sep / 14

s

The Collecting State

A Study About Argentina and Citizens' Personal Data

ADC / Asociación por los Derechos Civiles

policy paper

ADC / Asociación por los Derechos Civiles

policy paper

The Collecting State. A Study About Argentina and Citizen's Personal Data

September, 2014*

Every Argentine citizen is aware of the numerous proceedings, complex or not, which require that we submit our National ID Card (DNI). Such situation occurs every day: banking operations, buying long distance tickets and entering public and private buildings which require the submission of a card that has been with us since 1968, when the Executive Order 17671, issued by Juan Carlos Onganía, created the DNI as a document to identify all citizens. [1] Many societies would be surprised to see these little cards present in our daily life: there are many countries which do not have unique systems for identifying citizens and, when they tried to impose them, such systems failed given the strong rejection by the community. [2]

Public policies for *identifying, registering and classifying* "national human potential" became more efficient and effective with technological advances. [3] We changed from stored files which could be reviewed upon a person's request to digital information on computer systems for storage and verification. The unique DNI, which will become effective as from 2015, will allow

*This report was produced by the Privacy Area of the Asociación por los Derechos Civiles (ADC), as part of the *Cyber Stewards Network* and with the financial support of the International Development Research Center, Ottawa, Canada.

[1]*This document was carried out by the Privacy Area of the Association for Civil Rights (ADC), as part of the *Cyber Stewards Network* and with the financial support of the International Development Center, Ottawa, Canada.

[2]This was the case, e.g., in England.

[3]The law which created the DNI is called Law 17671 on Identifying, Registering and Classifying National Human Potential.

all Argentine citizens' data to integrate a unique database of biometric digitalized information. [4]

Technological advances regarding classification of Argentines' filiation data have spread, in general, through every area of the State. The information which was previously collected in analogue format is now obtained in digital format, which makes it more useful: digital formats enable automated analysis, remote access and low cost reproduction. However, such greater effectiveness has created new risks that did not arise with analogue systems. This document seeks to enquire about those risks by providing answers to the following questions:

- **1. Does the Argentine legal system properly protect our personal data or does it have deficiencies –in design or in implementation– which put such data at risk?**
- **2. What kind of databases does the Argentine State have? Do those databases have security measures, protected systems with remote control, authorization levels in order to access to them? Is there a recording of the access? Are there standardized security protocols?**
- **3. Has security regarding such databases ever been infringed? What has the State done in such cases?**

I Law on the Protection of Personal Data and two original sins

The Argentine legal framework concerning the protection of personal data is one of the best frameworks within the region. In fact, Argentina has a constitutional guarantee for the protection of personal data which is recognized in the Argentine Constitution, Section 43:

> "Any person shall file this action to obtain information on the data about himself and their purpose, registered in public records or data bases, or in private ones intended to supply information; and in case of false data or discrimination, this action may be filed to request the suppression, rectification, confidentiality or updating of said data. The secret nature of the sources of journalistic information shall not be impaired."

[4] Cfr. Telam. *A partir de 2015 el DNI tarjeta será el único documento válido*. Consulted on 19 June 2014 and La Nación. *A partir de 2015, sólo tendrá validez el nuevo "DNI tarjeta"*. Consulted on 19 June 2014. It is important to mention that when we talk about biometric data we refer to information regarding the individuals' physical features which is used for identifying purposes, such as fingerprints, photographs, facial images, etc.

Law 25326 on the *Protection of Personal Data* adopts the principles of the Directive No. 95/46/EC of the European Union. This rule sets high standards of protection and the EU has considered Argentina as a country with an adequate level of personal data protection since 2003 (Travieso, 2006).

However, this protective legal framework has two structural weaknesses: (a) a weak controlling agency which depends on the executive branch and (b) excessive allowances in favor of the State regarding storage, processing and communication of personal data.

As regards the first issue, the original version of the Law 25326 intended to create a controlling agency with "functional autonomy" that would act "as a decentralized agency within the framework of the National Ministry of Justice and Human Rights." Such agency would have a director appointed by the executive branch, with the approval of the Senate, for a period of four years. Those guarantees of functional autonomy and financial self-sufficiency were set aside when the executive branch promulgated the law partially by issuing the Executive Order 995/00, which kept the agency within the scope of the executive branch for financial reasons. Such decision was key to create a weak controlling agency which depends on the executive branch. [5]

In order to address the second issue, it is useful to analyze the structure of the Law 25326, which protects personal data by means of two general bans that seem to play a vital role in the legal architecture of the law: the bans on *processing* and *communicating* personal data without the consent of their owners. [6] Both bans seek to prevent the illegal use of citizens' data through a method which seems effective: empowering citizens with the capacity to prevent third parties from using such data for purposes not authorized by citizens. However, the law that gives us such power also takes it away from us when we want to enforce it against the State.

In fact, Section 5 requires consent but states that such consent shall not be deemed necessary when the data are "collected for the performance of the duties inherent in the powers of the State or when the data arise from a contractual relationship". This means that the guarantee of consent is useless when the data are collected by the State. Furthermore, Section 11 bans the *communication* of data if the data owner has not previously consented to it. However –again– this guarantee may be set aside when a law so provides, when the data are collected for the performance of the duties inherent in the powers of the State or when the communication of data takes place directly between governmental agencies to the extent of their corresponding compe-

[5] Even though the Regulatory Decree 1558/01, Section 29.1 states that the "Director shall exclusively devote to his or her functions, shall perform his functions independently and shall not be subject to any instructions"."

[6] Law 25326, Sections 5.1 and 11.1.

tencies.[7]. As we can see, the guarantees set forth by such law are in general set aside when data is collected by the State.

Through these broadly stated exceptions, Law 25326 allows the State to evade the bans which are the key of such Law's structure: the bans on processing or communicating data without the owner's consent. As a consequence, citizens are deprived of the main tool to protect the privacy of their data.

We are now in a position to answer the first question: does the Argentine legal system properly protect our personal data or does it have deficiencies which put such data at risk? Two problems related to the design of such law which seem to be particularly relevant to the purpose of this study have been identified:

1. On the one hand, the agency created by the law was set aside by the executive branch upon partial promulgation of the law. Moreover, the agency created instead lacks the guarantees of autonomy which were stated in the original version of the law.

2. On the other hand, the two structural bans which empower the right of citizens not to consent the processing of their data are not enforceable against governmental agencies which can also communicate such data to other governmental bodies with no major restrictions.

In the following section, we seek to analyze whether, in addition to these deficiencies in design, there are also difficulties in the application of the current system.

II The State and personal data

In Argentina, the agency in charge of the defense of citizens' personal data is the National Bureau of Personal Data Protection (DNPDP) which was created –as we have already seen– with serious limitations in its powers. Are those structural problems reflected in the agency's acts? In order to answer this, it is necessary to analyze whether the lack of *financial self-sufficiency* which was stated in the law has affected the structure of the DNPDP and whether the wide allowances granted to the State by such law have affected the performance of the agency.

[7] Cfr. Law 25326, Section 11.3.

Structure and performance of the DNPDP

If we analyze the operating budget of the DNPDP since it was created it may be seen that it has always been relatively low, both in terms of resources and of staff. [8] If we take into account the budget data and the year-on-year inflation, it is also possible to see that some cases of nominal increase represented an actual decrease of the budget for such years, such as the case of years 2005, 2006, 2008, 2009 and 2013. The budget of the DNPDP has only increased between 2010 and 2012. As a result, there has also been an increase in the staff (Table 1).

Year	Budget	Staff	Inflation	Actual Variation
2014	ARS 5,662,014	26		
2013	ARS 4,291,557	25	28.3	-
2012	ARS 3,809,908	25	25.9	+
2011	ARS 1,727,045	23	24.3	+
2010	ARS 1,021,095	21	26.1	+
2009	ARS 862,729	21	16.7	-
2008	ARS 728,605	11	23.5	-
2007	ARS 702,158	10	8.8	+
2006	ARS 396,667	10	1.9	-
2005	ARS 380,091	10	9.8	-
2004	ARS 595,124	9	4.4	

Table 1: Budget and structure of the DNPDP (2004-2014).

It is really useful to analyze the budget and structure of the DNPDP if we compare such data with its functions set forth in Law 25326 .

- To give any requesting party assistance and advice on the scope of this Act and the legal means available for the defense of the rights guaranteed by the same (Section 29.1.a).
- To pronounce the rules and regulations to be observed in the development of the activities covered by this Act (Section 29.1.b)
- To do a census of data files, registers or banks covered by the Act and keep a permanent record thereof (Section 29.1.c)
- To control compliance with the norms on data integrity and security by data files (Section 29.1.d)
- To request information from public and private entities (Section 29.1.e).
- To initiate proceedings and enforce the administrative sanctions that may apply (Section 29.1.f and Executive Order 558/01, Section 30.).

[8] The Regulatory Decree 1558/01, Section 29.3 stated that the DNPDP shall be financed with the funds collected as fees for the services provided; with the funds derived from the fines established in section 31 of the Law 25326; and with the budgetary allocation included in the Budget of the National Administration Law (Ley de Presupuesto de la Administración Nacional) as from year 2002.

- To assume the role of accuser in criminal actions brought for violations of this Act (Section 29.1.g).
- To control fulfillment of requirements and guarantees to be met by private files or banks which provide reports to obtain the corresponding registration with the Register created by this Act (Section 29.1.h).
- To monitor exofficio the due compliance of the legal principle of specification of purpose and to impose sanctions (Regulatory Decree 1558/01, Section 4).
- To check the due compliance with the legal and regulatory provisions concerning every stage of the use of personal data: collection, exchange, communication and cession (Regulatory Decree 1558/01, Section 4)
- To establish the requirements for the consent to be given by means other than written notification (Regulatory Decree 1558/01, Section 5).
- To stimulate the cooperation among public and private sectors (Regulatory Decree 1558/01, Section 9).
- To deal with complaints raised upon denial of the right to access to personal data (Regulatory Decree 1558/01, Section 14).
- To provide a sample form to exercise the right to access to personal data (Regulatory Decree 1558/01, Section 15).
- To issue complementary rules regarding contracts of chambers, associations and professional organizations.
- To issue the administrative and procedural rules related to registration proceedings as well as to the treatment and security conditions of public and private databases (Regulatory Decree 1558/01, Section 29.5)
- To deal with complaints related to the treatment of personal data (Regulatory Decree 1558/01, Section 29.5).
- To collect the fees established for the services of registration and other services provided (Regulatory Decree 1558/01, Section 29.5).
- To organize the Registry of public and private databases (Regulatory Decree 1558/01, Section 29.5).
- To elaborate the necessary tools suitable for the best citizens data protection (Regulatory Decree 1558/01, Section 29.5).
- To encourage the creation of codes of conduct (Regulatory Decree 1558/01, Section 30).

As shown in the previous list, the functions of the DNPDP set forth by the law and by the regulatory decree are extremely ambitious and seem to be designed for an independent agency with financial self-sufficiency and with a structure necessary in order to perform such functions properly. In fact, the functions of the DNPDP set forth by both the law and the regulatory decree include advice for citizens, regulation of powers, control and regis-

tration of public and private databases and application of sanctions upon default. The DNPDP shall has broad jurisdiction throughout the country. However, during the first six years of its creation, it only had ten employees (see Table 1). It is also important to highlight that the number of staff remained limited even when technology evolved and made storage and processing of all kind of data easier. In other words: the structure of the controlling agency was kept relatively unchanged as the controlling activity dramatically increased.

The issue mentioned in the previous paragraph is clearer if we carefully analyze the controlling powers of the DNPDP. According to the data provided by the DNPDP, between 2008 and 2012 the DNPDP has conducted 137 inspections (Table 2) even though there were more than 60 thousand databases registered with the National Registry of Databases by the end of 2006. [9]

Year	Number of inspections
2008	4
2009	16
2010	50
2011	28
2012	39

Table 2: Number of inspections conducted by the DNPDP (2008-2012).

The analysis shows that there is a correlation between the design of institutions and their actual performance: a controlling agency which has been denied the guarantees of autonomy and financial self-sufficiency set forth by the law and which had a low budget and a limited number of staff in order to perform activities that exceeded the actual institutional capabilities available. The difference between what was expected by the law and the structure created by the executive branch has limited the performance of the DNPDP, performance which has also been lenient with the State not only due to the lack of autonomy of the agency but also due to biases in the law which have been previously identified and will we described below.

Excercise of powers

Just like the budget and the structure of the DNPDP seem to evidence a situation of weakness, it is also possible to prove the allowances of the law in favor of the State regarding the performance of the DNPDP. In fact, the 137 inspections conducted by the DNPDP between 2008 and 2012 were car-

[9] Cfr. Diario Judicial. *Registro de bases de datos: esperan 60 mil inscriptos a fin de año*. (25 May 2006). Available at: www.diariojudicial.com/contenidos/2006/05/26/noticia_0009.html

ried out in private companies: governmental agencies responsible for any databases have never been inspected by the DNPDP between those years. [10]

It is also possible to check the penalties imposed by the DNPDP for breaching the law: the 36 penalties imposed by the DNPDP between 2005 and 2013 have been imposed on private entities. The State has always avoided the power to punish a controlling agency which depends on the executive branch and has –as a consequence– a weak power to impose penalties on agencies with the same or, in general, with superior powers.

Nevertheless, it is important to analyze the penalties imposed by the DNPDP: they show that the exercise of powers to impose penalties requires –for several reasons– a structure the DNPDP seems not to have. In fact, 42 per cent of the penalties have been imposed on private entities due to mistakes in registration, in re-registration or in updating databases (Table 4). Other 25 per cent of the penalties have been imposed due to unsolved deficiencies identified by the DNPDP upon inspections conducted on entities holders of databases. Therefore, 67 per cent of the penalties have been imposed due to minor issues or upon the result of the inspections conducted which were –as mentioned above– 137 inspections on a basis of more than 60 thousand holders of databases registered.

Reason to impose penalties	Percentage
Denial of the right to access information	8.33%
Wrong information regarding debtors	8.33%
Reports produced without legal background	8.33%
Inspections	25.00%
Re-registration, updating of data	41.67%
Wrong allocation of telephone lines	8.33%

Table 3: Category of penalties imposed by the DNPDP between 2005 and 2013 according to the data provided by the DNPDP.

The content of the remaining penalties relates to some of the most serious problems faced by Argentine citizens concerning their personal data: the incorrect registration of debtors with public and private registries, the denial of the right to access to their own personal data and the execution of reports regarding citizens which are contrary to Law 25326.

The first issue has been one of the main reasons for filing complaints regarding personal data: the incorrect registration of debtors with a debtors' registry raises a large number of difficulties related, specially, to the access of bank loans. The DNPDP has imposed penalties on three cases to private

[10] The lists of inspections conducted by the DNPDP are available at: www.jus.gob.ar/datos-personales.

entities which had provided wrong status of *debtors* concerning their clients.

The second issue relates to the denial of the *right to access* to data which means to enable individuals to know which data is held about them by the holder of a database.

The third issue is one of the most serious and is related to the spread of websites which sell citizens' reports including personal data, such as domicile, marital status or financial situation, among others. [11] For such reason, it is meaningful to analyze what the DNPD has declared regarding this issue.

There are three relevant penalties about this issue: one against the entity *Advanced Development Solutions S.R.L.* (hereinafter referred to as ADS), which maintains the website www.reportesonline.com, and two against *Globinfo Argentina*, which is an undertaking of *Open Discovery S.A*.

The complaint against ADS was the result of several individuals' complaints who obtained personal data reports through ADS's website. Complainants claimed they were able to access –through this service– to data concerning previous employments, property, relatives other than the spouse, level of wages and neighbours' personal data, among others. The DNPD considered that this service was contrary to citizens' *interests*, to the guarantee of *cession* of data and to principle of *specification of purpose*. The DNPDP has also highlighted that the access to information regarding *wages* is not possible through "databases of unrestricted public access". Therefore, it may be assumed that there has been an illegal processing of the data since the holder of such data has not given his/her free, express and informed consent.

The complaints against *Globalinfo Argentina*, on the other hand, have been filed by petition of the Ombudsman's Office for the City of Buenos Aires (Defensoría del Pueblo de la Ciudad de Buenos Aires) and by a private citizen. The analysis of the DNPDP shows one of the practices which has the greater impact on citizens' personal rights and which relates to entities engaged in the storage and processing of reports with trading purposes. [12] Such websites offer different kinds of reports. They often provide, for free, citizens' names, DNI number and address recorded in several public registries. However, if one is willing to pay, they provide more valuable data which is more difficult to obtain through the means referred to in the previous paragraph.

The DNPDP considered that the processing of data by *Globalinfo* was not necessarily contrary to the law but the *cession* of data to third parties was. It also considered that the reports produced by *Globalinfo* were excessive since

[11] Cfr. Emiliano Villa. 2014. *Privacy at Hand's Reach*. Digital Rights LAC, No. 12, 2 April 2014.

[12] Id.

they provided data concerning the financial situation of citizens in order to trace them and such financial reports contained the information needed to trace them[13]. As regards the information sources, the DNPDP considered that –in principle– *Globalinfo* had access to such data through public *sources of unrestricted access* but those sources were never described.

Much of the information contained in this reports comes from governmental databases which stored such data for specific purposes. For example, the National Registry of People, the Argentine Registry of Real and Personal Property, the National Social Security Administration (ANSES), among others. The opinion does not enquire about how such data was obtained: it only highlights that pursuant to Regulatory Decree 1558/2001, Section 11 "In the particular case of public databases or archives of an official agency which according to its specific functions were intended to be released to the general public, the requirement concerning the legitimate interest of the grantee shall be considered implicit in the general interest that caused the unrestricted public access". The question at stake is: Are all public governmental databases designed for the access of general public? Under which conditions and guarantees is the cession of data authorized? Neither does the opinion answer this issue nor does it question governmental practices which seem to be the main cause of spread of this practices for entities that infringe citizens' rights.

III The DNPDP and governmental databases

So far, we have seen how the law has created a weak enforcement agency and how it has been excessively lenient with respect to storage, processing and cession of data performed by the State. We have also proved that the weakness arising upon the partial promulgation of the law which created the enforcement agency was affirmed by a low budget and a limited number of staff. We have also shown that there is a considerable gap between the powers of the DNPDP and the resources available as well as a strong bias towards private entities which may derive from the permissibility of the law towards governmental agencies.

Based on such partial findings, we have tried to show governmental practices regarding their databases through 16 requests to access to public data[14]

[13]DNPDP. Regulation No. 005, 22 April 2008, page 184.

[14]The agencies and registries consulted were: National Criminal Intelligence Department (DNIC); National Registries of motor vehicles and secured loans (DNRPA); National Copyright Office (DNDA); National Registry of Information concerning Missing Minors (RNIPME); National Department for Human Rights and International Humanitarian Law (Dirección Nacional de Derechos Humanos y Derecho Internacional Humanitario); National Registry of Rural Land (RNTR); National Contracting Office (ONC); General Department for Personnel and Welfare of the Argentine Army (Dirección general de personal y

through which we searched for responses to specific basis questions. [15] In general, the number of responses was high: ten agencies answered such requests but in several occasions they raised legal defenses and addressed such requests partially. However, from such range of answers and of information concerning secondary sources, it is possible to get an overall image of the way in which the State processes citizens' data. The following findings raised from analyzing such answers:

- In general, all databases have different levels of access according to staff categories.
- Servers are usually located at the offices were such agencies perform their activities.
- Security measures seem to be related to personal passwords of each

bienestar del Ejército Argentino); Secretary of Institutional Organization and Management (Secretaría de gestión y articulación institucional); National Registry of Family Agriculture (RENAF); Federal Penitentiary Service (SPF); National Migration Office (DNM).

[15] The questions raised in the requests to access to public data were the following: "Integration of files, records, databases or data banks of the [Registry X]. Mainly, we are interested to know (a) whether [Registry X] has files, records, databases or data banks. If it has more than one, please identify them; (b) physical location of servers which contain files, records, databases or data banks; (c) data of individuals contained in such files, records, databases or data banks (such as DNI number, number of process, name, surname, photograph, etc). Define and identify (if more than one) each registration system separately. // Who can have access to those files, records, databases or data banks? Please indicate the name, surname and position of authorized officers. In the case of personnel of the [Registry X], are there several categories with different levels of access? Are third parties not related to the [Registry X] allowed to access to databases? If applicable, please identify third parties authorized to access. If there are different files, records, databases or data banks, please identify each case. // How can those files, records, databases or data banks be accessed? For instance, we are interested in technical details of the access, that is to say, if it happens through networking computers; if authorized persons have to use a password in order to access; if such password is personal, etc. If such password is lost, what is the proceeding to create a new one? Is this situation recorded? Where? If there are different files, records, databases or data banks, please identify each case. What kind of safety measures do those files, records, databases or data banks of the [Registry X] have? For example, we would like to know whether they are connected to the Internet and -if they are- what kind of safety measures do those files, records, databases or data banks have in order to prevent intrusions of unauthorized persons? If there are different files, records, databases or data banks, please identify each case. // Has there been any case of unauthorized downloading of data? If that situation has occurred, how has the [Registry X] acted upon knowledge of the situation? If there were no intrusions of unauthorized persons, what would be the proceeding if there were intrusions? // Who are in charge of providing technical support for the different problems that may arise in files, records, databases or data banks?// Do those persons have unrestricted access to the files, records, databases or data banks? Who do they report to? Please indicate the name, surname and position. // How are the requests of information of the [Registry X] recorded when they are required by other entities? Please distinguish between requests made by entities belonging to the executive, legislative or judicial branches (in the event of any difference)."

employee, however, in many occasions such agencies were reluctant to provide information regarding security measures techniques.

- Security depends on the computing area of each agency.

These findings arise from the different responses given by the public agencies which answered the requests to access to public data. It is important to highlight that it was not possible to obtain information regarding which officers are authorized to access the information contained in databases since those agencies considered that such information is reached by the exceptions to access to data which are set forth in the Regulatory Decree 1172/03, Annex VII. [16] They also denied the access to data regarding "technical and organizational measures the agency must take to guarantee the security and confidentiality of personal data" pursuant to Law 25326, Section 9. [17] In many cases, they only provided general information concerning the existence of staff categories with different levels of access. [18] For example, the National Registry of Information concerning Missing Minors (RNIPME) informed that the access is by "categories" (such as coordinator, social team, lawyers, technical operators) and that "each user [can] carry out the tasks allowed according to their category and only regarding information of their area". [19] In the same respect, the National Registry of Rural Land (RNTR)

[16]See, for example, the response of Esteban F. de Gracia, Director of the Nominative and Fingerprinting Registration of the National Registry of Recidivists (Registro Nominativo y Dactiloscópico del Registro Nacional de Reincidencia), 15 January 2014 (copy of the files available at ADC).

[17]Response of Esteban F. de Gracia, Director of the Nominative and Fingerprinting Registration of the National Registry of Recidivists (Registro Nominativo y Dactiloscópico del Registro Nacional de Reincidencia), 15 January 2014 (copy of the files available at ADC); response of Inés García Holgado, legal adviser of the National Copyright Office, 10 January 2014 (files available at ADC), response of Manuel Enrique Pedreida, Director of the National Registry of Family Agriculture, 7 November 2013 (files available at ADC). It is important to highlight that Section 9 of the Law 25326 does not prevent information regarding security measures from being requested since it sets forth –in its relevant part– the following: "Section 9.1. The person responsible for or the user of data files must take such technical and organizational measures as are necessary to guarantee the security and confidentiality of personal data, in order to avoid their alteration, loss, unauthorized consultation or treatment, and which allow for the detection of any intentional or unintentional distortion of such information, whether the risks arise from human conduct or the technical means used."

[18]See, for instance, the response of the National Copyright Office where it was affirmed that "only a part of the personnel of DNDA is authorized to access to data. There are several categories of agents with different levels of access and restrictions regarding the treatment of data as well as the possibility of uploading and modifying such data. The access is controlled through a restricted access with user name and personal passwords". See response of Inés García Holgado, legal adviser of the National Copyright Office, 10 January 2014 (files available at ADC).

[19]National Registry of Information concerning Missing Minors (RNIPME), Management Report 2012, 8 April 2013, available at: http://www.jus.gob.ar/media/774132/informe de gestion 2012.pdf.

detailed the different categories of users who can have access (operator, advanced operator, advanced operator with digital signature) and informed that they have all "signed confidentiality agreements" with the Registry. [20]

Some agencies provided information regarding security measures but in general terms. For example, the National Registry of Family Agriculture pointed out that its database is connected to the Internet through a "system for tracking and collecting" sworn statements which depends on the IT Department of the Ministry of Agriculture. [21]

The agencies which provided information concerning the location of databases pointed out that such databases are located in the buildings where the different departments work. [22] However, in some cases, they are located in the offices of other agencies. [23] In general, the technical offices of the Ministries where such databases are located are in charge of security measures, [24] which seems to suggest that there is not a centralized control system or unified standards regarding security.

The answer which showed a different trend –due to both the type of data provided and the details of such data– was the one from the National Contracting Office (ONC). [25] The ONC manages two important databases which are relevant for the hiring process of the State: the System of Identification of Goods and Services and the System of Information of Providers and Transparency, which contains the information published in the ONC's website. The physical location of these databases is distributed among three different places: the safe room of the AFIP, the DMZ of the Secretary of Finance (Secretaría de Hacienda) and the Data Center of the Under-Secretariat of Management Technologies (Subsecretaría de Tecnologías de Gestión).

In all these cases, ONC's databases have unrestricted public access through the website *www.argentinacompra.gob.ar*. Nevertheless, it should be noted that it is not possible to access to raw data contained in databases since it is necessary to follow different data identifiers and filters which provide access to specific information.

As regards the individuals who can have access to information, that depends on the safety measures of each server. For example, the safe room

[20] Response of the National Registry of Rural Land (RNTR), 22 January 2014 (files available at ADC).

[21] Response of Manuel Enrique Pedreida, Director of the National Registry of Family Agriculture, 7 November 2013 (files available at ADC).

[22] See, for example, the response of Inés García Holgado, legal adviser of the National Copyright Office, 10 January 2014 (files available at ADC).

[23] Such as the National Contracting Office (ONC).

[24] See, for example, the response of Juan Carlos Nadalich, Secretary of Institutional Organization and Management of the Ministry of Social Development, 11 November 2013.

[25] Response of María Verónica Montes, Director of the National Contracting Office, 6 November 2013 (files available at ADC).

of the AFIP can only be accessed by "authorized staff of the AFIP that belongs to the IT support division for databases", and they only do that upon request of the ONC. The staff of the ONC that works in the Information and Transparency System Division (Dirección de Sistemas de Información y Transparencia) can also have access to the safe room. The access is remote and "connected point-to-point between the ONC and the safe room of the AFIP" and by means of "usernames and passwords". The same situation occurs with the DMZ of the Secretary of Finance. The ONC does not have direct access to the Data Center of the Under-Secretariat of Management Technologies.

The safe room of the AFIP has relevant security measures to protect data: it is a protected, fireproof room with safety measures and access restricted to specially authorized people. [26] The room has a monitoring system regarding network traffic and cyber-attacks which may put the security of the data contained in such room at risk. According to AFIP, "between 200,000 and 300,000 attempted attacks occur daily". [27]

It should be noted that the safe room of the AFIP does not only include data of the ONC but also data from other agencies –for example, Presidency of the Nation– as well as tax data regarding the transactions that 8 million tax payers carry out with AFIP in real time. [28] It also includes data concerning tax statements and "exogenous information that [...] other entities provide, for example, credit cards, banks, registries of real property and of motor vehicles, it is all included in the safe room". [29] This datum is relevant since databases held by the State tend to include information that private entities provide to public entities.

> "The entity in charge of Ricardo Echegaray has an x-ray of the economic transactions of each tax payer, including the most frequent consumptions. Travels, purchases made online and at shops, maintenance expenses for buildings, banking transactions, credit card statements, online transactions in websites such as Mercado Libre, mobile phone or private health insurance expenses, among others, are closely followed by the inspectors who cross-check data in order to identify whether such expenses match with sworn statements and to identify inconsistencies and potential sanctions". [30]

This datum confirms a permanent surveillance policy which is possible as a

[26] Cfr. Acción Impositiva. *El centro de cómputos de la AFIP*. (2010).
[27] Id.
[28] Id.
[29] Id.
[30] Cfr. Pagano, M. (2014). *La AFIP ya controla todos los gastos de los consumidores*. Newspaper Clarin. Consulted on 19 July 2014.

result of technological advances and economy actors' obligations to inform. Such flow of information between private and public entities is permitted by the Law 25326 which sets forth that consent of the data owner shall not be deemed necessary when "the data are secured from source of unrestricted public-access"; when the data " are collected for the performance of the duties inherent in the powers of the State"; or when the data"refers to the transactions performed by financial entities, and arise from the information received from their customers in accordance with the provisions of Section 39 of Law 21526". (Law 25326, Sections 5 and 11). Financial entities shall transfer data pursuant to said Section 39 which allows such transfer in favor of"entities collecting national, provincial and municipal taxes based on the following conditions: (a) it must relate to a specific responsible; (b) a tax verification regarding such responsible must have been initiated; and (c) it must have previously been required formally". However, the data requests made by the AFIP"shall not be subject to the first two conditions set forth in this Subsection".

The Financial Institutions Law is a significant example given the way by which authorization is granted: there are bans established but with generous exceptions concerning transfer or access to data in favor of governmental entities. It follows a legislative method similar to the one followed by Law 25326, mentioned at the beginning of this document, which shows a common pattern: bans and guarantees are set aside when the State intervenes.

This trend of massive storage and incorporation of data from private entities is problematic from the point of view of privacy. Beatríz Busaniche from Fundación Vía Libre stated that:

> "The ability to register and process data as well as to cross-check data has no precedent in history. Ability to calculate, software development, advances which have no historical comparison. A key issue to consider is the fact that the State must not collect a quantity of data larger than that strictly necessary to fulfill its targets. The main point of a public policy by which the storage of data is considered a measuring instrument, is to collect a minimum quantity of data required to fulfill a target. Such processing of data must be transparent for citizens who must be aware of the purpose for which such data is collected and, when data are not essential, citizens must have the power to refuse to provide such data. Another point to consider is that the entity is not the owner of such data and must guarantee their privacy and security. I am particularly concerned about the fact that if you know the CUIT (tax ID) of a person, you can obtain at AFIP a lot of personal data, address, tax category, all of which represents an

> attractive target for thieves. The number of people who sell personal data obtained through AFIP is overwhelming. The State is not the owner of our data and thus must ensure its protection and comply with the guarantees set forth by the Constitution". [31]

The fact that data can be easily transferred among different public entities and that there are several obligations performed by the various economy actors create, in every way, puts the privacy of such data at risk. The safe room or the DMZ systems are of no use if the information there contained is shared with governmental entities whose practices or systems are less secure: the strength of a chain, as it will be described below, depends on its weakest link.

It is important to analyze the action of the DNPDP concerning governmental databases. The response of the National Migration Office (DNM) was significant since it answered the questions and enclosed the electoral registries of its databases contained on the DNPDP. It is relevant to analyze such data for the following reason: it allows to know what kind of information the DNPDP holds in governmental databases.

From analyzing such records of voters it may be seen that DNM has information regarding human resources and employees' fingerprints, images, marital status, university degree, occupation, sanctions, evaluations, clinical records, pre-employment examinations, retirement and labor union affiliations. All such data "must only be provided by the owner"[32]. Moreover, it was informed that such data is kept indefinitely, that is, forever. Such data is kept on a central server.

The information provided by the Registry for Admission of Foreigners (Registro de Admisión de Extranjeros) and by the Registry of Entry and Exit of Persons to the Argentine Territory (Registro de Ingresos y Egresos de Personas al Territorio Nacional) is also relevant: apart from the personal data which are similar to the registration of human resources, both Registries recognize that they process sensitive data and that they intend to transfer and make massive cessions of such data to third parties as well as to transfer such data to other data banks and entities abroad. [33] Regarding security measures, they informed that such data can be used by 14 governmental agencies, such as the Ministry of Foreign Affairs, the Ministry of Education, INDEC, RENAPER, the Secretary of Tourism, AFIP and all security forces.

[31] Cfr. Filozof, L. (2012). *El gran hermano fiscal*. Magazine Veintitrés. Consulted on 19 July 2014.

[32] Cfr. Memorandum No. 378/13 from the National Migration Office (DNM). Files available at ADC.

[33] Cfr. Memorandum No. 378/13 from the National Migration Office (DNM). Files available at ADC

34

IV The case of photographs on the electoral roll

Legal action

The case we will be discussing below reveals one of the problems of a permissive Act towards the treatment and transfer of information among governmental entities. The case came to the knowledge of ADC due to the work done by this organization to defend human rights in general and the right of individuals to their privacy in particular. In the context of this report it works as a paradigmatic case study that identifies the risks that may arise from the misuse of information of individuals.

The case reached ADC through Enrique Chaparro, President of Fundación Vía Libre, who found in the online consultation system of the Electoral Roll that the information about the place where he must vote in the election that took place in October 2013 included the photograph of his DNI. This revealed that the National Electoral Chamber had received such information from the National Registry of People, the public authority which stores such information pursuant to Executive Order 17671.

ADC's initial approach to the problem was to consider it as an unlawful communication of data that should be called into question because it also affected the principle of specification of purpose of the Law 25326, established in the Section 4.3: "The data subject to treatment shall not be used for any purpose or purposes which are different from or incompatible with those giving rise to their collection". Furthermore, we suspected that the prohibition of communication stated in Section 11 of the Law, which requires for its enforcement "to meet the purposes directly related to the legitimate interests of the person responsible for data file and the recipient" and "the consent previously given by the data owner, who must be informed about the purpose of such communication of data, and provided with an identification of the recipient or with the elements that enable him or her to identify such recipient", had been violated".

However, when we started to analyze the problem in depth, we noticed the situation was much more complex.

In fact, we soon realized that it was possible to argue that the extensive authorizations of storage, treatment and communication of personal data among governmental entities could be alleged to justify the communication between the National Registry of People (RENAPER) and the National Elec-

[34]Cfr. Memorandum No. 378/13 from the National Migration Office (DNM). Files available at ADC

toral Chamber. As mentioned above, Section 11.3c of the Law 25326 allows communications of data without the consent of the data owners when such communications of data "takes place directly between governmental agencies, to the extent of their corresponding competencies". That argument was problematic since the communication of data itself could not be called into question, even though it was anyway questioned for violating the principle of specification of purpose above mentioned. Nevertheless, we went to look for the Law that had introduced the photographs of citizens to the Electoral Roll.

The first regulation we found was the Decision 18/13 issued by the National Electoral Chamber in March 2013. Such decision stated that each voter's photograph should be included in the temporary online electoral system that was available on the website: *www.padron.gob.ar*. Also, the decision introduced new models of electoral rolls to be used in the elections that would include the voters' photographs for the so-called "special electoral roll", which is available to the presiding officer of the polling station.

The extensive data that shall be included in the National Electoral Register, in accordance with a judicial decision, was considered a problem for us. Given the fact that such extension affects constitutional rights like the right of privacy and the right to vote, it shall be stipulated by law. However, that law was already enacted: Section 3 of the Law 26744, passed in November 2012, under which the right to vote was extended to minors of 16 years old, amended Section 15 of the National Electoral Code.

> "Said Section 15 states that the National Electoral Register shall compile computerized records and information on paper. Computerized records shall contain the following personal data of each voter: first name and surname, sex, place and date of birth, address, occupation, type and number of the identity document required, specifying what type it is, date of identification and filiation data. The condition of absent shall be expressed in the event of enforced disappearance where appropriate. The competent authority shall determine the way in which fingerprints, photos and signatures of each voter shall be included. Information on paper shall contain, in addition to the personal data required for the computerized record, fingerprints, and the original signature of the voter, and the photograph (the highlighted belongs to us).

This means that the Argentine National Congress delegated in the National Electoral Chamber, as the competent authority of the argentine electoral regime, the power to include fingerprints, photographs and signatures. These data are contained in the DNI and also in the Argentine National Registry

of People (RENAPER) which is an agency that, pursuant to Article 17 of the National Electoral Code, shall

> "send to the National Electoral Register, in electronic form, the data belonging to each voter and future voters. Notwithstanding the foregoing, the Argentine National Registry of People shall send periodically documentary evidence of every computer entry that shall remain in the unique and centralized custody of the National Electoral Chamber (…)The National Electoral Chamber may regulate both the conditions under which the Argentine National Registry of People shall send the information and the appropriate mechanisms for its permanent updating and control, in accordance with the Law and the possibility of acquiring new technologies to improve the electoral registry system."

As we can see, the State did not need to justify that the communication of data had taken place upon the extensive authorizations granted in Law 25326; there were specific laws that allowed such communication.

The National Electoral Chamber explained, in the Decision 18/13, that the inclusion of the photographs would be implemented as a pilot project:

> "In this sense, and taking into account that the inclusion of photographs would be, as emphasized, a pilot project, it is therefore appropriate in that case to provide for the inclusion of the photograph, whether in print and on the Internet, to the provisional elector roll, in order for the electors to have the opportunity to make any pertinent observation in advance"[35].

According to the Judicial Information Centre's report, the online electoral roll database contained the photographs of 9,338,672 electors, meaning 30.59% of the total registered electors on the definitive national electoral roll[36].

The situation was serious. As ADC explained in the recourse of amparo, the images of the faces of more than 9 million citizens are available on the Internet and, therefore, any people who may know the minimum personal information can have access to them. Such personal information can be easily obtained and can also be subject to a data automatic recovery process".

[35]National Electoral Chamber. Decision 18/13. Recital 7.

[36]Cfr. Judicial Information Centre (CIJ). (2013). *Más de 9 millones de electores tienen su fotografía en los padrones*.

ADC's arguments

The right to privacy

The argument of ADC was based on the right to privacy recognized by the Argentine Constitution and by International Human Rights Treaties that were incorporated into the Constitution with constitutional hierarchy.

> "In the Argentine legal system, the right to privacy is a broad right which also includes a dimension related to personal autonomy and other related to intimacy. With regard to the first sense –which is broader and more generous and is set forth in Section 19 of the Constitution– the purpose is to 'guarantee that all individuals can be in a position to develop their own lives acoording to their own decisions'. The second sense is more limited and is set forth in Section 18 of the Constitution which states that 'the domicile may not be violated, as well as the written correspondence and private papers; and a law shall determine in which cases and for what reasons their search and occupation shall be allowed'. As Nino explains, it is 'a personal area which is safeguarded from other individuals' general knowledge'. Such area goes beyond the domicile or private papers and includes all citizens' communications as well as different aspects of the personality and spaces where one can 'reasonably expect privacy'.
>
> The right to privacy is also a fundamental right to develop a democratic citizenship. Without the right to decide regarding one's life and without a private space free from the view of others, some basic freedoms which are key to develop a democratic citizenship will not be fully exercised. For example, the rights of freedom of expression, of assembly or of association cannot be fully exercised if –for example– citizens are subject to control or surveillance measures by the State. In the same way, the right to informational self-determination guaranteed by personal data protection laws also has the purpose to guarantee a 'private' space necessary to perform self-determination and to be protected from third parties who may threaten such fundamental freedom". [37]

[37] Joint Habeas Data Action filed by ADC. Internal quotes belong to Gargarella, R. (2008). *Constitucionalismo y Privacidad*. Teoría y Crítica del Derecho Constitucional (1st. edition, Volumes 1-2, Vol. II, pages. 779–793). Buenos Aires: Abeledo-Perrot y Nino, C. S. (1992). Fundamentos de derecho constitucional: análisis filosófico, jurídico y politológico de la práctica constitucional. Astrea.

ADC considered that the careless treatment by the State concerning citizens' photographs collected as a result of the National ID Card (DNI) represented a risk for the autonomy of citizens since it prevented them from having control over such a personal and sensitive datum as the photograph of their own faces. Moreover, upon publication through a system of open access any person with a minimum quantity of a person's data could have access to them. Therefore, such a personal and sensitive datum became generally known by other citizens, as Nino described intimacy[38].

The right to self-image and the risks created

Furthermore, ADC argued that the rights to privacy and intimacy are not the only ones directly affected. The careless treatment by the State regarding personal and sensitive data indirectly produces a wider impact since it increases the possibility that third parties may use such data in violation of rights.

> "The possibility that the State or private entities may have access to citizens' sensitive data has never been so high. In fact, the careless publication of photographs on the Internet affects –as informed– more than 30 per cent of the electoral roll and represents a de facto transfer of data to third parties who may collect such data and include them in databases with illegal purposes". [39]

These arguments were used regarding the protection of the *image* as a special form to protect the right to privacy. [40] Moreover, the negative impact of the *right to self-image* was described. It is the right not to consent access, reproduction and publication of the image to third parties who lack authorization of the owner to do so.

In this respect, the Supreme Court of Spain has argued that the protection of the image "is guaranteed by recognizing the power to prevent unconditional dissemination of the physical appearance since it represents the first element to create the personal area of each individual. It is a basic instrument for external identification and projection as well as for self-recognition of the individuals as such". [41]

[38] Cfr. Nino, page 304 and subsequent pages.

[39] Cfr. Joint Habeas Data Action filed by ADC.

[40] Cfr. Human Rights Council. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*. A/HRC/17/27. 16 May 2011, paragraph 58.

[41] Cfr. SSTC 231/1988; 99/1994; 81/2001; 139/2001; 156/2001; 83/2002.

The image as sensitive data

ADC argued that images represent, in many cases, sensitive data pursuant to Law 25326 which defines them as "personal data revealing racial and ethnic origin, political opinions, religious, philosophical or moral beliefs, labor union membership, and information concerning health conditions or sexual habits or behavior".

The face of individuals may reveal –at least in many cases– their racial origin or even their religious beliefs. In fact, shameful acts of racial discrimination such as Jim Crow laws from southern United States or the *apartheid* in South Africa were based, almost entirely, on the skin color of people. Given the risk they pose to personal autonomy, this type of data deserve higher standards of protection than common personal data. The possibility to create databases with racial or ethnic origins of citizens and the fact that such data may be analyzed or classified automatically through algorithms which detect certain facial features evidences the nature of the risks created by the careless processing of data involved in this situation.

Such possibility increases with the use of automated facial recognition systems. This is possible through the analysis of the individual's facial features obtained from the image which is compared online to other images contained in a database. In practice, an "unknown" image is taken and compared to other image of the same face in an assembly of "known" images. In the case under consideration, the images uploaded to the online electoral roll belonged to the group of known images which included certain information that made the identification of individuals possible (name, surname, DNI, section and electoral circuit).

Violation of the principles of specification of purpose and proportionality

The incorporation of photographs to the National Electoral Register as a result of a communication of data made by the Renaper violated the principle of specification of purpose which is key for regulating the protection of personal data. This principle set forth in Section 4.3 of Law 25326 establishes that "the data subject to treatment shall not be used for any purpose or purposes which are different from or incompatible with those giving rise to their collection". In fact, the photographs of the new DNI were provided to be incorporated to the databases of Renaper and to the new DNI. The incorporation of such data to the National Electoral Register clearly represents a purpose different from the one established in Law 25326 and is, as a consequence, forbidden by law.

They are two separate registries with different legal purposes. The first one is the National Registry of People created by the Law 17671 with the purpose of gathering data of the entire Argentine population and of exercising the powers recognized in Section 2 of such law. The second one is the National Electoral Register, which is regulated by the National Electoral Code and has the purpose to register Argentine citizens who are entitled to vote in order to prepare the electoral rolls. From our point of view, the clear difference between the purposes of both registries makes it impossible for one registry to use the data collected by the other.

Moreover, the incorporation of photographs breaches the principle of *proportionality* which is also key to any protective framework of personal data. Indeed, the storage and use of personal data affect the right to privacy and thus must be strictly analyzed according to their proportionality. [42] As a consequence, the State must justify why the incorporation of citizens' photographs to the National Electoral Register is required in order to prepare the electoral rolls and why it represents a legal purpose of the State. In view of the fact that the electoral system has worked properly with a minimum quantity of data for years, a greater quantity of such data represents a higher influence on the right to privacy. ADC considered that the constitutionality of such influence was doubtful since there are no apparent reasons to believe, from a constitutional point of view, that the performance of the electoral system requires such a change.

Therefore, ADC has challenged the constitutionality of Sections 15 and 17 of the National Electoral Code since they set forth the incorporation of photographs to online electoral rolls and the transfer of data from the Renaper to the National Electoral Register. ADC has also challenged the constitutionality of the Decision 18/13 of the National Electoral Chamber which establishes the incorporation and organization of the photographs of voters to the electoral rolls without the necessary statutory and constitutional provisions of the case.

Lack of consent and of information

As mentioned above, although the communication of data was authorized by law, we challenged the fact that the duty to *inform* during such communication was breached: we considered that such duty –which is set forth in Section 11 of the Law 25326– is independent from the previous consent of the data owner. Such duty to inform allows citizens to know who storages and processes their personal data, which enables them to keep certain

[42] Cfr. Human Rights Council. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*. A/HRC/17/27. 16 May 2011.

control over such data and to monitor that they are not misused.

Insecurity on databases

Finally, a large part of the argument of ADC was based on a particular matter concerning how data had been uploaded to an online database which may be consulted by citizens. In fact, ADC emphasized that the security measures of databases which were consulted through the website of the electoral roll were not enough and thus all the information contained therein was at risk and the State had the duty to adopt urgent security measures.

Indeed, the information contained in the online electoral roll had been uploaded to private websites based abroad[43]. According to ADC, "the careless processing of such data by the National Electoral Chamber has placed them at risk and thus affected the rights to privacy and intimacy of all voters".

Subsequent events

The concerns regarding the deficiencies in the security of databases were verified a few weeks after the joint habeas data action was filed by ADC, the intervening judge having failed to adopt the precautionary measures which had been requested. In fact, before the action having been filed by ADC some deficiencies have already been detected: in August 2013 the blog Segu-Info reported to Computer Emergency Response Team from Argentina (ArCERT) the vulnerable condition of databases, no measures having been taken by the relevant authorities. This vulnerable condition had also been reported by Enrique Chaparro in a letter sent to the National Electoral Chamber. The only response was to remove –temporarily– his photograph from the online consultation system.

After the recourse of amparo was filed by ADC, such alleged vulnerable condition became real: in October 2013, a 16 year old boy found out how the online consultation website of the electoral roll was connected to the database of the National Electoral Chamber. Specifically, he detected how the application of the National Electoral Chamber for Android systems was connected to a database hosted in a server of the Ministry of Internal Affairs under a base64 secure data encryption system which is –as the young boy argued– "a reversible encryption algorithm, that is, not enough secure". [44] Since the Android application was programmed in Java, the original code was easily accessible and so it could be checked that the encryption system only replaced certain letters for others.

[43] For example, the website: www.argentinaelecciones.com.

[44] Cfr. Another Bit in the Wall. 20 October 2013.

> "By converting this pseudo-code into any programming language, one can arbitrarily apply queries to the database of the Electoral Roll with the risks involved: the data of any individual, such as the one holding the DNI number 1(...), can be requested without providing any other kind of information, only the DNI number and the sex, without captcha, without any limitation" (the highlighted belongs to us). [45]

A few days after this warning, somebody published anonymously at the website Jsfiddle.net a complete code which could be used in such website to obtain the photographs of the electoral roll. The *Privacy* Area of ADC used that code for one night and obtained the photographs of more than 5,000 Argentine citizens. Such information was submitted as part of the evidence of the recourse of amparo filed by ADC and the final judgment is still pending. The National Electoral Chamber eliminated the system when the news regarding the vulnerable condition reached the media.

Within the framework of the proceeding, the intervening judge requested a report to the *Department of Technological Crimes* (División Delitos Tecnológicos, DDT) of the Argentine Federal Police in order to analyze whether the facts alleged by ADC were in fact possible. The report from 10 June 2014 is concise: it only explains in two pages that DDT's technicians entered the websites where the code which allowed the users to download the photographs of the electoral roll had been uploaded. In this regard, DDT explained the following:

> "It should be noted that in order to carry out such task, the code must be used as it was published, in any server of Internet contents since such code is a **basic programming code** which does not include any SQL injection technique, or any similar technique, that allows the obtention of a large amount of data. On the contrary, it is a code which uses the website programming and evidences its security" (the highlighted belongs to us). [46]

As it may be seen, the expert opinion ordered by the Court proved that the complaint filed was true: the programming code was in essence vulnerable and the photographs of millions of Argentines was made available to any individual with basic programming knowledges. As of the completion of this report, the first instance ruling was still pending.

[45] Id.

[46] Judicial Notice of the Argentine Federal Police. Office for the Fight against Organized Crime. Computer Crimes Department. Received on 14 June 2014 at the Federal Court No. 1 in charge of María Romilda Servini de Cubría, in the case entitled "ADC c. Cámara Electoral s/ amparo ley 16.968, Expediente 3246/13".

V Conclusion and recommendations

The present report has tried to shed some light on the manner in which the State handles our personal data. Although in some cases it is possible to verify adequate security practices, such as the AFIP's safe room, it is also possible to see that those practices are not the result of public policies implemented by the authority in charge of the protection of Argentine citizens' data, that is, the National Bureau of Personal Data Protection (DNPDP). Said entity, which was thought out to be self-governed and independent, has been limited in its action capacity by low budget and low human resources allocations. Additionally, its operations made the DNPDP take a turn towards control, which is limited by the aforementioned reasons, over private parties. This means that the State seems to be absent under the DNPDP's gaze, and that is possibly the result of a large range of authorizations granted by Law 25326 to the treatment and use of personal data within the State. Accordingly, when the DNPDP gets close to one of the many serious problems concerning data, such as those created by sites that issue reports on private individuals, it only scratches the surface. To illustrate this, in the framework of complex sanctioning proceedings, with limited action capacity, the DNPDP cannot get to the bottom of the problem and this is all linked to the poor use of personal data on the part of the State.

The case of the online electoral roll is one example of that poor use, which is, however, highly revealing.

Indeed, the case shows that security measures would be strengthened if uniform criteria were adopted. For example, if the Renaper's data were in a *safe room*, that effort would be useless if the information is transferred to a party following insecure practices such as the ones adopted by the National Electoral Chamber. Consensual criteria for security do not seem to be present. For instance, after ACD's requests to access to information, it was established that server security depends on the technical areas of each department. It is unknown if those technical areas are coordinated. However, as revealed by the electoral roll case, they do not seem to be.

Furthermore, it is noticeable that transference and communication of data processes from Renaper to the National Electoral Chamber went completely unperceived for the DNPDP. This is probably related to the legal authorizations existing in that case, and to the significant fact that nobody has deemed necessary to ask the DNPDP to issue a ruling on that transference. As far as we know, the DNPDP did not intervene sua sponte neither. Permissive laws towards the State, as well as a subordinated enforcement authority, obstruct, rather than enable, the DNPDP's roles of control and defense of rights.

Finally, it should be noted that the DNPDP's role of control, and its powers and duties assigned by law widely exceed its budget and organization.

Beyond the flaws in the design of the law, which is a consequence of the presidential veto at the time the law was passed, the truth is that those flaws were ratified, year after year, through budget allocations. The DNPDP simply lacks resources to do what it is expected by law.

This report leads to, at least partially, certain conclusions that allow to think of an agenda of defense and protection of the right to privacy towards the future. This agenda cannot just be the result of the analysis of an organization, such as ACD in this case, that has sought to study the operation of the data protection system in practice. This agenda must be the result of a flowing dialogue among different parties interested in the defense of a fundamental right in a modern democracy. This report seeks to be a contribution in what we deem to be a necessary debate. Here are some recommendations we believe can inform a debate process over an agenda concerning privacy for the next years.

VI Recommendations

- **Law 25326 itself should be revised**. Indeed, the enforcement authority created by the law must be truly independent and must guarantee suitable financing for itself, so that it can comply with important functions of defense of the rights assigned by the law. It would be convenient to explore models of the *Privacy Commissioner* of some Anglo-Saxon countries, which seem to have succeeded in the defense of citizens' personal data.

- **Revision of Law 26,326 cannot be made in an isolated manner**. ADC considers necessary to analyze the Law taking into account the enactment of a law of Access to Public Information. Both rights, access and data protection, can come into conflict. We believe it is necessary that the Argentine legal framework accounts for the tension between the two of them and determine, with the utmost possible degree of certainty, those cases in which access must be prioritized and those cases in which privacy protection is imposed.

- **Storage capacity and communication of data within the State must be limited**. The current law is, as mentioned, too permissive. This would allow, not only to maintain a stricter control over governmental agencies, but also to avoid any risks of data falling into private hands and be exploited by private entities for commercial purposes or other kind.

- **Transparency and consensus on security criteria must be worked on**. It would be desirable that a public agency, which may be the National

Office of Information Technology (ONTI), establish consensual security criteria, which should be made public. Unlike the DNPDP, which prevented certain security guarantee details to be revealed, knowledge of those guarantees does not increase vulnerability for systems, but it allows citizens to evaluate it their data have the level of protection they deserve.

References

[1] Juan Antonio Travieso María del Rosario Moreno. La protección de los datos personales y de los sensibles en la ley 25.326. *La Ley*, (14/07/2006), Julio 2006.

[2] Roberto Gargarella. Constitucionalismo y privacidad. En Roberto Gargarella, editor, *Teoría y Crítica del Derecho Constitucional*, volume II, páginas 779–793. Abeledo-Perrot, Buenos Aires, 1a. edición, 2008.

[3] Carlos Santiago Nino. *Fundamentos de derecho constitucional: análisis filosófico, jurídico y politológico de la práctica constitucional*. Astrea, 1992.

Contents

List of Tables

ADC / Asociación por los Derechos Civiles

This report was produced by the Privacy Area of the Asociación por los Derechos Civiles (ADC), as part of the Cyber Stewards Network and with the financial support of the International Development Research Center, Ottawa, Canada.