Personal Data Protection and Online Services in Latin America [*]

Alberto J. Cerda Silva

INTRODUCTION

When the government of Chile announced the monitoring of online social networks, like MySpace and Twitter, it created such broad citizen outcry that government was forced to drop the initiative. When Facebook unilaterally modified its privacy policies disclosing the participation of Iranian citizens in antigovernment groups, the government's security groups adopted repressive measures against those citizens and their families. When the government of Venezuela published online the list of supporters of a request for a national referendum, it generated cross persecution between its supporters and opponents. In spite of their differences, each of these cases makes clear how adequate protection of personal data can guarantee the exercise of freedom of speech and other fundamental rights, and also the critical role that the Internet plays in preserving those rights.

Personal data protection satisfies public interest purposes that are inherent to democratic societies. That protection not only satisfies individual needs for privacy but also safeguards the free exercise of fundamental rights. Thus, for example, imposing limitations on the processing of personal data about political, religious, and sexual choices protects the free exercise of the right to association, the freedom of thought, and sexual self-determination, among others. The opportunity to exclude oneself from society whichever the legal approach – namely the inviolability of home and communications, the right to privacy, the right to protection of personal data, and even the right to a secret vote– preserves a space for free expression and the full development of personality, which are essential objectives for democratic order.

Recently, some authors have made a series of arguments to erode the right to protection of personal data. They have said protection should limit only to private information. They have contended the concept of personal data is extremely broad which creates legal uncertainty. They have claimed that the mere consent of a data subject is enough to justify any processing of his data. These arguments are not due to free speech concerns but result from the desire for

---

[*] This essay attempts to reduce to writing the participation of the author in the workshop *"Freedom of Speech and Internet: Issues on Regulation in Latin America"*, organized by the Center for Studies on Freedom of Expression and Access to Information of the University of Palermo Law School, in Buenos Aires on September 12 and 13, 2011. The author wants to express his deep gratitude for being invited to take part in that event.

having a legal environment more inclined towards an immune and unpunished trafficking of personal information.

These arguments that tend to erode an adequate protection for personal data have been particularly officious when applied to the Internet; in fact, they have been put forward with the purpose of providing larger flexibility to online service providers. Suffice it to recall some recent situations, such as the contextual advertisement and streets view by Google, the geographic information system by Apple, the unilateral modification of privacy settings by Facebook, and online passport by Microsoft. In facing each of them, European authorities on data protection have reacted energetically and, as was predictable, the progressive adoption of similar measures in Latin America has raised concerns among online service providers within the region.

This essay discusses each of the abovementioned arguments that attempt to diminish adequate levels of protection for personal data. The first section posits the real protected juridical good (i.e., values and goods protected by legal system) and rejects the argument that it is merely the right to privacy. The second section contests the statement that Latin American law on data protection is excessively protectionist when it defines personal data. The third section emphasizes that mere consent is not enough to legitimate the processing of personal data. The fourth section attempts to reveal the actual purpose of those arguments and, in contrast, expresses its concerns on the role that online service providers have on data retention in Latin America. Some brief comments and conclusions finish this essay.

I. PERSONAL DATA PROTECTION AS AN AUTONOMOUS RIGHT

Countries started enacting legislation on personal data protection in the seventies, as a reaction to the increasing power of technologies for processing personal information and, consequently, using it for illegitimate purposes of social control by governments. In order to provide an integral protection, the scope of the regulation has been progressively extended. To avoid the circumvention of such regulation, particularly in sensible areas like data processing in the health sector, which resisted automation and stuck to paper, governments extended the scope of regulation also to manual processing. Similarly, as the technology was available not only for government but also for the private sector, governments extended these laws to the processing of personal data done by non-state actors. As a result, several countries currently have comprehensives law that protect people from manual and automatic processing of their personal data by both the public and private sector.

Data protection laws initially focused on the right to privacy. In part, because the central concern was safeguarding personal information from its potential misuse, especially sensitive data about people's intimate spheres. In part, because the conceptual development of legal theory did not have any other more proper juridical good to support that protection. As Warren and Brandeis did, when they constructed the right to privacy from the right of property, the right to

protection of personal data was initially built on the right to privacy. However, in the civil law tradition, to which Latin America is party, the right to privacy and the right to protection of personal data are currently two different legal entities.

The right to protection of personal data became autonomous in the early eighties. In 1983, the Constitutional Tribunal of Germany, which has been particularly cautious about controlling the laws that empower government for processing personal information, declared the Census Act unconstitutional. In doing so, it held that «*...the general right of personality... includes... the power of a person, derived from the idea of self-determination, for deciding basically by herself when and within which limits disclose situations about her own life*». Similarly, in 1998, the Constitutional Tribunal of Spain identified «*an autonomous fundamental right to control the flow of information about oneself being or not part of the strictest scope of intimacy, in order to preserve the full exercise of his rights*». This right, known in the legal scholarship as informational self-determination or informational freedom, allows people to control the information about themselves, whether that information is public or private.

In Europe, the right to protection of personal data has not only scholarly acceptance but also legal one. In fact, several constitutions have recognized it as a right distinct from the right to privacy. Even more, the Charter of Fundamental Rights of the European Union, adopted at Nice on December 7th 2000, draws a clear distinction. After recognizing the right to respect for private and family life in its article 7, article 8 recognizes that «*Everyone has the right to the protection of personal data concerning him or her*», and sets forth, from a human rights viewpoint, the minimum exigencies for the adequate protection of this right.

In Latin America as well, the right to protection of personal data has constitutional recognition. In general, the constitutions of the region not only recognize the right to privacy but also the so-called *habeas data*, which is the right to protection of personal data. This right exists, with some differences, in the constitutions of Argentina, Brazil, Colombia, Mexico, Peru, and Venezuela. But even in those countries where blurring between the concepts still persists in their constitutional texts, it has been overcome by their constitutional courts, which have recognized the right to control personal information; this is the case, for instance, of a recent decision of the Constitutional Tribunal of Chile that recognized expressly the right to informational self-determination, even when it is not express in the constitution, by declaring the unconstitutionality of a law that required cybercafés to record their users' personal data for purpose of criminal enforcement.

Comparatively, Latin-American constitutionalism has been more efficient in safeguarding the right to protection of personal data. First, by recognizing it as an autonomous right. Second, by providing constitutional remedies for its protection, thought the *acción de amparo* –also known as *acción de tutela* in Colombia, *recurso de protección* in Chile, and *mandado de segurança* in Brazil– and an specific action for personal data protection, which is also called *habeas data.* Third, unlike the U.S. Constitution and with more emphasis than in European

constitutionalism, constitutions of Latin American countries recognize rights and remedies not only against the public sector but also against non-state actors. As a result, even when lacking specific laws on the matter, several countries of the region grant the right to protection of personal data at the constitutional level when the government processes personal data, and also when telecommunication companies and providers of credit report process personal data infringing the fundamental rights recognized by the constitution.

However, constitutional protection has not been enough for guarantying an adequate level of protection for personal data in Latin America. This is because that protection takes place after the fact, before courts, which makes clear several limitations, such as its high transactional costs, its inefficiency in preventing infringement, and its lack of experience on various technical issues. Moreover, as in other civil law countries, in Latin American countries, judicial decisions lack *stare decisis* (*i.e.,* judicial precedents are not legally binding in future cases), except in some highly limited exceptions. In the praxis, this forces data subjects to (re) start individual legal actions from scratch each time their data is illegally processed; for instance, Equifax and its domestic affiliates in Latin America have been sued over and over for identical infringements when issuing credit reports.

Constitutional precepts are too general and, thus, allow too much for interpretation. According to Robert Alexy, constitutional provisions set forth principles which when applied in a concrete case may result in equivocal or ambiguous rules. This has been the case, for instance, in the so-called *right to be forgotten* in relation with processing of personal data on debts after they have been paid. For the Supreme Courts of Argentina and Costa Rica, processing personal data on paid debts infringes fundamental rights, whereas for the Supreme Court of El Salvador it does not. This clarifies that protection based on pure constitutional precepts is insufficient and creates some legal uncertainty for both data subjects and data controllers.

Latin America is adopting comprehensive laws on the processing of personal data, that is, laws that regulate automatic and manual processing of personal data by both the private and public sector. Several reasons explain this phenomenon: new democratic spirits that encourage providing an adequate protection for people's rights; the desire for minimizing the legal uncertainty of a protection model based on mere constitutional provisions; and, most importantly, the aspiration for becoming nations that provide an adequate level of protection for personal data, according to the European Union's standards, in order to access cross-border transferences of such data and, consequently, facilitate investment in those niche markets that require processing personal data that comes from the European Union. By making these changes, numerous Latin American countries may soon join Argentina, which was recognized early as a safe country: Uruguay is imminent; meanwhile, Colombia, Costa Rica, Mexico, and Peru have already modified their domestic law for that purpose; Brazil and Chile also have bills pending before their legislatives with similar intentions.

The Latin-American model of protection for personal data is in a phase of transition. A few years ago, personal data protection was situated in constitutional provisions and various different laws, which made the regulation fragmentary and sometimes inconsistent. Currently, in the main economies of the region, constitutional protection overlaps a comprehensive law that regulates the processing of personal data by both the public and private sectors. As a result of this overlap of constitutional and statutory rules, personal data protection in Latin America appears strong, but countries still need to work on law enforcement.

Limiting personal data protection to private data, therefore, misunderstands the nature of the protected juridical good. Stating that personal data protection should be limited to private data ignores the ideas historic progression by taking legal theory and jurisprudence back more than 30 years. This confusion between privacy and data protection also introduces serious difficulties for setting limits on protecting data, because of numerous and contradictory theories around the extension of privacy, an issue authors have written abut vastly and which is beyond the scope of this essay. Limiting protection to privacy, moreover, would diminish protection for people and damage international legal harmonization, high costs in a globalized environment. Instead, the right to protection of personal data guarantees to people control over information about themselves independently of whether it is private or public, by passing completely the muddle concept of privacy.

Obviously, supporting the extension of the right to protection of personal data beyond privacy does not prevent protecting person's intimate aspects. This is exactly what is achieved through a reinforced protection for so-called sensitive data, thus is, data that discloses information that deserves special protection because of the higher risk posed by its processing to citizen's rights and freedoms. According to the United Nations *Guidelines concerning computerized personal data files* (1990), processing this data may cause illegal and arbitrary discrimination. That is the case of data about people's racial and ethnical origins; their color and sexuality; their political, religious, philosophical, or other beliefs; their participation in a given association or their membership in a trade union. Some countries, according to their own experience, add to the list genetic information, political affiliation, and other data. All Latin-American countries that have data protection laws provide a reinforced protection for sensitive data.

In sum, even when there is an overlap between the right to privacy and the right to protection of personal data, the latter is autonomous, and guarantees a person's right to control one's own information, independently of whether such information is public or private. The opposite would reverse the progression of fundamental rights in general and data protection in particular.

II. THE PROPER SCOPE FOR CONCEPTUALIZING "PERSONAL DATA"

A second argument that attempts to minimize personal data protection in Latin America states that those countries within the region that have adopted laws on the matter have mistakenly and excessively extended the scope of protection

not only to data about identified people but also to data about identifiable people. This implies that the scope of the regulation includes not only data related to a person who is already unequivocally individualized, but also data about an unidentified person who is susceptible of being identified. This is exemplified by, for instance, the case of data associated to the unique tax number in Chile, the social security number in the United States, the fiscal identification number in Spain, or someone's fingerprints. In all these situations, it is possible to identify the person to whom data refers through a later procedure.

The protection of personal data actually extends over data related to identified and identifiable people in all international instruments and domestic laws on the matter. In fact, since the Organization for Economic Co-operation and Development (OECD) *Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data* (1980), through the *Data Protection Directive* adopted by the European Union in 1995, to the most recently *APEC Privacy Framework,* adopted in 2005 by the *Asia-Pacific Economic Cooperation*, all and each international instrument on the matter extends its protection to both identified and identifiable people. Latin American law does similarly than comparative law. Therefore, stating that countries from Latin America have made a mistake is, at the very least, wrong.

Extending the right to protection of personal data to data about identifiable people guarantees an integral protection. It avoids defrauding the purpose of the law by using a technical subterfuge that delinks data from people in appearance. If a person is potentially identifiable, such as in each of the aforementioned examples, the law applies, the data subject enjoys her rights, and the data controller must comply with its legal duties and is potentially liable. Therefore, the protection extends to data about identifiable people.

Protecting data related to identifiable people guarantees updating the law to meet the continuous changes in technology. In that way, people do not become unprotected because of technical progresses that allow associating them with given data. If it is possible to link data with a person –according to the state of art in fields such as dactyloscopy, biometry, genetic, or mere crossing of databases– allowing personal identification, that processing of data is under the scope of the personal data protection law. This brings us to the root of the problem, at least for online service providers: the IP address.

An IP address is a numerical identifier that allows identifying a device connected to the Internet. It is an essential part of the protocol of Internet communications, much like a telephone number for phone calls. However, unlike with phone numbers, generally speaking, an IP address is not assigned permanently to a particular subscriber, instead it is assigned to users on request for connecting to the Internet by the company that provides them access to the Internet from the pool of numbers that it manages. This allows Internet service providers to link IP addresses with their subscribers' information and, potentially, to identify a given user connected to the Internet. Consequently, because data is

susceptible of being linked to a given person, the processing of that data must comply with personal data laws.

Online service providers argue that IP addresses are not personal data and they should be excluded from the scope of the law. According to them, IP addresses were not adopted for identifying users but devices; therefore, an IP address allows to determine the equipment that took part in the communication, but it does not identify who used that equipment.

European data protection authorities, instead, state that processing of IP addresses is under the scope of personal data protection law. In fact, even if the initial technical purpose of IP addresses was only facilitating online communication, they actually allow identifying some users; as a result of that capacity, several countries have adopted special rules on retention of traffic data, including IP addresses, for the purpose of criminal enforcement, because they facilitate identifying supposed infringers. This is the case of the *Data Retention Directive* adopted by the European Union, the *Convention on Cybercrime* adopted by the Council of Europe, and even the *Digital Millennium Copyright Act* in the United States.

New standards for online communication will increase the risk of processing IP addresses. The current protocol IPv4 has a limited sequence of numbers, which forces users to share them and manage them through their Internet service provider. However, the protocol IPv6, which already has been implemented in several countries, increases those numerical sequences exponentially. Soon, this will allow not only our computer, cell phone, and GPS to connect to the Internet, but also our vehicle, home security system, and even some appliances. IPv6 will allow continuous connection to the Internet and, therefore, a larger processing of personal data of those users whose devices are connected.

In sum, domestic laws adopted by Latin American countries have done well by inclusively conceptualizing personal data as data about identified and identifiable people. That concept guarantees legal compatibility with overseas law, an integral protection for people's right to control information about themselves, and the adequacy of law to progress in science and technology, particularly related to identifying online users.

III. CONSENT AS LEGITIMIZATION FOR DATA PROCESSING

The right to protection for personal data grants to its right holder the control over the information about herself. The right holder determines to whom, when, and how to provide her personal information. Even more, she decides when and how to exercise the rights granted by law, such as access to her data, and requiring its modification, its elimination, or even its blockage. Therefore, excepting cases provided by law, personal data processing requires the consent of the data subject. In fact, even with authorization, the data subject may revoke her consent and, consequently, hinder any later processing of her data. Consent is therefore essential for legitimating personal data processing.

However, sometimes consent is not enough to validate personal data processing. For instance, an employee's acquiescence to his employer allowing the employer to access to the employee's e-mail, or a consumer's consent to her provider allowing the provider to transfer the user's personal data to third parties; in those situations, consent appears conditioned on the relationship in which it takes place. The consent obtained there, wherever contractual form it takes, is constrained. This has led some countries to adopt special rules that protect employees and consumers in relation to personal data processing by their employers and providers.

The consent for processing personal data is still more problematic with regard to the Internet and online services, particularly when the validity of consent rests on being informed and provided freely. The level of information available for an average user in relation to the opaque functioning of information technologies is questionable. It is still arguable in the case of an advanced user because of the information asymmetry between her and her service provider. Similarly, freedom of consent is likewise debatable when it is given to a non-competitive service provider; in most of Latin America, access to the Internet is a monopolistic service, in the best case an oligopolistic one. This situation puts the user in the unfortunate dilemma between consenting to her personal data being processed to get Internet access and safeguarding her personal information by staying off line.

Online social networks have specific problems in relation to the real consent given by their users. This is explained by the so-called *network economies,* in which the best service provider does not necessarily prevail but the one capable of bringing together a critical mass of the demand for services does, by providing access not only to its service but to its network. For example, when a given user has the chance to choose between several telephone providers under similar economic conditions, the user will select the one that provides preferential access to a broader network of subscribers or additional services. This has been the case of users of the Microsoft's office suite, the instant messaging service of Gmail, and the apps for Apple's devices. In Chile, this is the case of Facebook, the online social network that 50% of Chileans use; it is natural that any new Chilean user will tend to choose that service because of the comparative advantages of accessing such a broad network of users, without careful consideration of the privacy policies of the company.

The limited protection that mere consent provides to data subjects has led legislators and data protection authorities to the adoption of some corrective measures. One of those measures is requiring that personal data processing must comply with the purpose that justified its collection, the one that was informed to data subject when she consented. For instance, processing of personal data during a hiring process for employees must be limited to information needed for establishing the labor capacities of candidates; requiring data beyond that purpose, even when consented to, is an illegal processing of personal data. Paraphrasing the aforementioned United Nations Guidelines on the matter, processing of personal data must be adequate, pertinent, and non excessive in relation to a legitimate purpose. This raises concerns about some practices of

online processing of personal data, such as Google's contextual advertising and Facebook's system for facial recognition of users.

Additionally, limiting all the legitimacy of processing personal data to contractual terms eludes the public responsibility to safeguard the fundamental rights of users. Transactional costs of enforcing the law on a case-to-case basis are high and abandoning the respect of law to *laissez-faire* is leaving it to chance. This is particularly disastrous when users are contractually forced to solve their differences with their providers before foreign jurisdictions. Precisely, the need for emphasizing the protection of people in relation with their personal information has led most developed countries, and progressively also Latin American ones, to establish a public authority that enforces the law.

In sum, except in those exceptions set forth by law, the consent of data subject is necessary for a legitimate processing of personal data, but it is not sufficient. Processing must also comply with other norms of personal data protection law, in particular that the processing of data must be adequate, pertinent, and non excessive in relation to a legitimate purpose.

IV. RISKS ON PROCESSING PERSONAL DATA BY ONLINE SERVICE PROVIDERS

Arguments that attempt to reduce the protection for personal data based on limiting it to private data, about identified people, and subject to mere contractual measures have a motive. Through those arguments, online service providers try to achieve a legal environment more favorable to provide services, by removing legal obstacles that obstruct the functioning of their version of the Internet. This is, in some cases, the environment that those providers have enjoyed in their country of origin: the United States. With the purpose of promoting the Internet, some time ago, the U.S. Congress awarded legal immunity to online service providers with respect to content provided by third parties, but excepting contents that infringe copyright. In practice, this has granted not only immunity but also impunity to online service providers for users' infringements, even if the former had actual knowledge of it. The right to privacy and the right to protection of personal information, as they are understood in civil law countries, have been diminished as a result of this policy.

The features of the Internet suggest the necessity for some special rules on online personal data processing. For instance, those norms are required for the automatic collection of data, which is inherent for the technical functioning of networks, such as in the situations of IP addresses and cookies. Similarly, the hosting of content by third parties raises doubts about the potential responsibility of those that provide the service of storage for that content. Expressing consent, identifying users, protecting children online, among other issues, require adopting appropriate rules for the online environment.

However, adopting specific rules for processing personal data on the Internet cannot derogate the right to its protection. In some cases it may be necessary to adopt some flexibilities, safeguards, and limitations. For example,

with respect to the aforementioned *right to be forgotten*, that supposes no processing of personal data in some given cases, such as criminal and administrative sanctions, and debts already paid. In those cases, processing of personal data is based on legitimate purposes, such as recovering a debt or imposing a punishment; however, once that purpose is accomplished, the data must be erased or blocked, according to what is set forth in domestic law. That elimination or blockage must also take place on the Internet. Even so, recognizing the right to be forgotten must leave some exceptions, such the need for allowing processing of personal data for purposes of journalistic, historical, and scientific research. Through those flexibilities, safeguards, and limitations, the right to protection of personal data stays in place, but recognizes some exceptions in order to comply with compelling public interest purposes.

Adopting specific rules about processing personal data on the Internet, as has been suggested, will also require determining the liability of online service providers for online infringements. That liability is clear when a single service provider processes personal data illegally, for example, by collecting users' data surreptitiously or linking information to people without asking them. The situation is more complex when splitting liability between service providers and content providers. In the latter case, guarantying complete immunity is as antagonistic to the adequate respect of third parties' rights as forcing service providers to censor content just because it does not please some person, without even a court order. However, in Latin America a more serious problem seems to be the retention of users' personal data by online service providers and its subsequent use.

Unlike with data protection law, there is less progress on regulating data retention by online service providers in Latin America, that is, collecting and preserving collected data about the provider's users, such as their assigned IP addresses, date and time of connection, and others. Some providers have been forced to process that data for purposes of pricing and controlling access to their services, but other providers do it only because of legal obligations set forth by law to facilitate identifying users.

Unfortunately, data retention regulation in Latin America is neither harmonized nor uniform; in fact, some countries do not have it at all, and those having one are tailored to domestic law that satisfies different legislative impulses. For instance, Argentina lost its data retention law, after its Supreme Court of Justice declared it unconstitutional in the highly controversial Halabi case. Of course, both constitutional provisions and data protection law apply, but they are not enough for a complete and proper regulation of data retention. In Mexico, the federal telecommunications act regulates data retention, whereas in Chile, the criminal procedure code sets forth rules on the matter, in the context of identifying suspects in the cases of child pornography and other serious crimes. Differences in legislative impulse are important, because they affect the legislature's carefulness in drafting the law.

One of the critical aspects for regulating data retention by online service providers is adopting safeguards for fundamental rights of people to whom the

information refers. It is necessary to determine what kind of service provider is obligated to keep data, what data, how, and for how much time it must be preserved. It is also essential to set forth to whom and under which conditions the data may be disclosed. Adopting adequate regulations is difficult; in fact, constitutional objections against the regulation are usual. In addition to the recent decision about the unconstitutionality of several data retention provisions adopted by the Constitutional Tribunal of Germany, and the aforementioned decision of the Supreme Court of Justice of Argentina in the Halabi case, the recent judgment by the Constitutional Tribunal of Chile held unconstitutional a system of registering cybercafé Internet users, that was intended to complement the obligation of Internet service providers to keep users' data. All those decisions have emphasized the need for appropriate safeguards of users' information when imposing on online service providers a legal duty to keep users' personal data.

In the coming years, Latin American countries, particularly those that have signed free trade agreements, have committed to adopt special norms on personal data retention in order to enforce intellectual property. In fact, Chile already implemented that commitment, leading to a severe inconsistency in which users' data is available for purposes of enforcing the law in serious crimes and in any copyright infringement. In Colombia, the bill called *Ley Lleras,* which attempts to implement similar commitments into domestic law, has caused citizens' reprobation, forcing the government to redraft the bill and delay its legislative discussion. The same is foreseeable in other countries in the region that have became parties to free trade agreements (e.g., Peru, Dominican Republic, and El Salvador) or are considering its adhesion to new international instruments on intellectual property (e.g., Mexico).

In sum, processing personal data on the Internet creates serious challenges for online service providers, for users, and for governments within the region to adopt practices and norms that satisfy legitimate purposes of public interest and an adequate respect of the right to protection of personal data. Regulating data retention is maybe the most critical issue for the coming years.

V. CONCLUSIONS

The right to protection of personal data satisfies more than the mere individual interest of someone for seclusion, this right protects the public interest in respecting people's fundamental rights and preserving conditions that are inherent to democratic societies.

Latin American countries have made significant progress on personal data protection, passing from a model of protection based on constitutional provisions to one complemented with comprehensive legislation. This process has granted more integral protection, incremented legal certainty, and advanced international legal harmonization.

The Internet raises new challenges for personal data protection in online environments. It suggests the need for special norms. In this context, it has been

argued that protection should be limited to private data, about determined people, and that contractual measures should prevail. This essay has discussed each of those suggestions, because, instead of adopting adequate norms for online environment, they would limit seriously the right to protection of personal data, sacrificing each of the achievements obtained to date.

Among the multiple relevant issues, in the coming years the adoption of data retention law allowing online service providers to preserve users' data will be a critical point. Whatever interest pushes the regulation, it must not omit the inclusion of appropriate measures to safeguard the rights of people to whom information refers. Increasing the efficiency of law cannot be achieved at any price. The right to protection of personal data cannot be sacrificed, because its detriment affects not only the person to whom the information refers but also the survival of human rights and the very foundations of democracy.