Serge Gutwirth
Ronald Leenes
Paul De Hert *Editors*

Reloading Data Protection

Multidisciplinary Insights and Contemporary Challenges

Springer

Reloading Data Protection

Serge Gutwirth • Ronald Leenes • Paul De Hert
Editors

Reloading Data Protection

Multidisciplinary Insights and Contemporary Challenges

Springer

Editors
Serge Gutwirth
Law, Science, Technology
and Society (LSTS)
Faculty of Law and Criminology
Vrije Universiteit Brussel
Brussels, Belgium

Paul De Hert
Law, Science, Technology
and Society (LSTS)
Faculty of Law and Criminology
Vrije Universiteit Brussel
Brussels, Belgium

Ronald Leenes
Tilburg Institute for Law, Technology
and Society (TILT)
Tilburg University
Tilburg, Netherlands

ISBN 978-94-007-7539-8 ISBN 978-94-007-7540-4 (eBook)
DOI 10.1007/978-94-007-7540-4
Springer Dordrecht Heidelberg London New York

Library of Congress Control Number: 2013947601

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Foreword

On 23 January 2012, the European Commission presented its proposal for a new "Data protection package". With the new package, the Commission seeks to strengthen data protection for the European citizens and set a standard for the rest of the world. The proposal has indicated clear directions for the future of data protection on the agenda. These include a 'right to be forgotten', stricter rules regarding online profiling, and stronger sanctions for non compliance. Although the proposal clearly follows the avenue already taken with Directive 95/46/EC, it also introduces controversial new elements as well as uncertainty. And thus, as expected, the new and re-considered, directions put forward by the Commission have spurred and extensive highly challenging process of discussion, negotiation and lobbying in 2012 and 2013. At the time of writing this foreword (June 2013), the European Parliament is discussing the almost 4,000 amendments that were tabled as a result of these discussions and everyone in the field is eagerly awaiting the outcome of the parliamentary decision making.

The sixth annual CPDP conference, held in Brussels on 23–25 January 2013, was sharply influenced by the fresh release of the European Commission's new plans and proposals, and quite some attention was given to the new or reformulated concepts of the package. This "reloading" of data protection, or even its "rebooting", has given a boost to reflection and research on the subject. This book volume bears witness to this reloading of data protection.

The present book is one of the products of the sixth edition of the annual Brussels based international International Conference on Computers, Privacy and Data Protection. CPDP 2013, was held under the same title: *Reloading data protection*. The conference welcomed 750 participants at 'our' venue—the magnificent *Les Halles*, while another 1,200 people were reached through free public events organized in the evenings, also in Brussels. The 3 day conference offered participants 45 panels and several workshops and special sessions, with 199 speakers from academia, the public and private sectors, and civil society.

This volume brings together 16 chapters offering conceptual analyses, highlighting issues, proposing solutions, and discussing practices regarding privacy and data protection. The first section of the book, provides an overview of developments in data protection in different parts of the world. The second section focuses on one

of the most captivating innovations of the data protection package, namely how to forget and the right to be forgotten in a digital world. The third section proposes five chapters on a recurring, and thus, obviously still important and disputed theme of the CPDP-conferences : the surveillance, control and steering of individuals and groups of people and the still more performing tools (data mining, profiling, convergence) to realise those objectives, and this with illustrations from the domain of law enforcement and smart surveillance. The book concludes with five chapters that aim at increasing our understanding of the changing nature of privacy (concerns) and data protection.

The chapters in this volume stem from two tracks. Nine chapters (3, 4, 5, 10, 11, 12, 13, 14, and 15) originate from responses to the conference's call for papers and have thus already been presented during the conference. The remaining chapters (1, 2, 6, 7, 8, 9, and 16) were submitted by invited speakers in the months following the conference. All the chapters of this book have been peer reviewed and commented on by at least two referees with expertise and interest in the subject matter. Since their work is crucial for maintaining the scientific quality of the book we would explicitly take the opportunity to thank them, *ad nominatim*, for their commitment and efforts: Claudia Aradau, Petra Bard, Rocco Bellanova, Laurent Beslay, Diana Alonso Blas, Caspar Bowden, Ian Brown, Lee Bygrave, Johann Ças, Helena Carrapiço, Claudia Diaz, Rodrigo Firmino, Gus Hosein, Simone Fischer-Hübner, Catherine Flick, Marieke de Goede, Gloria González Fuster, Antonella Galetta, Seda Gürses, Dara Hallinan, Marit Hansen, Hans Hedbom, Hielke Hijmans, Gerrit Hornung, Julien Jeandesboz, Christopher Kuner, Eleni Kosta, Marc Langheinrich, Daniel Le Métayer, Tobias Mahler, Gary Marx, Lucas Melgaço, Charles Raab, Joseph Savirimuthu, Dimitra Stefanatou, Anton Vedder, John Vervaele and Tal Zarsky.

May this book meet the reader's expectations and contribute to the quality of the, today particularly actual and pertinent, debate about the next steps of the becoming of privacy and data protection.

Serge Gutwirth
Ronald Leenes
Paul De Hert

Contents

Contributors

Marion Albers is Professor of Public Law, Information and Communication Law, Health Law and Theory of Law at Hamburg University. She studied law, sociology and political science at the universities of Berlin and Bielefeld and received her Ph.D. in law with a thesis on crime prevention and provisions for prosecution. Her postdoctoral thesis (Habilitation) focused on questions of informational self-determination. She was assistant at the Federal Constitutional Court in Karlsruhe. From 2002–2005 she served as an expert in the Advisory Committee of the Bundestag (German Parliament) for Ethics and Law of Modern Health Care. Her main areas of research include Fundamental Rights, Information Law and Data Protection, Health Law and Biolaw, Police Law and Law of Intelligence Services, Theory and Sociology of Law. She is engaged in several, partly interdisciplinary projects dealing with legal aspects of privacy, data protection, biobanks and health data, surveillance problems or measures against the financing of terrorism.
e-mail: marion.albers@web.de

Colin Bennett received his Bachelor's and Master's degrees from the University of Wales, and his Ph.D. from the University of Illinois at Urbana-Champaign. Since 1986 he has taught in the Department of Political Science at the University of Victoria, where he is now Professor. From 1999–2000, he was a fellow at Harvard's Kennedy School of Government. In 2007 he was a Visiting Fellow at the Center for the Study of Law and Society at University of California, Berkeley. In 2010, he is Visiting Professor at the School of Law, University of New South Wales. His research has focused on the comparative analysis of surveillance technologies and privacy protection policies at the domestic and international levels. In addition to numerous scholarly and newspaper articles, he has published five books, including *The Privacy Advocates: Resisting the Spread of Surveillance* (The MIT Press, 2008), and policy reports on privacy protection for Canadian and international agencies. He is currently the co-investigator of a large Major Collaborative Research Initiative grant entitled "The New Transparency: Surveillance and Social Sorting."
e-mail: cjb@uvic.ca

Dr. Paul Bernal is a Lecturer in Information Technology, Intellectual Property and Media Law at the University of East Anglia Law School. His background is unusual for a legal academic: his original degree from Cambridge University was in

mathematics, he qualified as a Chartered Accountant and has worked in business and in the voluntary sector, working in mental health and criminal justice, before returning to academia. He has a Ph.D. from the LSE, based on research into data privacy and autonomy, and in particular the role of commercial data gathering in the internet as it develops. His current research is centred around privacy and human rights, particularly on the internet, and includes such elements as the role of communications surveillance, the interactions between businesses and governments in relation to data privacy, children's rights on the internet, and Data Protection reform. Paul also specialises in the burgeoning area of social media—both as an academic looking into the roles played by social networks and social networkers and the laws and practices that have an impact upon them, and as a personal, legal and political blogger and tweeter. blog: http://paulbernal.wordpress.com/, Twitter: @paulbernalUK
e-mail: P.A.Bernal@lse.ac.uk

Denis Butin is a postdoctoral researcher in the Privatics team at Inria (Lyon, France). His research currently focuses on security policy languages and accountability by design. He holds a Ph.D. in computer science from Dublin City University, where he worked on the application of formal methods to electronic voting protocol analysis. Earlier, he earned a Master,Äôs degree in mathematics and computer science at the University of Tours. He is involved with the Security chapter of the European FI-WARE project.
e-mail: mchicote@dc.uba.ar

Marcos Chicote is a research intern at Inria (Lyon, France). His areas of interest include software engineering, automatic program analysis and program verification and has broad experience in industrial software development. He holds a Master's degree in Computer Science from the University of Buenos Aires.
e-mail: denis.butin@Inria.fr

Liane Colonna is a second-year doctoral candidate at the Swedish Law and Informatics Research Institute located at Stockholm University. The working title of her research project is the "Legal Implications of Data Mining in the European Union and the United States." She is a member of the New York bar and has an LLM in European law from Stockholm University.
e-mail: liane.colonna@juridicum.su.se

Vlad Coroama is a postdoctoral researcher in the Center for Industrial Ecology, University of Coimbra, Portugal. For more than a decade, his research revolved around the relation between ICT and sustainability. While in recent years he focused on the environmental dimension, Vlad is also interested in the societal effects induced by an expanding ICT monitorisation of everyday life. Vlad holds a Ph.D. in Computer Science from the ETH Zurich, Switzerland. Vlad can be reached at vlad.coroama@dem.uc.pt
e-mail: vlad.coroama@dem.uc.pt

Els De Busser studied Law at Antwerp University and obtained an additional degree in Criminology and an Advanced Master's degree in European Criminology and Criminal Justice Systems from Ghent University, Belgium. From March 2001 to October 2009, she worked as a researcher and professor's assistant in the field of European Criminal Law at Ghent University, Institute for International Research on Criminal Policy where she defended her Ph.D. entitled 'EU internal and transatlantic cooperation in criminal matters from a personal data perspective. A substantive law approach' in May 2009. In November 2009, she joined the European Criminal Law section of the Max Planck Institute in Freiburg, Germany. Her research and publications focus on international cooperation in criminal matters and data protection.
e-mail: e.busser@mpicc.de

Paul De Hert is professor of law at the Faculty of Law and Criminology of Vrije Universiteit Brussel. He is the Director of the research group on Fundamental Rights and Constitutionalism (FRC) and senior member of the research group on Law, Science, Technology & Society (LSTS). Paul De Hert is also associated-professor Law and Technology at the Tilburg Institute for Law and Technology (TILT)
e-mail: Paul.de.hert@vub.ac.be

Danilo Doneda is a professor of Civil Law at the Law School of FGV Direito Rio and a researcher at the Centre for Technology and Society (CTS) in the same institution. He holds a Ph.D. in Civil Law from the State University of Rio de Janeiro with a thesis about data protection later published as a book, a Master degree from the same institution and a Law degree from the Federal University of Paraná. He also works in the Brazilian Ministry of Justice as General Coordinator for Market Studies and Monitoring at the National Department for Consumer Protection.
e-mail: danilo@doneda.net

Rachel Finn is an Associate Partner at Trilateral Research & Consulting since 2010. Her research expertise includes the social effects of surveillance; new surveillance technologies; surveillance and the law; crime, deviance and social control; risk and security; and identity-based social exclusion. She also conducts research on stakeholder engagement mechanisms and privacy impact assessment methodologies, and advises on ethics, policy and implementation. Rachel has published articles in peer-reviewed journals and is co-authoring a book for Routledge on the social impacts of 'new technologies' of surveillance. She has a Ph.D. in sociology from the University of Manchester, UK.
e-mail: rachel.finn@trilateralresearch.com

Antonella Galetta is Ph.D. researcher at Law, Science, Technology and Society (LSTS) of the Vrije Universiteit Brussel, Faculty of Law and Criminology. Her research interests focus on law, privacy, data protection, technology and surveillance studies. She is currently doing research in the framework of the FP7 project IRISS, Increasing Resilience in Surveillance Societies. She holds a B.A. in Law (University of Macerata), a M.A. in European and International Studies (University of Trento)

and a M.A. in International Relations (University of Bologna). She has working experiences at the European Parliament and European NGOs.
e-mail: antonella.galetta@vub.ac.be

Dorota Głowacka Lawyer at the Helsinki Foundation for Human Rights, Poland dealing with freedom of expression and right to privacy issues. Coordinator of the HFHR's 'Observatory of Media Freedom in Poland' programme. Ph.D. candidate at the Public International Law Department, Law Faculty, University of Lodz, Poland.
e-mail: d.glowacka@hfhr.org.pl

Serge Gutwirth is a professor of human rights, legal theory, comparative law and legal research at the Faculty of Law and Criminology of the Vrije Universiteit Brussel.(VUB), where he studied law, criminology and also obtained a postgraduate degree in technology and science studies. Gutwirth founded and still chairs the VUB-research group Law Science Technology & Society (http://www.vub.ac.be/LSTS). He publishes widely in Dutch French and English. Amongst his recent co-edited publications are *Safeguards in a world of ambient intelligence (Springer, 2008), Profiling the European citizen* (Springer 2008), *Reinventing data protection?* (Springer 2009), *Data protection in a profiled world* (Springer, 2010) and *Computers, privacy and data protection: an element of choice* (Springer, 2011) and European Data Protection: in good health? (2012). Currently, Serge Gutwirth is particularly interested both in technical legal issues raised by technology (particularly in the field of data protection and privacy) and in more generic issues related to the articulation of law, sciences, technologies and societies.
e-mail: serge.gutwirth@vub.ac.be

Beata Konieczna Researcher and lecturer of the Faculty of Law and Administration at the University of Cardinal Stefan Wyszyński University in Warsaw, Poland. A member of the Board of the Legal—Information Scientific Center. Research interests are: personal data protection, computerization of public administration. The author of scientific articles devoted to protection of personal data.
e-mail: beata-konieczna@wp.pl

Paulan Korenhof is a Ph.D. student at the Tilburg Institute for Law, Technology and Society (TILT, Tilburg University) and Privacy & Idenity Lab (PI.Lab, a collaboration between Radboud University, SIDN, Tilburg University and TNO). As part of PI.Lab she works as a guest researcher at the digital security department of the Radboud University. She holds a masters degree in both Public Law and Philosophy. Paulan focuses her research on the problems that are associated with the so-called "Right to be Forgotten" by looking at them from a meta-perspective.
e-mail: p.e.i.korenhof@tilburguniversity.edu

Marc Langheinrich is an assistant professor in the Faculty of Informatics at the Università della Svizzera Italiana (USI) in Lugano, Switzerland, where he heads the Research Group for Ubiquitous Computing. Marc received his Ph.D. in Computer Science from the ETH Zurich, Switzerland, in 2005 with his work on "Privacy in Ubiquitous Computing". Marc is one of the authors of P3P, a W3C-standard for

privacy on the Web, and has published extensively on privacy aspects of ubiquitous and pervasive computing systems. Marc can be reached at langheinrich@acm.org
e-mail: langheinrich@acm.org

Ronald Leenes is professor in Regulation by Technology at TILT, the Tilburg Institute for Law, Technology, and Society (Tilburg University). His primary research interests are privacy and identity management, regulation of, and by, technology. He is also involved in research in ID fraud, biometrics and robotics. Ronald has worked on several EU projects in the privacy and identity domain, such as the EU FP6 PRIME project, EU FP7 PrimeLife and A4Cloud. He has co-edited numerous volumes on privacy and identity-management, including Digital Privacy: PRIME - Privacy and Identity Management for Europe (2011), Computers, privacy and data protection: an element of choice (Springer, 2011), European Data Protection: in good health? (Springer 2012), European Data Protection: Coming of Age (Springer 2013).

Daniel Le Métayer is Research Director for Inria (the French National Institute for Research in Computer Science and Control) and head of the Inria Project Lab CAPPRIS. CAPPRIS is an interdisciplinary initiative involving seven research teams working on various aspects of privacy. From 2000 to 2006, Daniel Le M√©tayer worked for Trusted Logic, a leading company in security and open middleware for embedded systems. Daniel Le Métayer has been involved in various international projects on IT security, software design and analysis, testing, etc. He has also served on programme committees of many IT international conferences and he has been the editor of special issues of computer science journals such as ACM Transactions on Software Engineering and Theoretical Computer Science.
e-mail: daniel.le-metayer@inria.fr

Laura Schertel Mendes is a Ph.D. candidate at the Humboldt University of Berlin, under the supervision of Prof. Stefan Grundmann, with a scholarship of the German Academic Exchange Service (DAAD). Her research addresses data protection in the private sector, focusing the problem of consent. She holds a Law Degree and a Master of Law from the University of Brasilia, Brazil. She worked from 2007 to 2010 in the Brazilian Ministry of Justice as General Coordinator for Market Studies and Monitoring at the National Department for Consumer Protection.
e-mail: lauraschertel@hotmail.com

Adam Molnar is a Ph.D. candidate in the Department of Political Science at the University of Victoria and a Researcher with the New Transparency project. His research interests focus on the legal, normative, and technical dimensions of digitally mediated surveillance and privacy, particularly in the areas of policing, national security, and public safety governance. His dissertation focuses on the legacies of security and policing operations associated with major sporting events, with an empirical focus on current trends in national security, including public order policing, civilian-military relations, disaster management, and a range of applications of surveillance technologies in contemporary policing.
e-mail: apm@uvic.ca

Anthony Morton is a Research Student in the Information Security Research Group at the Department of Computer Science, University College London (UCL), UK. He commenced his Ph.D. in 2010, having gained an M.Sc. in Information Security at UCL. He is a Chartered Engineer through the British Computer Society, and also has an MBA in Technology Management, an M.Sc. in Computing for Commerce and Industry and an M.A. in Classical Studies, all from The Open University. His Ph.D. research focuses on the influence of the privacy behaviour of technology services—consisting of a technology platform and providing organisation—on the construction of peoples' privacy concerns. Prior to commencing his studies at UCL, he was employed in the IT industry for 25 years in software development, technical management and consultancy roles.
e-mail: anthony.morton.09@ucl.ac.uk

Nóra Ní Loideain B.A., L.L.B., L.L.M. (Public Law) is a Ph.D. candidate and CHESS scholar at the Faculty of Law in the University of Cambridge. Her doctoral thesis concerns the Data Retention Directive (2006/24/EC), specifically the surveillance of communications data by law enforcement authorities and the right to respect to private life and correspondence in Europe. She has previously worked as a Legal Research Officer in the Office of the Director of Public Prosecutions and as a Judicial Researcher for the Supreme Court of Ireland. Her main research interests and publications are in the fields of EU law and policy-making; civil liberties and human rights, particularly under the EU and ECHR systems; and data protection.
e-mail: nl301@cam.ac.uk

Christopher Parsons is a doctoral candidate at the University of Victoria, Canada. Christopher's research, teaching, and consulting interests involve how privacy is affected by digitally mediated surveillance, and the normative implications that such surveillance has in (and on) contemporary Western political systems. His current research streams examine how and why Internet service providers use deep packet inspection technologies, the privacy and policy challenges raised by social media network communications, and difficulties concerning the use of electronic identity cards to access government services. In addition, he has published in the Canadian Journal of Law and Society, European Journal of Law and Technology, Canadian Privacy Law Review, CTheory, and has book chapters in a series of academic and popular books and reports. Christopher is a Ph.D. Candidate in the Department of Political Science at the University of Victoria, a Privacy by Design Ambassador and a Principal at BlockG Privacy and Security Consulting.
e-mail: Christopher@Christopher-Parsons.com

Wouter M.P. Steijn has graduated Developmental Psychology at Leiden University and is now a Ph.D. candidate at Tilburg Institute for Law, Technology, and Society at Tilburg University and partner of the Privacy & Identity Lab. His research is part of the multi-disciplinary project "Social dimensions of privacy" and investigates individuals' behaviour on social network sites and their privacy attitudes and conceptions. A special point of interest is age related differences.
e-mail: w.m.p.steijn@uvt.nl

John Vervaele is full time professor of economic and European criminal law at Utrecht Law School (the Netherlands) and professor of European criminal law at the College of Europe in Bruges (Belgium). He is vice-president of the AIDP, in charge of the scientific coordination of the world organization for criminal law. His scholarly work is dealing with collar crime and economic offences and European criminal law and procedure. The main topics in his research field are: enforcement of Union law; standards of due process of law, procedural safeguards and human rights; criminal law and procedure and regional integration; comparative economic and financial criminal law; terrorism and criminal procedure. He has realized a lot of research in these areas, both for Dutch Departments and European Institutions and worked as well as a consultant for them. He is regularly teaching as visiting professor in foreign universities, in Europe, the US, Latin America and China.
e-mail: J.A.E.Vervaele@uu.nl

David Wright is Managing Partner of Trilateral Research & Consulting, a London-based limited liability partnership, which he founded in 2004. Trilateral specialises in privacy, data protection, surveillance, security, risk and foresight issues. He has initiated and organised many successful consortia for European projects. Among recent projects is one on privacy and risk management for the UK Information Commissioner's Office. Another concerns privacy seals for the Institute for the Protection and Security of Citizens (IPSC) in Italy. He has published many articles in peer-reviewed journals. His most recent book is Privacy Impact Assessment, published by Springer in 2012.
e-mail: david.wright@trilateralresearch.com

Gabriela Zanfir holds an L.L.M. in Human Rights, obtained at the University of Craiova (Romania). She is currently a Ph.D. candidate at the same university, writing a thesis about the rights of the data subject in EU data protection law, with a focus on Romanian law. She is especially interested in the civil law mechanisms of protection of these rights and in conceptualizing the right to the protection of personal data as droit subjectif. Her research interests recently extended to cloud computing regulation. She was a visiting researcher for three months in 2012 at the Tilburg Institute for Law and Technology (The Netherlands). She is also a Teaching Assistant for the property law and torts courses.
e-mail: gabriela.zanfir@gmail.com

Part I
Data Protection in the World: Brazil and Poland

Chapter 1
Data Protection in Brazil: New Developments and Current Challenges

Danilo Doneda and Laura Schertel Mendes

1.1 Introduction

In the twentieth century, few legal concepts have transformed as much as that involving the right to privacy. The concept departed from discussions about the violation of privacy of celebrities photographed in embarrassing or intimate situations and reached discussions on massive data processing of millions of citizens by public and private entities through modern information technologies.[1] In this context, Stefano Rodotà affirms that privacy has been reinvented in the twentieth century, since this right has come to involve concepts such as transparency and control of personal data (beyond the right to be let alone and the notion of confidentiality), inducing the development of the right to data protection.[2]

This transformation has been observed since the 1970s in national data protection laws and in international treaties and agreements on the matter.[3] This legislative production started in Europe and North America as a response to the rise of electronic data collection and processing by governments and large companies.[4] Since then, technology and data protection laws have evolved, and the geographic boundaries of

[1] Simitis (1987, p. 709).
[2] See Rodotà (2008, p. 15).
[3] Regarding transnational policy instruments on data protection, including, e.g., Convention 108 of the Council of Europe, the Guidelines of the Organization of Economic Cooperation and Development (OECD), the Directive 95/46/EC of the European Union, see Bennett and Raab (2006, p. 83–115).
[4] Mayer-Schönberger (2001, p. 221).

D. Doneda (✉)
FGV Direito Rio-Praia de Botafogo,
190-13° andar-CEP 22250-900-Rio de Janeiro, RJ, Brazil
e-mail: danilo@doneda.net

L. S. Mendes
Humboldt-Universität zu Berlin,
Juristische Fakultät (Lehrstuhl für Bürgerliches Recht, Deutsches-,
Europäisches- und Internationales Privat- und Wirtschaftsrecht),
Unter den Linden 6, 10099, Berlin
e-mail: laurascherte l@hotmail.com

S. Gutwirth et al. (eds.), *Reloading Data Protection,*
DOI 10.1007/978-94-007-7540-4_1,

data protection legislation have spread throughout the world.[5] It is clear today that the new frontiers are regions such as Asia and Latin America, where in the last decade several countries have updated their legislation to incorporate some degree of protection of personal data.

In Brazil, the concept of privacy and the instruments for its protection have undergone constant development in recent years by both courts and legislatures, to deal with the challenges of data processing. Although Brazil does not have a general data protection law as do several South American countries, a data protection framework is being developed from various elements such as the privacy rights provided in the Brazilian Constitution or several statutes that deal directly with personal data.

In fact, data protection is increasingly becoming a matter of autonomous regulation in Brazil, in relation to the constitutional right to privacy, what can be seen as a turning point in this matter. That is, more and more conflicts regarding data processing are being considered within a framework of transparency and control, rather than a privacy framework, which emphasizes opacity and confidentiality. This is due to the recent developments of the case law, the enforcement efforts of public authorities and the new acts issued in 2011 (i.e., the Credit Information Law and the Access to Information Law), which are the object of analysis of this paper.

As a consequence, one can observe the coexistence of two kinds of legal tools that deal with the flow of information in the Brazilian legal system, that is, privacy tools and data protection tools, in the words of Paul de Hert and Serge Gutwirth.[6] This paper concentrates on the data protection framework in Brazil, from its foundations to new developments, examining perspectives for further evolution and challenges to be faced. Rather than conduct a static analysis,[7] we aim to discuss the direction in which the Brazilian data protection framework is evolving.

The goal of this paper is, therefore, to analyze how data protection is guaranteed in Brazil, considering the recent development of new instruments and laws. The analysis is organized in three steps: (1) The first part addresses the foundations of data protection in Brazil, in particular, the constitutional provisions and the consumer protection code; (2) The second part addresses the new developments of data protection laws and instruments in the last years, particularly, the Credit Information Law and the Access to Information Law; (3) The third part analyses the challenges of guaranteeing data protection in Brazil and the tasks that must be carried out to improve data protection in the country.

---

[5] For an overview of the data protection legislation in the world, since the 1970s, see Table 5.1 "The diffusion of data protection legislation by region" in Bennett and Raab (2006, p. 127).

[6] According to them, privacy tools and data protection tools are complementary: while the former focuses more on opacity, the latter emphasizes control and transparency. See De Hert and Gutwirth (2006).

[7] Highlighting the non static feature of privacy and data protection, even within a more or less stable legal framework (e.g. the Data Protection Directive of 1995): Gutwirth et al. (2011), p. v.

1.2 Foundations of Data Protection in Brazil

A legal framework for data protection in Brazil has been developed from constitutional grounds up to specific legal measures in the last decades. Among several other sets of legislations that, in various ways, foresee some extent of generic privacy provisions, we will focus on the roots of the Brazilian data protection framework, based both on its constitutional grounds, and on the Consumer Protection Code.

1.2.1 Constitutional Protection and the Habeas Data Writ

The Brazilian Constitution directly addresses issues regarding information by providing for the fundamental rights of freedom of expression[8] and access to information and transparency.[9] In addition, it acknowledges the inviolability of private life and privacy[10] and also of telephonic, telegraphic and data communications,[11] and establishes that the home is the holy and inviolable refuge of the individual.[12] Furthermore, it provides for the writ of habeas data,[13] which gives citizens a way to access and correct data about themselves held by third parties.

The writ of habeas data was originally introduced in Brazil's 1988 Constitution and has since influenced several other Latin American countries to adopt similar provisions, to the extent that it was, at some point, taken as the root of a new Latin American data protection framework.[14] Habeas data also bears resemblance to the inscription of rights regarding privacy, data protection and computers in the new constitutional charts of two European countries that also were transitioning back to democracy in the 1970s after a period of dictatorship, i.e., Portugal and Spain.

The essence of Brazil's habeas data writ is to provide citizens with a tool to access and correct personal information stored by public bodies. It has been considered, as its legislative process indicates, to be an instrument much needed in the political situation in which it arose, when Brazil (like several countries in the region) was in transition to a democratic political regime.[15] At this time citizens needed a tool to access information that the military dictatorship had gathered about them,[16] and the habeas data was envisaged as this instrument. This means that the main inspiration for Brazil's writ of habeas data wasn't the legal framework about data protection

[8] Art. 5°, IX; art. 220, Federal Constitution.

[9] Art. 5°, XIV; Art. 220; Art. 5°, XXXIII; Art. 5°, XXXIV, Federal Constitution.

[10] Art. 5°, X, Federal Constitution.

[11] Art. 5°, XII, Federal Constitution.

[12] Art. 5°, XII, Federal Constitution.

[13] Art. 5°, LXXII, Federal Constitution.

[14] See Pulcinelli (1999); Guadamuz (2000).

[15] See Barroso (1998, p. 211). See also Dallari (1997, p. 72), Barbosa Moreira (1998, p. 127).

[16] Stella Calloni. "Los archivos del horror del operativo Condor", in: <www.derechos.org/nizkor/doc/condor/calloni.html>.

that several European nations had developed by that time nor the U.S. legal privacy tradition, but rather the mentioned requirements of the country's political moment.[17]

In fact, habeas data was not proposed as a modern data protection tool nor did it develop into one over time. It is a relatively costly and slow writ—it must be presented by a lawyer and only after the plaintiff has already requested the data directly from the defendant without success. Instead of adapting habeas data to a more dynamic environment, other instruments were developed in Brazilian law to address the increase of electronic data processing.

1.2.2 Ensuring Data Protection Through the Consumer Protection Code

Although the Brazilian Constitution recognizes a variety of privacy rights as well as the habeas data writ, as seen above, data protection, in a modern sense, initially emerged in Brazil as a consumer protection issue. In fact, the Consumer Protection Code (Law 8.078 of 1990) provided a multifaceted framework in which privacy and data protection demands could develop and be addressed. As the evolution of the issue in other countries reveals, the right to data protection tends to emerge in those legal fields that are more likely to welcome the new social demands. This task fell in Brazil to the Consumer Protection Code, since it entails a variety of principle-based norms, which are broad enough to offer solutions to new conflicts related to information technology.

Consumer protection plays a central role in Brazil's legal system. The Consumer Protection Code was enacted to balance the information and power asymmetries between consumers and traders.[18] It establishes norms regarding private, procedural and criminal law, as well as provides for an administrative structure for the enforcement of consumer rights. Moreover, it organizes a National Consumer Protection System, to coordinate the more than 600 public bodies responsible for consumer protection at the federal, state and local levels, which operate as an extrajudicial dispute resolution structure. Nonetheless consumers can also seek redress in the judicial system, particularly in small claims courts.

The recognition of consumer protection as a constitutional matter is central to the Brazilian legal system. Article 170, V, of the federal Constitution foresees consumer protection as a principle of the economic order and Art. 48 of its temporary provisions stipulates an obligation of enacting a Consumer Protection Code. The Constitution establishes, moreover, in its chapter of fundamental rights that "the State shall promote, as provided by law, consumer protection" (Art. 5°, XXXII). This norm implies not only a subjective right, but also a duty to protect,[19] which is directed to the state as a whole—the executive, legislative and judiciary branches. The duty to protect can involve, for instance, the duty to interpret law, taking into

[17] Doneda (2006, p. 328).

[18] Marques et al. (2006, p. 33).

[19] Concerning the concept of the fundamental right as being the duty of the state to provide protection, see Pieroth and Schlink (2005, p. 23).

account the vulnerability of consumers and their need for protection, or the duty of the state to develop a regulatory system to protect consumers.[20]

Four pillars of the Brazilian consumer protection system explain how it could promote and enforce data protection standards: (a) specific regulations for consumer databases that address the rectification and notice process; (b) a broad clause governing damage claims (overall liability); (c) a public consumer redress structure, which includes both an administrative and a judicial system of redress (small claims courts); and (d) a broad conceptualization of who are consumers.

The Consumer Protection Code establishes, in its Art. 43, specific rights and safeguards regarding personal information stored in databases, namely: (a) consumers shall have access to all the personal information stored on databases (right of access); (b) all stored data shall be objective, accurate and in a comprehensible language (principle of data quality); (c) consumers shall be notified, through written communication, before the storage of any negative personal information (principle of transparency); (d) the party responsible for the database shall immediately promote the rectification or cancellation of any inaccurate data that is being stored (right of rectification and implicitly justified cancellation[21]); and (e) the time limit for storage of negative personal data is 5 years (right to forget). This norm, which was inspired by the U.S. Fair Credit Reporting Act,[22] clearly has many similarities with the fair information principles of data protection.[23]

These data protection standards provided by Article 43 gain relevance when associated with the general clause of overall strict liability established by Article 6, VI, and Article 14, of the Consumer Protection Code. In fact, courts have recognized a broad right to compensation, for instance, when negative personal data about a consumer is stored without previous notification or when a consumer's application for credit is refused, based on incorrect data. Since the Brazilian judicial system has a variety of small claims courts, which facilitate consumer litigation and dispense the need for hiring a lawyer, this single norm had a huge impact on the legal system. Furthermore, consumers may register their complaints against credit information databases at the Public Consumer Protection Bodies, which will handle the individual complaint through an extra-judicial conciliation procedure. The National Register of Consumer Complaints in Brazil (SINDEC) recorded in the year 2012 more than 20,000 complaints about problems regarding the inappropriate storage or processing of credit information.[24]

Finally, the Brazilian Consumer Protection Code establishes a broad concept of consumer, which allows its application in a variety of cases, beyond the strict

[20] Pieroth and Schlink (2005, p. 23).

[21] Gambogi Carvalho (2003, p. 77–119).

[22] See Herman Benjamin et al. (2005, p. 400).

[23] In a comparative study of the data protection policies of four countries (Sweden, the United States, West Germany and the United Kingdom), Bennett systematizes the Fair Information Principles in six principles: openness, individual access and correction, collection limitation, use limitation, disclosure limitation and security. See Bennett (1992, p. 101).

[24] The total of registers in the year 2012 was 2.031.289. The National Register of Consumer Complaints in Brazil (SINDEC) is a public database and can be accessed through the website: http://portal.mj.gov.br/sindec/.

contractual relation between consumers and traders. The conceptualization of consumer in the Code comprises four definitions: (a) according to the standard definition, consumer is any physical person or corporate entity who acquires or uses a product or service as a final user (Art. 2°): (b) consumer is also a collectivity of persons who participate in consumer relations (Art. 2, § 2°); (c) consumer is, furthermore, anyone who has suffered damages caused by a commercial activity (Art. 17) and (d) any person who is exposed to a commercial practice, such as advertising or databases is also considered a consumer (Art. 29).[25] This means that if any of these definitions fits the case, the Consumer Protection Code is applied.

For this reason, a person doesn't need to prove any contractual relation to exercise his rights to correction and disclosure of his personal information against a database. Furthermore, this means that consumer damage claims can be directed not only against the firm with which he has a contract, but also against the party responsible for the database. That is why the data protection norms of the Consumer Code have had a much broader application than the strict relation between consumers and traders, promoting a modernization that extended beyond consumer relations.[26]

1.3 New Developments in the Brazilian Data Protection Framework

As seen above, the Brazilian legal system has a variety of privacy and data protection instruments, found in both the Constitution and ordinary laws. While the Constitution provides, in addition to the habeas data writ, many confidentiality guarantees (inviolability of home, private life and privacy as well as the confidentiality of correspondence, and telephonic, telegraphic and data communications), the Consumer Protection Code establishes a specific data protection norm, based on the concept of notification, rectification and compensation. Although they play an important role in protecting privacy, some of these instruments were found to have limitations and needed to be complemented to meet new challenges and problems. Against this background, one can understand the recent developments in the Brazilian data protection system, namely the Credit Information Law and the Transparency Act, both issued in 2011.

1.3.1 The Credit Information Law

The Credit Information Law (Law 12.414 of 2011) aims to regulate credit information systems, especially, borrowers' payment histories. Under the Consumer Protection Code, there was no doubt about the lawfulness of recording "negative" data about a

[25] Marques (2011, p. 385, 386).

[26] Tepedino (1999, p. 199–216).

consumer, that is, information about consumer default. There was, however, legal uncertainty about storing borrowers' payment histories ("positive information"). It was therefore important for the Credit Information Law to provide detailed regulations concerning credit information databases, thus establishing a secure legal framework that simultaneously encourages data flow and protects personal data. Given the size and complexity of the law, and its accompanying regulation (Decree 7.829 of October 2012), it is not possible to analyze all its rules in detail. Rather, we will examine the main principles and norms, concerning data protection rights.

In summary, it can be said that this law established a variety of rules ranging from the creation of a payment history to the establishment of responsibilities in case of damages, determining, for instance, when a payment history can be created (Art. 4), what information can be stored (Art. 3, § 2 and § 3), what are the rights of the data subject (Art. 5), what are the duties of the data processor (Art. 6), who supervises the databases (Art. 17) and who is liable in case of damages (Art. 16). Regarding the type of its norms, one could say that the Credit Information Law corresponds to a typical U.S. regulation issue, i.e., credit reporting, although it has a European form. As we will see, many of its norms correspond to the principles provided in Convention 108 of the Council of Europe and in the European Directive 95/46/EC.

The key principle of the Credit Information Law is that the consumer should have control over his personal information and, therefore, over the creation and use of his payment histories. In this sense, the law grants the consumer power over the creation, transference and cancellation of his credit history. Consumer consent is, hence, the touchstone of this framework, as provided by Article 4. Furthermore, according to Article 5, consumers shall obtain the cancellation of the record upon request and, as determined by Article 9, the sharing of information is permitted only if expressly authorized by the consumer. As seen, the main goal of the act is to grant consumers control over the flow of personal information in the market.

Like the Consumer Protection Code, the Credit Information Law establishes the principle of quality or accuracy of personal data (Art. 3, § 1), as well as the rights to the access, rectification and cancellation of data (Art. 5, II and III). Furthermore, it grants the consumer access to the main criteria used in the credit rating process, that is, the consumer has the right to know the criteria upon which a calculation of credit risk is based (Art. 5, IV). In relation to risk assessment, the act grants consumers the right to ask for a review of any decision made exclusively by automated means (Art. 5, VI). This rule is comparable to Article 15 of the European Directive 95/46/EC[27] and aims to ensure the possibility of human intervention in a process of making decisions that can significantly affect his or her life.

A very important improvement made by the Credit Information Law was to provide an explicit legal basis for the purpose limitation principle in the Brazilian system, which was already implicit under the Consumer Protection Code. As established by

[27] According to Art. 15 of the Directive 95/46/EC, "Member States shall grant the right to every person not to be subject to a decision that produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc."

the act, the principle of finality permeates the entire credit information system. Firstly, the act defines the strict scope of its application, which are solely databases related to risk assessment in credit and commercial transactions (Art. 2, I). Secondly, it establishes the right of the data subject to have the processing of personal information limited to the original purposes of collection (Art. 5, VII). Thirdly, Article 7 describes the purposes for which the data collected under this act can be used: either to conduct risk analysis or to assist decisions regarding the granting of credit or other commercial transactions that involve financial risk. This implies that these databases cannot be used for direct marketing or any other activity not mentioned in the law. In this context, one notices another similarity to the European Directive, particularly Article 6, 1, b, which determines that personal data should be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."

A key rule of the Credit Information Law is the prohibition against storage of sensitive and excessive information, as provided by Article 3, § 3. According to the act, excessive information is that which is not related to the credit risk analysis. The act describes as sensitive information that related to social and ethnic origin, health, genetic information, sexual orientation and political, religious and philosophical beliefs. This prohibition is based on the fact that the processing of some types of information can lead to discrimination, violating the principle of equality. Therefore, it is possible to make another parallel to the European Directive, namely, Article 8, which concerns the processing of special data categories.

Furthermore, the Credit Information Law stipulates a system of strict liability, in which all material and moral damages must be repaired (Art. 16), without needing to prove negligence or fault. This rule is in accord with the liability clause of the Consumer Protection Code and relies on the concept that the liability arises from the risk of the activity.

Finally, an important concept endorsed by the act is the need for data processing to be controlled by an administrative authority. Rather than creating an authority to fulfill this function, the Credit Information Law designates the existing public consumer protection bodies, at the federal, state and local levels, as responsible for the supervision (Art. 17). Moreover, it establishes that the administrative penalties provided by the Consumer Protection Code shall be applied as well. Both provisions are only to be applied when the data subject qualifies as a consumer.

1.3.2 The Access to Information Law

Although the 1988 Brazilian Constitution established transparency as a principle for public administration and granted every citizen the right to access information from public bodies[28], the statute that created the procedures for this access only entered into force in 2012.

[28] Art. 5°, XIV; art. 5°, XXXIII; art. 5°, XXXIV, Federal Constitution.

The Access to Information Law (Law 12.527 of 2011) regulates the general constitutional rules regarding this issue and was drafted to respond to a particular need: to define rules for the treatment of personal information processed by public bodies. Its main goal was, of course, to grant free access to public information, which includes a considerable amount of personal information that can be classified as such. Since there was no general rule for the specific protection of personal information in other statutes (although this protection can be derived from constitutional principles), the Access to Information Law had to include a specific topic about protection of personal data held by public bodies.

Protection of personal data in this law basically comprehends that data concerning a particular individual shall not be disclosed to third parties who have sought access to the information. However, such information can be disclosed if the data subject has provided consent, if the data was produced more than 100 years before the access request, or if it qualifies for one of the exemptions (in case of health requirements, relevant public research, in compliance with a warrant, is needed for the protection of human rights or in a case of preponderant public interest).

The legal basis mentioned by the law for protecting personal data is also particularly relevant. For the first time in the Brazilian legal system, the treatment of personal information was directly related not only to the protection of privacy but was also seen as a means to ensure individual freedom in general. In this sense, Brazilian law contemplated for the first time a modern and general statement of the data protection principles tied to individual freedoms in a broader sense—something that the habeas data writ, even with its genealogy, has never attained.

Looking more closely at Article 31 of the Access to Information Law (the article that deals with personal data), it becomes evident that the law treats the protection of personal data as secondary to the disclosure of information. This can be inferred both from the broad nature of the exemptions for the free access to personal data and from the lack of other specific measures for its protection (for example, sensitive personal data has no special level of protection).

The architecture of data protection present in the access to information law is no more than that strictly necessary for the harmonization of the access to information—which is the purpose of the statute—and the protection of personal data, considering that without some form of mandatory protection of personal data the statute could be found to be seriously lacking compliance with constitutional provisions. Even so, the secondary nature of the data protection provisions in this statute and the importance the regulation of personal data plays in the complete legal framework for information demonstrate the need for specific measures regarding personal data protection to be found outside the Access to Information Law.

Nevertheless, the access to information law has made a concrete contribution to the Brazilian data protection framework, and not only because of the specific provisions of its Article 31. The statute, by creating a simple process with time limits to order a public body to produce information after a request is made, has also developed an instrument that makes it easier for citizens to request their own personal information from public bodies, without the burden or inconvenience that could be faced if the request were made by general administrative means (which

would lack the specific enforcement of the access to information law) or through a writ of habeas data (which, among other drawbacks, would require a lawyer).

This is a potential intersection between access to information and data protection statutes, which, according to David Banisar, is often used in countries that have no specific law to deal with personal information but have some kind of access to information mechanism or, in countries that have both statutes but in some way filter or adapt the access to personal information requirements to the access to information framework.[29]

1.4 Current Challenges of Guaranteeing Data Protection in Brazil

As analyzed in the previous section, new developments in ordinary law have complemented the legal foundations of data protection in Brazil, improving the instruments for dealing with data processing problems in the country. Nonetheless, there are still many challenges to be faced to adequately respond to the risks arising from data processing in a network society. These challenges can be divided into two categories: on the one hand, there are challenges related to enforcement, since there is already a data protection framework that needs to be implemented; on the other hand, there are regulation issues, since there is a lack of legislation in some areas, which must be addressed by the Congress.

1.4.1 Enforcement: The Role of the Judiciary and of the Consumer Protection Bodies

A systematic interpretation of the Consumer Protection Code and the Credit Information Law builds a framework for data protection in Brazil's private sector. A key element of this framework is the broad concept of consumer established by the Consumer Protection Code, so that its application is not limited to the person who acquires or uses a product or service as a final user, but applies to anyone who is exposed to a commercial practice or who has suffered damages caused by a commercial activity.[30]

Against this background, it is possible to outline the principles and procedures that private data controllers must meet, to comply with the data protection system in Brazil: (1) Transparency: all processing of personal data shall occur in a transparent way. Data controllers must assure that the data subject knows about the purpose of the collection and the use of the data, the kind of data being processed, and the identity of the data controller; (2) Control of personal information: a central element of data

[29] Banisar (2011).

[30] See Sect. 2.2.

protection is that the data subject should have control of his personal information. Consent is, therefore, the legal instrument that materializes this control and may be limited only in exceptional circumstances; (3) Purpose limitation principle: any processing of personal data must comply with the context in which data are collected. Thus, information collected for one purpose cannot be further processed in a way incompatible with those purposes; (4) Guarantee of the rights to access, rectification and cancellation: the data subject shall have free access to his data, should be able to rectify inaccurate and outdated information and should be able to cancel data that was stored improperly; (5) Special protection for sensitive data: personal information that could generate consumer discrimination should have stronger protection, such as data concerning religious and political choices, sexual preference, race, health and genetic data.

As can be seen, a framework exists for data processing in the Brazilian private sector, which corresponds to the main concepts of the Fair Information Principles, Convention 108 of the Council of Europe and Directive 95/46/EC. A current challenge in this field is, therefore, to enforce the existing norms, in order to guarantee protection for the data subject. There are many actors that are responsible for the implementation of data protection norms.

Primarily, the courts play an important role in this enforcement, interpreting and applying data protection instruments and concepts. In fact, a qualitative analysis of the Brazilian case law on data protection indicates that the decisions of the courts are moving from a strict view of the credit information issue to a broader perspective, in which the processing of personal data is understood as a general risk to a citizen's personality.[31] Two cases can illustrate this shift.

Well-known in this context is a 1995 decision of the Superior Court of Justice, under the leading opinion of the rapporteur, Minister Ruy Rosado de Aguiar, concerning time limitation for the storage of personal data. The court is the highest jurisdiction for non-constitutional cases in Brazil. In this case, the court decided that credit records about consumer default could not be stored for more than 5 years, as provided by the Consumer Protection Code, and not for 20 years, the period in which the debts prescribe, according to the Civil Code.[32] In this decision, the Court extended its analysis to the risks of the processing of personal data in general and not only to the credit reporting activity. This case was an innovation in Brazilian case law, because it drew attention to the risks arising from the data processing activity, by both the public and private sectors.

In recent years, issues concerning data protection on the Internet have entered the courts and compel the courts to find adequate solutions within the existing framework. A recent decision of the Superior Court of Justice, concerning a disclosure of a picture on a website, indicates how the problem of data protection on the Internet is increasingly gaining relevance in the Brazilian legal system. In this case, the court decided that the company that controlled the website was liable for the misuse of the

[31] Mendes (2011, p. 54).

[32] STJ, REsp 22.337–9/RS, 4.ª T., j. 13.02.1995, v.u., rel. Min. Ruy Rosado de Aguiar, DJ 20.03.1995

image and had to pay compensation for material and moral damages.[33] Central to the decision was the opinion of the rapporteur, which discussed the new challenges posed by the Internet to the legal system and recognized that technological innovations gave rise to the development of a new concept of privacy, based on the control of personal information by the individual.

In addition to the judiciary, the executive branch also has a very important role in enforcing data protection rights in the private sector. As mentioned before, Brazil's Consumer Protection System comprises more than 600 public bodies, at the federal, state and local levels. The Consumer Protection Code grants all of them the same legal powers, which range from receiving consumer complaints to applying administrative penalties to the companies, in case of non-compliance with the law.[34] Although there is no hierarchy among these public bodies, the National Secretary of Consumer Protection, which is part of the Ministry of Justice, performs the political coordination of the system.[35]

In fact, data protection is becoming an issue of public policy in Brazil and the consumer protection bodies are taking actions to enforce data protection rights within the existing framework. One interesting step, for instance, was the creation of a "do-not-call registry" in many states.[36] In São Paulo, the registry was created by a state law, which made the consumer protection body (Procon São Paulo) responsible for its management and supervision.[37] Furthermore, the National Secretary of Consumer Protection is working at many levels to enforce data protection rights of consumers. It published, for instance, a study on consumer right to data protection in Brazil, as an effort to stimulate discussion on this issue[38] and added data protection as a subject of the training courses to the staff of the consumer protection bodies.[39] Concerning the supervision activities, it has the power to investigate practices, which indicate violation of data protection and privacy rights of consumers. An example of an ongoing investigation is the Phorm-case.[40] The company is being investigated for suspected privacy violation caused by its behavioral advertising system.

---

[33] STJ, REsp 1.168.547/RJ, 4.ª T., j. 11.05.2010, v.u., rel. Min. Luis Felipe Salomão, DJe 07.02.2011

[34] Art. 55 and 56 of the Consumer Protection Code.

[35] Art. 106 of the Consumer Protection Code.

[36] This measure is currently available in the states of Mato Grosso do Sul, Paraná, Rio Grande do Sul, Alagoas and São Paulo. See the following websites: <http://www.procon.pr.gov.br/modules/conteudo/conteudo.php?conteudo=485>; <http://www.proconbloqueio.rs.gov.br>; <http://www.procon.ms.gov.br/index.php?templat=vis&site=115&id_comp=2309&id_reg=96052&voltar=home&site_reg=115&id_comp_orig=2309>; <http://naoperturbe.itec.al.gov.br>.

[37] http://www.procon.sp.gov.br/BloqueioTelef/

[38] <http://portal.mj.gov.br/main.asp?Team = {B5920EBA-9DBE-46E9-985E-033900EB51EB}>

[39] <http://portal.mj.gov.br/main.asp?ViewID ={3DB528D3-F9F0-4B22-AA4B-6CF6BBA31173} &params = itemID = {FDD46AEE-F356-420E-A868-C18A4BC52E98};&UIPartUID = {2218FAF9-5230-431C-A9E3-E780D3E67DFE}>

[40] http://www.senado.gov.br/noticias/opiniaopublica/inc/senamidia/notSenamidia.asp?ud=20100630&datNoticia=20100630&codNoticia=409485&nomeOrgao=&nomeJornal=O+Globo&codOrgao=47&tipPagina=1; http://veja.abril.com.br/agencias/ae/economia/detail/2010-06-29-1132438.shtml

1.4.2 Regulation: The Need of Comprehensive and Sectorial Data Protection Laws

Although some problems regarding data protection in Brazil require enforcement measures, as seen above, there are some issues that can only be adequately addressed by a broad regulation such as a comprehensive data protection act. This would increase the legal certainty of business activities involving the processing of personal data and guarantee wider protection to individuals against the risks to privacy arising from data processing. This explains why there have been many attempts to create a general legal framework for data protection in Brazil.

In spite of some legislative activity around bills that addressed the issues of data protection in the last decade, to this day no comprehensive data protection bill has reached the final stages of deliberation in either of Brazil's federal legislative bodies. In fact, until recently, none of the few data protection bills proposed[41] even contemplated all of the usual components of a general data protection bill, such as its application to both the public and private sectors or the prevision of a public authority to enforce its rules.

Since 2005, however, the Brazilian government has pondered the prospect of a general data protection bill, after the Argentine government proposed, in a Mercosur working group, the establishment of rules governing data protection in the region to improve citizenship and commerce. As a result of the debate generated at the time, the Brazilian Ministry of Justice drafted a data protection bill and submitted it to public consultation over an online platform in late 2010.[42] During the process of public consultation, the draft bill received more than 800 proposals from public and private entities.[43] The federal government is now expected to present formally a bill to Congress.[44]

The publically available version of the draft bill[45] has its structure based on standard data protection principles that, in a broad way, are akin to those present in international documents such as Convention 108 of the Council of Europe or Directive 95/46/EC. It includes, for instance, provisions about transborder data flow and contemplates the creation of a public authority responsible for enforcing the law. The structure of the draft bill indicates the influence of established national data protection statutes, such as the Italian, German, Portuguese and Spanish ones. Moreover, Brazilian laws, such as the Consumer Protection Code and the Competition Act, influenced the draft.

---

[41] Bills such as PLS 321 of 2004 or PLC 4060 of 2012.

[42] The public discussion is still available in read-only mode at: <http://culturadigital.br/dadospessoais/>

[43] <http://portal.mj.gov.br/main.asp?View={08DEBD27-66DA-4035-BE88-27126C102E22}&Team=&params=itemID={53B2C85F-206D-4DCC-A3D0-85E8E38F6D41};&UIPartUID=2218FAF9-5230-431C-A9E3-E780D3E67DFE}.>

[44] <http://www.tiinside.com.br/15/02/2013/governo-prepara-projeto-de-lei-para-protecao-de-dados-na-web/ti/325360/news.aspx>.

[45] <http://culturadigital.br/dadospessoais/files/2011/03/PL-Protecao-de-Dados_.pdf>.

Overall, the architecture of the data protection framework contemplated in the draft is for a general law that applies to both the public sector and to companies. It is based on a unified and centralized scope rather than on sectorial provisions and relies on unified rules to be applied to the whole country rather than on empowering states and local authorities. Finally, its provisions are directly based on constitutional principles for protecting individuals and personal freedom.

Much of these specifications are not to be considered as options that the legislator could freely choose. Since the Brazilian civil law derives directly from continental European models[46], it tends to privilege a systematic and centralized approach to the regulation of fundamental rights, in contrast to options such as a sectorial approach or even solutions strongly based on self-regulation. In addition, the characteristics of the Brazilian federation require a law of federal scope rather than a regional one, due to the specific nature of Brazil's federal system.

Considering the recent comprehensive reform of the European data protection framework[47], proposed by the European Commission, it is interesting to analyze if and how it is influencing the current efforts of developing new legislation on data protection in Brazil. Examining the Brazilian draft bill, it is possible to notice that some of the proposed norms are comparable with the articles of the European Regulation proposal, such as the breach notification (Art. 27, draft bill) and the norm regarding the binding characteristic of self-regulated codes (Art. 45, draft bill)[48]. Therefore, although it is not possible to establish a direct relation between both processes, we can see that the formulation of the draft bill of data protection has clearly taken into account the new developments in Europe.

Meanwhile, the data protection scenario in the region has changed since 2005. Several Latin American countries have adopted a general data protection law: in addition to Argentina, which pioneered the issue, Mexico, Uruguay, Colombia, Peru and others have statutes governing the area.[49] In Brazil, the lack of a broad regulation in this field has increasingly been considered as a problem both by citizens and by companies: on the one hand, citizens are more and more aware of the risks of an uncontrolled data flow, as issues such as identity theft and commercial abuse of personal data have gained visibility[50]; on the other hand, compliance with international standards concerning the international transfer of personal data and a strong

---

[46] René (2002).

[47] <http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm>.

[48] See the draft at: <http://culturadigital.br/dadospessoais/files/2011/03/PL-Protecao-de-Dados_.pdf>

[49] Regarding the development of data protection legislation in Latin America, see http://www.redipd.org/ (Ibero-American Network of Data Protection).

[50] The Press is increasingly reporting on these matters. See, e.g.: <http://www1.folha.uol.com.br/mercado/1182808-crescem-as-fraudes-com-uso-do-cpf-alheio-um-terco-dos-casos-envolve-telefonia.shtml>; http://www1.folha.uol.com.br/folha/dinheiro/ult91u418838.shtml.