by choice and not by coercion and fear of penalties.

On one condition: the commitment of the team (both health and IT) and the institutions around the will and the understanding (Rational Ethics) about the importance of PH. Respect for privacy is a fundamental requirement for the existence of a society that is respectful of itself and the other. It is a parameter for a just, fraternal and dignified nation in a civilizing project to be achieved through a long process of struggle and collective learning based on solidarity, democratic praxis, shared responsibilities, rational ethics... and historical patience!

Collaborations

IHS Moraes worked on the concept, study design, methods, analysis and interpretation of the data and on drafting the paper; LA Prado worked on research, methods and final drafting.

References

1. Lévy P. Cibercultura. São Paulo: Ed. 34; 1999.
2. Lévy P. O que é o virtual? São Paulo: Ed. 34; 1996.
3. Ball J. US and UK struck secret deal to allow NSA to 'unmask' Britons' personal data. *The Guardian* [daily newspaper] 2013 Nov 20; [acessado 2017 Mar 03]. Em: https://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data
4. Vargens JM. *Uma abordagem sociotécnica para design e desenvolvimento de sistemas de informação em saúde no âmbito do SUS* [tese]. Rio de Janeiro: Escola Nacional de Saúde Pública Sérgio Arouca; 2014.
5. Koichi K, Pazello M. e-Saúde e desafios à proteção da privacidade no Brasil. *PoliTICS* [revista online] 2013 Nov; 16. [acessado 2017 Jan 06]; Em: https://politics.org.br/edicoes/e-sa%C3%BAde-e-desafios-%C3%A0-prote%C3%A7%C3%A3o-da-privacidade-no-brasil
6. Moraes IHS. Prefácio. In: Keinert TMM, Sarti FM, Cortizo CT, Paula SHB, org. *Proteção à privacidade e acesso às informações em saúde*: tecnologias, direitos e ética. São Paulo: Instituto de Saúde; 2015. p. 9-20.
7. Electronic Frontier Foundation (EFF). *Secure Messaging Scorecard*. [site] 2014. [acessado 2015 Fev 15]. Disponível em: https://www.eff.org/
8. Fundação Getúlio Vargas (FGV). Centro de Tecnologia e Sociedade da Escola de Direito do RJ. *Relatório de políticas de internet*: Brasil 2011. São Paulo: Comitê Gestor da Internet no Brasil; 2012.
9. Os 10 apps de mensagem mais seguros. *Revista Exame*; 2015 jan 22; [acessado 2017 Jan 06] Em: https://exame.abril.com.br/tecnologia/os-10-apps-de-mensagem-mais-seguros/
10. Hobsbawm E. *Era dos extremos*: o breve século XX 1914-1991. São Paulo: Companhia das Letras; 1995; p.537.
11. Paim JS, Almeida Filho N. Saúde coletiva: uma "nova saúde pública" ou campo aberto a novos paradigmas? *Rev. Saúde Pública*. 1998; 32(4):299-316.
12. Almeida Filho N. O conceito de saúde: ponto-cego da epidemiologia? *Rev. bras. epidemiol*. 2000; 3(1-3):4-20.
13. Silva AB, Moraes IHS. O caso da Rede Universitária de Telemedicina: análise da entrada da telessaúde na agenda política brasileira. *Physis* 2012; 22(3):1211-1235.
14. Vasconcellos MM, Gribel EB, Moraes IHS. Registros em saúde: avaliação da qualidade do prontuário do paciente na atenção básica, Rio de Janeiro, Brasil. *Cad. Saúde Pública* 2008; 24 (Suppl 1):s173-s182.
15. U.S. National Library of Medicine (NLM). National Center for Biotechnology Information. *Medical Subject Headings Database*. 2017 [acessado 2017 Dez 20]. Em: https://www.nlm.nih.gov/mesh/meshhome.html
16. Biblioteca Virtual em Saúde (BVS). *DeCS* - Descritores em Ciências da Saúde. [acessado 2017 Dez 20]. Em: http://decs.bvs.br/P/decsweb2017.htm
17. *Security Report* Exposição de falhas dos gigantes da tecnologia continuará em 2018. 2018 Jan 24; [acessado 2018 Jan 25]. Em: http://www.securityreport.com.br/overview/exposicao-de-falhas-dos-gigantes-da-tecnologia-continuara-em-2018/#.Wmz3RK6nHDd
18. Assange J. *Cypherpunks*: Liberdade e o futuro da internet. São Paulo: Boitempo; 2013
19. Fortes PAC. A bioética em um mundo em transformação. *Rev. Bioética* 2011; 19(2):319-327.
20. Dallari SG. A justiça, o direito e os bancos de dados epidemiológicos. *Cien Saude Colet* 2007; 12(3):633-641.
21. Beilinson J. Glow pregnancy app exposed women to privacy threats, consumer reports finds. *Consumer Reports*; 2016 Jul 28; [acessado 2017 Mar 03]. Em: https://www.consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats/
22. Dias T. Os aplicativos sobre os ciclos menstruais e a exposição de dados pessoais das usuárias. *Nexo*; 2016 Out 03 [acessado 2017 Mar 03]. Em: https://www.nexojornal.com.br/expresso/2016/10/03/Os-aplicativos-sobre-os-ciclos-menstruais-e-a-exposi%C3%A7%C3%A3o-de-dados-pessoais-das-usu%C3%A1rias
23. Marx K. *O Capital: crítica da economia política*. São Paulo: Martins Fontes; 1983.
24. Information security consulting market to reach $26.15 billion by 2021. *Help Net Security* [site] 2017 Dez 20; [acessado 2017 Mar 03]. Em: https://www.helpnetsecurity.com/2017/01/10/information-security-consulting-market/
25. Moraes IHS, Veiga L, Vasconcellos MM, Santos SFR. Inclusão digital e conselheiros de saúde: uma política para a redução da desigualdade social no Brasil. *Cien Saude Colet* 2009; 14(3):879-888.
26. Fornazin M, Joia LA. Articulando perspectivas teóricas para analisar a informática em saúde no Brasil. *Saude Soc* 2015; 24(1):46-60.
27. Fornazin M, Joia LA. Remontando a rede de atores na implantação de um sistema de informação em saúde. *Rev. adm. empres.* 2015; 55(5):527-538.
28. Cukierman HL, Teixeira C, Prikladnicki R. Um olhar sociotécnico sobre a Engenharia de software. *Revista de Informática Teórica e Aplicada* 2007; 14(2):199-219.
29. Spinoza B. *Ética*. Belo Horizonte: Editora Autêntica; 2007.

Article submitted 31/01/2018
Approved 06/03/2018
Final version submitted 11/06/2018