laws

MDPI

Article

The Proportionality and Solidarity Principles and Their Impact on Privacy Laws in German Jurisprudence

Klaus Schmidt [1,*] and Alejandro Laje [2]

[1] Department of Technology, Illinois State University, 5100 Turner Hall, Normal, IL 61790, USA
[2] Faculdad de Derecho y Ciencias Politicas, Universidad Abierta Interamericana, Buenos Aires C1048AAF, Argentina; Alejandro.Laje@UAI.edu.ar
* Correspondence: kschmid@ilstu.edu; Tel.: +1-309-438-3661

Academic Editor: Jacqueline D. Lipton
Received: 13 January 2016; Accepted: 7 June 2016; Published: 15 June 2016

Abstract: Privacy laws and the use of information technology that guarantee confidentiality and information integrity are components of an individual's rights in German jurisprudence. The protection of a person's identity, information, ideas, feelings, emotions and particularly the way to communicate them is considered essential to human dignity. Extensive studies in these areas has made this protection a central pillar of law-related research in Germany.

Keywords: principle of proportionality; principle of solidarity; German jurisprudence; analysis of cases; international jurisprudence

1. Introduction

Privacy laws and the use of information technology that guarantee confidentiality and information integrity[1] are components of an individual's rights in German jurisprudence. The protection of a person's identity, information, ideas, feelings, emotions and particularly the way to communicate themis considered essential to human dignity [1].[2] The extent of studies in these areas has made these topics a central pillar of law-related research in Germany.

Article 1(1) of the *Grundgesetz* (Basic Law) imposes an affirmative obligation upon the government to protect human dignity ([2], pp. 194–95). Regarding data protection, Germany was amongst the first countries to enact a national law protecting data. In fact, in 1970, the State of Hesse passed the first data protection law in the world. The first German data protection act on a federal level came into effect in 1979.

The German approach to privacy seems clear. The *Bundesgerichtshof* (Constitutional Court) has ruled to include within the right of privacy anything the individual may wish to do; only able to be restricted by law, satisfying all substantive and procedural requirements set by the constitution ([2], pp. 165–66). More specifically, limits to the scope of the right to privacy are much more broadly defined than in the United States or other European Union members. In the realm of data protection, the Constitutional Court has developed the right to informational self-determination, by which personal data in Germany are constitutionally protected. German jurisprudence has been

[1] 1BvR370/07.
[2] The Federal Constitutional Court has consistently held in its case-law that a core area of a person's private life is inviolable and enjoys absolute protection because of its particular proximity to human dignity (*see* BVerfGE 6, 32 (41); 6, 389 (433); 27, 344 (350–351); 32, 373 (378–379); 34, 238 (245); 35, 35 (39); 38, 312 (320); 54, 143 (146); 65, 1 (46); 80, 367 (373–374); 89, 69 (82–83); 109, 279 (313)).

used by international law makers as a leading example to protect data and respect human dignity. For instance, the United States legislature adopted a new data protection law following the German Constitutional Court criteria. American interest in Germany's national security jurisprudence arose because, like the United States, Germany is a constitutional democracy. Yet, in contrast to the United States, modern Germany's historical encounters with violent authoritarian, anti-democratic, and terrorist movements have endowed it with a wealth of constitutional experience in balancing security and liberty [3].

2. Purpose of this Paper

German and European Courts provide a series of principles upon which legislation is governed on both local and international platforms. The authors chose to focus on two major principles, namely the principle of solidarity and the principle of proportionality in their relation to the protection of privacy and security. Understanding both principles may help to shed light on challenges provided by the advancement of information technologies. The paper will discuss how information technology affects German jurisdiction considering that privacy and anonymity set a stage for the application of the solidarity and proportionality principles. The discussion will be concluded by an examination of the value of privacy and confidentiality. The authors will then review a set of five cases in which those principles were applied in order to demonstrate how courts may respond to unprecedented legislative scenarios that were not directly addressed in previous jurisdiction. Finally, an in-depth discussion of both principles in their struggle to adapt to new technological circumstances and the respective role of the state in this process concludes the paper.

3. Information Technology, Privacy, Proportionality and Solidarity

In order to understand the working forces involved in the dynamic legal triangle of privacy-solidarity-technology, it is important to comprehend the complexity of computational systems and the cloud. Technology has two basic resources: time (the number of steps involved processing digital data) and space (location and amount of memory used to store data). The availability of these two elements, time and space, determines, in principle, the solution of many technological problems [4]. The World Wide Web and the "cloud" are complex open-computer networks of autonomous spaces (hosts, routers, gateways) that are self-organizing and autonomous with no intervention from any central devices. It works, learns and adapts continually by information added and retrieved. Intelligent virtual organisms (agents) learn and organize themselves, and attempt to adapt to information preferences set by the users. However, the real power of the World Wide Web does not come from any one of these individual devices; rather, it comes from the collective interaction of all of them. In fact, processors, chips and displays of these smart devices do not even require user interfaces, but just a pleasant and effective place to get things done [5]. Cyberspace has now become ever more invisible to users as technologies become ubiquitous and more diffused. Cloud computing therefore means that information and programs are run and retrieved from many locations simultaneously. In other words, information technology assigns resources from where they are available to where they are needed.

How to regulate "the Web" is constantly debated, as it entails crucial issues for democracies. In many countries, the notion of "privacy" is still developing and certainly perceived in different ways. Technology can both guarantee and threaten privacy. Some sophisticated users may prefer using programs allowing almost total privacy, while others are far from being aware of the extreme transparency of their online interactions. Nevertheless, the Internet is considered a realm of freedom. Implementing boundaries on digital content may threaten to undermine public information, which is a democratic right, and it may even interfere with the very idea of accumulation of knowledge for

scientific purposes[3] [6]. However, there is an opposite and easier alternative, that is, to simply consider technological knowledge as a public good [7].

Additional challenges have entered the privacy and solidarity discussion, as governments now have access to more data than ever by surveilling Internet activities. Also challenging is the fact that the Internet is ubiquitous and therefore governments are confronted with the extraterritoriality of data privacy laws. In addition, since technology has made it possible to collect data and all types of information, and data storage has become inexpensive, it is no longer necessary to decide which information to keep and which to delete. Some IT corporations and governments may be inclined to keep information forever [8]. This may lead to the challenge that intelligence agencies around the world store huge amounts of information indiscriminately. "Wholesale blanket surveillance" [8] is being carried out around the world and intelligence agencies are capturing every conversation, search or email sent anywhere. For example, Section 702 of the FISA Amendments Act of 2008 allows the United States National Security Agency (NSA) to use data-mining programs (such as PRISM) and requires from telecommunication and Internet providers to turn over any data matching court-approved search terms [9]. The NSA also allegedly uses XKeyscore (XKS), another computer system, to search and analyze Internet data about foreign nationals across the world. The National Security Agency in the US is (lawfully) collecting and storing almost 200 million messages per day all over the world [10]. According to news magazine *Der Spiegel*, Xkeyscore, which has the ability to retroactively import several days' worth of queued metadata, has been used by Germany's foreign intelligence service, the BND, and by the Federal Office for the Protection of the Constitution [11].

Clearly, the multifaceted nature of data privacy laws requires new approaches. Two main challenges of privacy in technology-related legislation are: confidentiality, as in privacy of content; and anonymity, as in privacy of identity [9]. Technology allows for confidentiality and anonymity to be possible, although absolute privacy is a considerable risk to law enforcement and national security. Likewise, complete lack of anonymity and confidentiality may breach basic human rights. Regulating privacy issues and yet enabling proper law enforcement is currently one of the most urgent public debates. As both of these extreme options are unacceptable, a balance between privacy and public safety is needed. An adequate solution would be to ensure that individuals may enjoy privacy and confidentiality, while law enforcement may effectively operate where society for reasons of solidarity considers these operations appropriate [12]. Furthermore, when addressing difficulties created by the extraterritorial application of data privacy laws, one may consider incorporating the solidarity principle as a reference for privacy and data protection laws.

For example, technological solidarity makes information available for technical reasons, while legal solidarity requires information to be available for various social needs. There is no reasonable expectation for information to be unavailable. There is, however, a reasonable expectation for information not be used for purposes other than those previously established by law and by authorized judicial (or equivalent) request. This conceptualization of the solidarity principle therefore makes solidarity a legal instrument compatible with the plurality of legal systems across Europe while still allowing minimal common standards among individual countries. The solidarity principle as stated by the German Constitutional Court is, arguably, extraterritorial and can be a helpful element to incorporate in the interpretation of uniform statutes around the world.

---

[3] Luciano Gallino develops this concept extensively in his book [6] and Stefano Rodotà also works with this idea in his book [7].

4. The Value of Privacy and Confidentiality

4.1. Privacy

In the era of information, privacy has become an increasingly important concern. Two key elements of privacy include dissemination and concealment. The Basic Law has determined privacy as valuable in and of itself and not as an intermediate good. However, Posner argues that the will of privacy is the will to manipulate other people's opinions about themselves by misrepresentation of the facts [13]. At some point, nondisclosure becomes fraud, and concealment may lead to faulty information. Viewing privacy from the angle of an economic analysis of the law, Posner further argues that people should not have the right to conceal material about themselves and that reticence to let other people access personal information comes from fear that others may gain some kind of benefit.

In a non-legal approach, IT leaders such as Scott McNealy (CEO and co-founder of Sun Microsystems, Inc.), Eric Schmidt (former CEO of Google), Mark Zuckerberg (co-founder of Facebook) have repeatedly stated that there is zero privacy in the technology age. Search engines retain all information, and privacy is an outdated concept and no longer a social norm [14]. Nevertheless, even detractors still highly value privacy in areas and circumstances where sensitive government-related issues appear. However, these arguments are in stark contrast to and incompatible with the rights to personality, privacy, and the protection of data as expressed by the German Basic Law. Nevertheless, a diversity of viewpoints helps to give the legal discussion a wider scope and perspective, and opens doors to further discussion and debate.

4.2. Confidentiality

The key notion to the principle of confidentiality is whether the person in question has a reasonable expectation of privacy regarding the disclosed facts, or, in other words, if the person who discloses the said information knows or ought to know that the other person can reasonably expect his or her privacy to be protected.

The intimate aspects of a person's sexuality, for example, are confidential matters, which no one has the right to disclose and, certainly, cannot force others to disclose. This occurred as an example in the case of Ms. Van Kueck *versus* Germany that was brought to the European Court of Human Rights[4] because German courts failed to acknowledge Ms. Van Kück's legitimate expectation of privacy. The European Court ruled in her favor.

The argument can be built that confidential information (all private data) must be treated confidentially, meaning it may be used to fight crime, to enforce the law, to plan health and security or to protect other socially valuable interests. In the Information Age, individuals are aware that communication and Internet data are used, tracked, shared, and stored. Such exceptions to the duty of confidentiality is the issue of "public interest". Should there be a public interest involved, confidentiality yields a social good. Confidentiality can also lose its protection when it has become generally accessible and therefore no longer regarded confidential, or, when the information is considered "trivial" even though it might be confidential, or when the disclosure is required by law, and if the claimant consented to its disclosure [15].

The issue of confidentiality among parties continues to be disputed among German legislators. For instance, if confidentiality is not expressively addressed during an arbitration process, the duty of confidentiality may be void [16]. However, it is widely accepted and part of standard procedure that all parties involved in arbitration proceedings are under an obligation to maintain confidentiality. In any case, confidentiality does not prevent complying with statutory duties of information, particularly those of regulatory, administrative and penal proceedings.

---

[4] ECHR: Van Kück v. Germany Publication: 2003-VII.

5. The Principle of Solidarity

The philosophical discussion in Germany has emphasized the importance of solidarity [17,18] in connection with every major social, legal, scientific and technological breaking point. It is particularly the case for health and biomedicine, as well as genetic engineering of humans [19], but also for information technology, digital universal inclusion [20] and, as argued here, privacy right and data protection.

Consensus on core values such as solidarity is therefore essential to the promotion of human dignity. Solidarity is one of the basic human experiences, since it is generally acknowledged that membership in a group affords greater protection. Children, the weak and ill, the poor and the elderly have always depended on solidarity and support from immediate or extended family, as well as from their neighbors [21]. Communities of solidarity have been the long-standing answer to communal dangers. However, this concept is not always clear and its role remains frequently quite obscure. Scholars throughout history have addressed it in different ways, but, if considered from a modern point of view, it is easy to see that fraternity can be interpreted as a synonym of solidarity and that this very solidarity is directly related to personal freedom and equality. A person is supportive of another as long as this other is considered worthy, equal and free. Solidarity therefore holds the same value and status as freedom and equality [22].

Solidarity is one of the founding values of the European Bill of Basic Rights, and is considered to be an essential ethical value because it is an expression of support, and enables assistance to and cooperation with worthy and respected peers. Solidarity is therefore a central value in Western civilization and springs from core civil structures, constitutions and bills of rights, the very foundation of peaceful human coexistence. The idea behind these claims is that solidarity may serve as a corrective to the currently prevalent emphasis placed on individual choice and autonomy in socio-political and legal trends, with the ensuing high cost to the wider social grouping.

Collaborative behavior and trust mechanics are not only moral and legal trends but also technological phenomena of the highest importance. The perception of solidarity with respect to the virtual world spontaneously moves individuals to *share*, *link*, *group*, *save*, *collaborate*, *torrent* and *join* in spaces and ways not previously anticipated. Every time someone engages in any of these actions, a collective process of communication is established. Every individual communication tends to be perceived to add a value to solidarity when virtually shared. Every action leaves a trail which cannot be deleted and may actually be followed to generate trends, consumption preferences and profiles accommodating a system's transparency. The information revolution is changing the world profoundly and irreversibly at a breathtaking pace and in an unprecedented scope [23].

6. The Principle of Proportionality

The concept of proportionality can be found among most European countries. However, it is most elaborate in Germany. Even though a definition of this principle is hard to come by, for the purpose of this paper we define this principle as a legal principle binding the executive, judicial and legislative powers of a country to the protection of the freedom of citizens of that country. Emiliou defines the principle of proportionality *stricto ensu* as a "Principle that requires a proper balance between the injury to the individual and the gain to the community caused by a state measure" [24]. Emiliou further states that this principle "prohibits measures whose disadvantage to the individual clearly outweighs the advantage to the community" [4].

Even though the principle of proportionality is not directly reflected in the German *Grundgesetz*, BVerfGE 19 S 342 states that "as an expression of the general right of the citizen towards the State that his freedom should be limited by the public authorities only to the extent indispensable for the protection of the public interest."

Proportionality was most fully developed within German law, in which it appeared initially to challenge policing measures that were excessive or unnecessary in relation to the objective being pursued [24]. Craig reviews proportionality as positive law on a normative foundation and discusses

both narrow and broad rationality approaches [24]. Nevertheless, proportionality is now established as a general principle of community law [24–27]. The principle of proportionality has therefore entered many aspects of our daily life, including biotech ethics, medical ethics and certainly information technology ethics and subsequently cybersecurity and cybercrime. The principle attempts to balance to which degree computer or internet users may be surveyed. The principle of proportionality encounters particular challenges as interpretations of the principle vary vastly within an international scope. One interesting observations] may be stated at this point with respect to the different interpretations of the surveillance imposed on major European Leaders by the United States government in 2015.

7. Decisions of the Bundesverfassungsgericht

The following section analyzes decisions made by the Bundesverfassungsgericht on issues related to privacy and data protection laws. The analysis undertaken here is meant to help understand the court's rationale regarding these topics, so as to establish an argumentative thread on the solidarity and proportionality principles as a reference for privacy and data protections laws.

We are looking at a total of five key court decisions regarding data protection in cases such as the "Automatic Plate Numbers Recognition"; "Precaution Storage of Data"; "Acoustic Surveillance of Housing Space"; "Admission of Personal Information in Criminal Proceedings Collected Unlawfully" and the "Protection of the North Rhine-Westphalia Constitution Act". All the above cases are leading decisions of the court regarding data protection.

7.1. Automatic Plate Numbers Recognition—1 BvR 2074/05; 1 BvR 1254/07

The First Senate of the Federal Constitutional Court upheld the complaints by several registered motor vehicle holders against provisions under police law in the states of Hesse and Schleswig-Holstein authorizing automatic recognition of vehicle number plates.

The court ruled such automated processes as in violation of information self-determination rights since the provisions lack the required definition and clarity, and fail to establish the cause and the purpose of such recognition. However, should the data collected be deleted right after they are matched, without further evaluation, the process would not necessarily violate constitutional standards. What is deemed a threat to the right of personality is the automatic collection and retention of such personal information for possible further use.

Nevertheless, data recognition by itself does not constitute a dangerous act. However, when number plates are kept and can become the basis for further measures, an interference with fundamental rights does exist. This ruling is therefore relevant to us because the Constitutional Court establishes the circumstances in which data collection is compatible with the Basic Law.

7.2. Precaution Storage—1BvR 256/08; 1BvR 263/08; 1BvR 586/08

A constitutional complaint challenged the provisions for data storage in the German Telecommunications Surveillance Act and required an amendment in December 2007 to implement a European Union directive on data retention specifically in German law. The challenged provision ordered that, in the case of individuals who in their business capacity provide telecommunication services or assist in providing such services, data should be stored by way of precaution. In addition, such information providers shall in the individual case supply, without delay, information to the competent agencies, upon their request, on the data collected pursuant to §§ 95 and 111. This precautionary data storage should be done if particular information were necessary (a) for the prosecution of criminal or regulatory offences; (b) to ward off dangers to public security; (c) to perform the statutory duties of Federal and state authorities concerning the protection of the constitution; and (d) for use by the Federal Intelligence Services and the Military Counterintelligence Service.

The constitutional complainants' argument that this provision violates articles 1.1 and 2.1 in conjunction with articles 1.1, 10.1 and 19.2 of the *Grundgesetz,* in particular since Art. 10.1 guarantees the secrecy of telecommunications, protects the incorporeal transmission of information to individual

recipients by means of telecommunication traffic against the observation by state authority and beyond state authorities' bearing. This protection not only relates to the contents of the communications undertaken, but also covers confidentiality of the immediate circumstances wherein the process of telecommunication is taking place, in particular whether, when and how often telecommunication traffic occurred or was attempted between specific persons or telecommunication equipment. The court considered that an encroachment upon fundamental rights includes every observation, recording and evaluation of communication data, and every analysis of their content or other use by state authorities.

Likewise, the Constitutional Court ruled such encroachments upon the secrecy of telecommunications to be substantively constitutional if their purpose is of public interest and if they comply with the principle of proportionality. Thus, as an exception to the rule, storage of telecommunications traffic data without cause for six months, for qualified uses in the course of prosecution, to insure the warding off of danger and for intelligence service duties is therefore not in itself incompatible with article 10 of the *Grundgesetz*.

The court also claimed legitimacy for the legislature to order such six-month storage as a way to create detection possibilities otherwise not possible. In other words: data storage is not by itself a threat to privacy. Arguably it is, for a limited period of time, a kind of common good, available to all. Nevertheless, in the above case, the court ruled that the challenged provisions did not meet the particular high standards of data security required by the proportionality principle.

7.3. Acoustic Surveillance of Housing Space—1 BvR 2378/98

On 3 March 2004, the Constitutional Court decided that some provisions included in the Code of Criminal Procedure concerning acoustic surveillance of dwellings partly violate the Basic Law. Article 13.3 of the Basic Law allows acoustic surveillance of dwellings for reasons of prosecution of severe crimes defined individually by law and other means if exploration of the facts using other means would be unproportionally difficult or futile.

The court determined confidentiality of communication as secure in private dwellings, therefore acoustic surveillance of housing space should not be allowed in this sphere of privacy. Even predominant public interests cannot justify such encroachment. However, not all acoustic supervision violates human dignity, as there are certain conversations which do not integrate such intimate space, *i.e.*, those concerning committed criminal offences. In this way, the court introduced a flexible method to distinguish between constitutional and unconstitutional acoustic surveillance of conversations in private rooms.

However, some provisions of the Code of Criminal Procedure were considered unconstitutional because they did not fulfill certain requirements, such as the need to hold a judicial order concerning the surveillance of dwellings, details of the duration of the surveillance, and the extent of the measures to be used for the surveillance.

7.4. Admission of Personal Information Collected Unlawfully in Criminal Proceedings and the Issue of Life Insurance Policies—2 BvR 2500/09, 2 BvR 1857/10

The complainants, convicted for being members of and supporting terrorist activities, applied for life insurance policies in 28 cases, nine of which were concluded. The complainants were apprehended before being able to further enact their planned offence. The conviction evidence was collected from preventive dwelling police monitoring carried out during several months in 2004, prior to starting the criminal investigation proceedings against the complainants suspected of planning terrorist attacks.

The required judicial order for preventive surveillance in cases of imminent risk of public security was carried out lawfully according to Rhineland-Palatinate Police and Regulatory Authorities Act (*Rheinland-Pfälzisches Polizei-und Ordnungsbehördengesetz*—POG RP).

The Federal Court of Justice (*Bundesgerichtshof*) confirmed the information obtained by preventive police monitoring of dwellings could be admitted, but amended the guilty verdict to distinguish

between "fraud", where life insurance policies had been issued *versus* "attempted fraud" where life insurances were not issued.

The Constitutional Court remitted the case, ruling that the guilty verdict for completed or attempted fraud violates the principle of determinedness set in Article 103.2 GG, which states an act can be punished only if the criminality was determined by law before the act is committed. However, it upheld the Federal Court's criteria by which the admission of information from the monitoring of dwellings does not violate the complainants' fundamental rights.

Regarding personal information obtained by monitoring dwellings, the court decided it did not violate the complainants' general right of personality. The legal foundation was to consider that admission of personal information handed down by a criminal court is constitutional. In particular, it is consistent with the proportionality principle when it serves purposes having constitutional status, such as the state obligation to guarantee the administration of criminal law. The admission of information is hence also proportional, in principle, if—as in the original proceedings—the information is originally collected for another purpose and further used in criminal proceedings.

7.5. Protection of the Constitution in the North Rhine-Westphalia Act—1 BvR 595/07

The Constitutional Court considered some aspects of this act (*Gesetz über den Verfassungsschutz* in *Nordrhein-Westfalen* as of 20 December 2006) to be null and void, particularly because various instances of data collection and handling by information technology systems were considered incompatible with Article 2.1 of the Basic Law in conjunction with Articles 1.1, 10.1 and 19.1 sentence 2 of the same law.

This provision allows the constitution protection authority to carry out two types of investigative measures: first, secret monitoring and other Internet reconnaissance (alternative 1), and second, secret access to information technology systems (alternative 2).

The state provision was the first explicit empowerment of a German authority to engage in "online searches".

The Constitutional Court determined that the general right of personality (Article 2.1 in conjunction with Article 1.1 of the Basic Law) includes the fundamental right to confidentiality and integrity of information technology systems:

> "Secret infiltration of an information technology system to monitor the use of that system and read its storage is constitutionally permissible only if factual indications of a concrete danger to a predominantly important legal interest exist. Predominantly important are a person's life, limb and freedom or the threat to certain public interests affecting the basis or continued existence of the State or of human existence" [28].

The court went on to state: "Secret infiltration of an information technology system is in principle to be placed under the reservation of a judicial order. The statute granting powers to perform such an encroachment must contain precautions in order to protect the core area of private life" [28].

Insofar as empowerment is restricted to a state measure by means of which the contents and circumstances of ongoing telecommunication are collected in the computer network, or the data related thereto is evaluated, the encroachment is to be measured against Article 10.1 of the Basic Law alone, namely, that the privacy of correspondence, posts and telecommunications shall be inviolable.

If the state obtains knowledge of communication contents publicly accessible on the Internet, or if it participates in publicly accessible communication processes, in principle there is no encroachment on fundamental rights.

8. Adapting to New Technological Circumstances and the Principle of Proportionality

Technology continues to provide ever-new ways of human interaction and has therefore required judges to have an open mind. Many existing legal categories have been considered inappropriate to provide protection of basic human rights. As a result, the German Constitutional Court developed

traditional civil-law categories, adapting them to the Basic Law and to new social needs and modern life. Thus, the German Constitutional Court has reshaped legal guarantees.

The German Constitutional Court has also addressed issues concerning gender, property, private and public life, technology-related challenges, and matters concerning the new role of state sovereignty. The court has furthermore heightened the concept of the free development of personality beyond cultural or social limitations, based on the concept of equality. This development sets the German Constitutional Court at the forefront of social events, as individual initiative in search of identity shapes the future path of society. In response to such demands, the court has established and defined new dimensions of property, privacy and the Internet. Arguably, it has evolved towards the idea of global public goods, limiting property and privacy when the proportionality principle calls for such limitations on the basis of social good. In so doing, the court has found a new balance between the rights of personality and a democratic society.

Likewise, the rulings of the Constitutional Court analyzed above show that, in giving proper protection to fundamental rights, the court is pragmatic and acknowledges the different scopes of state, legislature, lower courts, as well as international and supranational jurisdictions.

9. The Affirmative Role of the State and the Solidarity Principle

Another axiomatic principle the German Constitutional Court advances is the affirmative obligation of the state to further human dignity and to encourage solidarity among its citizens. In doing so, protection of freedom and security becomes one of its first duties. Respect for private and family life, marriage, home and communications, as well as protection of personal data is always present in the court's doctrine. Special consideration has been given to fair processing of such data and to the requirement of consent for its use.

The court has proven to be open to a complete redesign of legal structures if required by the demands of contemporary societal life. It is open to redefine what is public and what is private. The court furthermore has outlined the human condition as being in a reciprocal relationship with other individuals and with the state. The court rejects the idea that a human being is first alone and only enters into relations with others humans later. In fact, the doctrine for the German Constitutional Court has determined fundamental rights as part of the whole of the human condition in which solidarity is what unites the group according to the qualitative degrees of participation of its members in a society. Examples of the above are the court's rulings that privacy rights depend not on the condition of certain individuals alone, but rather on those authentic privacy expectations such persons might have.

The court rulings analyzed here deal with the notion that rights belong not to abstract individuals but rather to actual, everyday people. The court frequently uses the principle of proportionality to fine-tune and balance its decision, specifically, the court is attempting to reach a balance between fundamental rights of an individual and popular sovereignty. It is therefore possible to state that the court's reasoning changed regarding what counts as key elements of the legal system. There is a transition from the old supremacy of specific legislation to a system in which legal principles are of the most and highest importance; the proportionality principle being one frequently used by the Constitutional Court. Furthermore, the *Bundesversfassungsgericht* created specific rights such as the right to information self-determination, which is crucial to data protection, as well as corporal and psychological integrity, non-discrimination, and solidarity among all citizens, particularly the unemployed, children, the elderly and the physically and mentally challenged.

10. Conclusions

Nevertheless, the right to privacy does not come without limitations. The principle of solidarity, for instance, entails certain restrictions to privacy. Likewise, national security and certain requirements regarding democratic transparency call for and allow for some restrictions on privacy. For this reason, data storage for a certain amount of time can also be deemed legitimate and may be accepted by the court. In particular, regarding information technology, data and the Internet, the court now

allows access to this information regardless of ownership. Current technological circumstances have genuinely led the court to move from a discourse of exclusiveness to one of accessibility.

The ruling of the Constitutional Court regarding temporary data storage by Internet and communication providers may be interpreted as being open to the idea of online data as a common good. There is a point in which data does not belong to anyone; in a cloud with no center, everyone shares this property and, as such, the property becomes available to everyone, for different social needs. Protection of an individual's rights is not related to exclusiveness, but rather refers to the way a particular good is used. Thus, at least for six months in the German case, data is a collective good accessible to all those who have a legitimate interest. Common goods have a diffuse and non-concentrated ownership; belonging to all and to no one at the same time, they are accessible to all and no one can feign exclusiveness. The data must be managed, consequently, by the solidarity principle [6].

Knowledge has become a common good, just as technological innovation, cultural and artistic goods are common goods. The court has stated that the greater the information value of a fact for the general public, the more the right to protection has to yield. Conversely, where the interest in public information decreases, protection of the person concerned carries greater weight. It is relevant, states the court, to weigh the importance of an encroachment or trespass on privacy against the information value of an issue for the makeup of public opinion.

An individual's private life is inviolable and enjoys absolute protection. This has consistently been the stance on human dignity of the *Bundesverfassungsgericht*.[5] All possible interpretations of the court's reasoning (liberal, institutional, value-oriented, democratic and social) agree that human dignity is an absolute value. Thus, any instance marking a distinction between a life being not worthy or less worthy is void of legitimacy. Protection of human dignity and fundamental rights allows the legislature to impose restrictions on other rights or to assign solidarity duties to the community or individuals as long as certain constitutional provisions are taken care of. And for this intent, the principle of proportionality is of paramount importance.

Author Contributions: Klaus Schmidt and Alejandro Laje equally contributed to the first draft of this paper. Laje developed the detailed case analysis. Klaus Schmidt did all remaining revisions and edits.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Samuel Warren. "The Right to Privacy." *Harvard Law Review* 4 (1890): 193–220. [CrossRef]
2. David P. Currie. *The Constitution of the Federal Republic of Germany*. Chicago: The University of Chicago Press, 1990, pp. 194–95.
3. Russell A. Miller. "Balancing Security and Liberty in Germany." *Journal of National Security Law* 4 (2010): 369.
4. Luciano Floridi. *The Blackwell Guide to the Philosophy of Computing and Information*. Hoboken: Blackwell Publishing, 2003.
5. Klaus Mainzer. "Systems: An Introduction to Systems Science." In *Philosophy of Computing and Information*. Edited by Luciano E. Floridi. Hoboken: Blackwell Publishing, 2004, pp. 35–36.
6. Luciano Gallino. *Tecnologia e Democrazia. Conoscenze Tecniche e Scientifiche Come Beni Pubblici*. Turin: Einaudi, 2007.
7. Stefano Rodotà. *Il Diritto di Avere Dirito*. Roma-Bari: Laterza, 2012.
8. Jake Edge. "Living with the Surveillance State." *IWN.net*, 29 October 2013. Available online: https://lwn.net/Articles/571875/ (accessed on 9 June 2016).

[5] *See* BVerfGE 6, 32 (41); 6, 389 (433); 27, 344 (350–351); 32, 373 (378–379); 34, 238 (245); 35, 35 (39); 38, 312 (320); 54, 143 (146); 65, 1 (46); 80, 367 (373–374); 89, 69 (82–83); 109, 279 (313).

9. Siobhan Gorman, and Jennifer Valentino-DeVries. "New Details Show Broader NSA Survillance Reach: Programs Cover 75% of National Traffic. Can Snare Emails." *The Wall Street Journal*, 20 August 2013. Available online: http://www.wsj.com/articles/SB10001424127887324108204579022874091732470 (accessed on 21 August 2013).
10. BBC News. "Report: NSA Collected 200m Texts per Day." 18 January 2014. Available online: http://www.bbc.com/news/world-us-canada-25770313 (accessed on 14 June 2016).
11. Spiegel Online International. "'Prolific Partner': German Intelligence Used NSA Spy Program." 20 July 2013. Available online: http://www.spiegel.de/international/germany/german-intelligence-agencies-used-nsa-spying-program-a-912173.html (accessed on 21 July 2013).
12. Philip R. Reitinger. "Encrypton, Anonimity and Markets." In *Cybercrime, Law Enforcement, Security and Srsurveillance in the Information Age*. Edited by Douglas A. Thomas. New York: Routledge, 2000.
13. Richard Posner. *The Economics of Private Law*. Cheltenham: Edward Elgar, 2001.
14. Edwin L. Cieh. "Personal Data Protection and Privacy Law in Malaysia." In *Noriswadi Ismail, Beyond Data Protection*. Berlin: Springer, 2013.
15. Paul Stanley. *The Law of Confidentiality: A Restatement*. Oxford: Hart Publishing, 2008.
16. Kyriaky Noussia. *Confidentiality in International Commercial Arbitration*. Berlin: Springer, 2010.
17. Jürgen Habermas. *The Future of Human Nature*. Cambridge: Polity Press, 2003.
18. Marcos M. Córdoba. "Nueva regulación del derecho sucesorio argentine." Speech delivered at the Tempelhof Schöneberg City Hall, Berlin, Germany, 13 April 2013.
19. Darry Gunson. "Solidarity and the Universal Declaration on Bioethics and Human Rights." *The Journal of Medicine and Philosophy* 34 (2009): 241–60. [CrossRef] [PubMed]
20. Philip Leith. "Europe's Information Society Project and Digital Inclusion: Universal Service Obligations or Social Solidarity?" *International Journal of Law and Information Technology* 20 (2012): 102–23. [CrossRef]
21. Michael Stolleis. *History of Social Law in Germany*. Berlin: Springer, 2014.
22. Guido Alpa. *Congreso Internacional Buena Fe y Solidaridad Jurídica*. Buenos Aires: Universidad Abierta Interamericana, 2013.
23. Nicholas Emiliou. *The Principle of Proportionality in European Law: A Comparative Study*. London: Kluwer Law International, 1996.
24. Paul P. Craig. "Proportionality, Rationality and Review." Oxford Legal Studies Research Paper No. 5/2011, University of Oxford, Oxford, UK, February 2011. Available online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1756271 (accessed on 9 June 2016).
25. Gráinne de Búrca. "The Principle of Proportionality and Its Application in EC Law." *Yearbook of European Law* 13 (1993): 105–50. [CrossRef]
26. Aldo Sandulli. "Eccesso di potere e controllo di proporzionalità: Profili comparati." *Rivista Trimestrale di Diritto Pubblico* 2 (1995): 329–70.
27. George Gerapetritis. *The Application of Proportionality in Administrative Law: Judicial Review in France, Greece, England and in the European Community*. Oxford: University of Oxford, 1995.
28. GFCC, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—paras. 1–333.