

Beyond privacy: the right to health information, personal data protection, and governance

Para além da privacidade: direito à informação na saúde, proteção de dados pessoais e governança

Además de la privacidad: derecho a la información sobre la salud, protección de datos personales y gobernanza

Miriam Ventura ¹
Cláudia Medina Coeli ¹

doi: 10.1590/0102-311X00106818

The right to information and the use of personal data in the production of information raises numerous challenges in the face of “surveillance capitalism”, with intense commodification and attempts at subordination of public interests to private ones, as highlighted in the article by Keinert & Cortizo ¹. The aim of this commentary is to identify some problematic issues pertaining to personal data protection, based on discussions by researchers in the field of Public Health, in order to propose adequate regulation and governance in the use and treatment of personal data.

Brazil lacks specific federal legislation on personal data protection, the regulation of which has been implemented by different agencies according to specific needs and demands and their legal jurisdictions and attributions. The Public Health field has extensive experience in the production of information using personal data, but the sector still relies on limited, fragmented, and unstable regulation for this purpose.

We identify at least two difficulties in the discussion on regulation and governance of personal data. One such difficulty is conceptual, concerning the notion of public and private when defining goods and interests for regulation. Another difficulty relates to the operationalization of these concepts in the development of a normative model for regulation and governance of personal data that covers authorization of access to data and their treatment.

The first of these difficulties requires reflecting on how “private” can become “public” in such a way as to overcome restrictive and antagonistic dichotomies, preserving fundamental rights and legitimate individual and collective interests in relation to privacy and health. The second requires the development of more effective collective custody in protecting and guaranteeing the use of personal data for public interest purposes.

The debates are fed by the discussion on which interests should prevail in conflicting situations (public and private) and the type of effective legal custody for protecting privacy in access to personal data. This reveals a reduction of the notion of “public” to that of “governmental”, as the only alternative to private. It also illustrates the need to go beyond the simple formulation of formal protection of personal data as an individual’s private and exclusive good, emphasizing that we should seek alternatives for the production of a common good in the public interest, linked to the local and global normative, social, and political contexts.

¹ Instituto de Estudos em Saúde Coletiva, Universidade Federal do Rio de Janeiro, Rio de Janeiro, Brasil.

Correspondence

M. Ventura
Instituto de Estudos em Saúde Coletiva, Universidade Federal do Rio de Janeiro.
Av. Horácio Macedo s/n,
Cidade Universitária,
Rio de Janeiro, RJ 21941-598,
Brasil.
miriam.ventura@iesc.ufrj.br



Privacy and personal data: between public and private

The different ways that privacy has been defined throughout history illustrate how this notion is not univocal and that the type of protection is based on the different uses and purposes in the collection, treatment, and nature of the information produced. The right to privacy conceived as one's right to be left in peace and free of intromission in one's private life has been emphasized as the right to control the use that others make of personal information, constituting the right to information ².

While the right to information initially devoted special attention to privacy and individual protection, more recently it has incorporated the more complete notion of data protection, which extrapolates individual custody and seeks to reconcile such protection with the growing social demand for access to information on various aspects of life, as a fundamental right in public and private decision-making ³.

Brazil's *Law n. 8,080/1990* regulates the citizen's right to information and the state's duty to base its policies and actions on health information and scientific evidence, legitimizing the collection and use of personal information. Beyond the law, the population's general expectation is that health information will allow for better quality of life and the reduction of health risks. Still, individuals display some resistance to furnishing information that may result in some type of control over their behavior, while the reasons cited for the data collection may affect their claim to privacy ⁴.

Beyond the protection of privacy, personal data in health definitely play another role in the production of a common good. The collective interest is intrinsic to understanding the common good in health, determining the values and parameters that should orient the use and availability of personal data as a protected legal good, while seeking to meet collective needs.

This dynamic resignification of the right to privacy and health information requires regulation and governance with a virtual link between the protection of privacy and the promotion of access to information, in keeping with the above-mentioned collective needs and the available technological possibilities.

However, as critically analyzed by Teixeira ⁵, the excessive focus on the public-private dichotomy has sometimes limited thinking and action in the production of the common good in health, which calls for progress in overcoming this restrictive and antagonistic dichotomy.

Another aspect is the inherent conceptual fluidity in the notions of common good, public interest, and collective needs ⁶, alongside the difficulty in weighing fundamental rights that enjoy equal Constitutional status, namely privacy and public health ⁷. In this sense, Binetbojm identifies the legal duty of government to conduct a weighted judgement guided by proportionality and maximum optimization of the interests at stake, without establishing an a priori theoretical prevalence of certain interests over others, rather considering the profound interweaving of collective and individual interests ⁷.

Privacy and governance in data access

Governance, defined as a means by which society collectively seeks to ensure the conditions to achieve a given objective, takes place mainly but not exclusively in the governmental domain. This requires coordinated action by different interest groups ⁸ and adequate mechanisms to ensure explicit and systematic assessment based on ethical principles for making and reviewing decisions ⁹. The Brazilian legislation on access to public information (*Law n. 12,527/2011*) only includes limited provisions on personal data and government management of access ³.

The rapid evolution of information and communication technologies, especially the intensive use of the Internet, unlimited in time and space, has led to a growing volume and variety of data that can be combined, increasing the risk of reidentification even after anonymization or de-identification of single databases ¹⁰. Acknowledgement of the limited effectiveness of such procedures as anonymization, de-identification, and informed consent in the protection of privacy has increasingly highlighted the need for mechanisms to allow greater control over the use of data ¹¹.

A successful experience is that of Population Data BC (PopData), an innovative model for access, treatment, and use of population databases with relevance for health research ¹². The center functions as a reliable third party that conducts mediation between researchers and database managers in the

province of British Columbia, Canada, with the database managers responsible for final approval of requests to use data under their custody. As for security, researchers' access to data is virtual, thus increasing the control over the data's use and minimizing the risk of reidentification of the databases. The center itself does not conduct research; its mission is to train researchers in the use of secondary data and provide a safe environment for storing, treating, and accessing data.

Researchers associated with PopData have suggested the adoption of a data governance model that seeks to adjust the legal principles of privacy to a risk assessment of the demands for access to population databases, proportional to the level of risk involved in the request for access ¹¹. In this model, the assessment is based on three domains, each of which is associated with four risk levels, ranging from "low" to "very high". The domains include assessment of the request's scientific merit and potential impact, the type of question to be explored (test of hypothesis vs. generation of hypothesis), type of data requested (granularity, risk of identification, sensitive data), characteristics of the requesting party (academic affiliation, expertise), security of the environment where the data will be stored, and the type of interest (public, commercial). Requests classified as higher risk undergo a more detailed review process. The proposal provides a reference chart for risk assessment, but various aspects require more in-depth definition in each context, considering the views of database managers as well as those of the other actors involved.

The above-mentioned data governance model is an alternative that ensures a balance between safeguarding the right to privacy and the potential gains from the data's use in evaluation and population research.

The rights to privacy, personal data protection, and information, as fundamental and subjective citizens' rights, represent pillars in the democratic rule of law and require broad social participation. In the face of globalized and neoliberal "surveillance capitalism" ¹ with multiple market and personal interests, our challenge is how to formulate information laws and policies for personal data as a common good of public interest, guaranteeing the public (not exclusively governmental) dimension and the state's duties in the protection of privacy and promotion of access to information.

Contributors

The authors participated in all stages of the article's production.

Acknowledgments

Brazilian National Research Council (CNPq – 447199/2014-5; CNPq 305545/2015-9) and Rio de Janeiro Research Foundation (Faperj – E-26/203.195/2015).

1. Keinert TMZ, Cortizo CT. Dimensões da privacidade das informações em saúde. *Cad Saúde Pública* 2018; 34:e00039417.
2. Rodotá S. A vida na sociedade da vigilância – a privacidade hoje. Rio de Janeiro: Renovar; 2008.
3. Ventura M. Lei de acesso à informação, privacidade e a pesquisa em saúde. *Cad Saúde Pública* 2013; 29:636-8.
4. da Silva EM, Coeli CM, Ventura M, Palacios M, Magnanini MM, Camargo TM, et al. Informed consent for record linkage: a systematic review. *J Med Ethics* 2012; 38:639-42.
5. Teixeira RR. As dimensões da produção do comum e a saúde. *Saúde Soc* 2015; 24 Suppl 1:27-43.
6. Quéau P. A revolução da informação: em busca do bem comum. *Ciência da Informação* 1998; 27:198-205.
7. Binenbojm G. Da supremacia do interesse público ao dever de proporcionalidade: um novo paradigma para o direito administrativo. *Revista do Direito Administrativo* 2005; 239:1-31.
8. Bennet B, Gostin L, Magnusson R, Martin R. Health governance: law, regulation and policy. *Public Health* 2009; 123:207-12.
9. Fairchild A, Gable L, Gostin LO, Bayer R, Sweeney P, Janssen RS. Public goods, private data: hiv and the history, ethics, and uses of identifiable public health information. *Public Health Rep* 2007; 122 Suppl 1:7-15.
10. Mooney SJ, Pejaver V. Big data in public health: terminology, machine learning, and privacy. *Annu Rev Public Health* 2018; 39:95-112.
11. McGrail KM, Gutteridge K, Meagher NL. Building on principles: the case for comprehensive, proportionate governance of data access. In: Gkoulalas-Divanis A, Loukides G, editors. *Medical data privacy handbook*. Cham: Springer; 2015. p. 737-64.
12. Pencarrick Hertzman C, Meagher N, McGrail KM. Privacy by design at Population Data BC: a case study describing the technical, administrative, and physical controls for privacy-sensitive secondary use of personal information for research in the public interest. *J Am Med Inform Assoc* 2013; 20:25-8.

Submitted on 31/May/2018
Approved on 06/June/2018