Oct 28th, 9:00 AM - 10:30 AM

The impact of public interest in the information privacy: Analyze of the ECHR Decisions

Jorida Xhafaj
University for Business and Technology, jorida.xhafa@ubt-uni.net

Almarin Frakulli
Albanian University, marin_ruse@yahoo.it

The impact of public interest in the information privacy: Analyze of the ECtHR Decisions

Jorida Xhafaj[1], Almarin Frakulli[2]

[1]UBT – Higher Education Institution, LagjjaKalabria, 10000 p.n., Prishtine, Kosovo
[2]Albanian University, Bul. Zogu I, Tirana, Albania
jorida.xhafaj@ubt-uni.net, marin_ruse@yahoo.it

Abstract. The main object of this paper is the tender balance that exists and arises even more between the use of personal information that people provide in the course of most public security actions and privacy.
The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, and how law allocates power over information in different countries, will give us the possibility to define how much privacy are we willing to give up in exchange for greater public safety and other public interest, how ECtHR has decided this tender dilemma – the criteria's and principles applied in these cases.
The methodology used in his paper is based on the method of description, the method of conceptual analysis and the method of evaluation.

Keywords: Personal information, public security, impact and barriers, ECtHR.

Introduction

The protection of personal data is one of the basic subjective personal rights, which is construed with particular reference to the right to respect for private life on the one hand and other important personal rights and/or public interests on the other. Data protection right ensures a person the right of disposal over all data in connection with his personality. From the beginning of its legal definition as a personal right[47], it has become issues of many studies with the scope to analyse the tender balance between the rightof privacy and other basic values for a person as the freedom of expression, confidentiality, the public interest, national and public security, information security, or criminal disclosures, etc
The fundamental right to personal data protection is guaranteed in most of the countries from national legal framework and the international one. Based on the Articles 8 and 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[48], special laws on the

[47]On 1970 The German State of Hesse introduces the first modern privacy law and on 1973 Sweden creates the Data Act, the first national privacy law.

[48]Rome, 4 November 1950, European Treaty Series (ETS) No. 5. Hereafter also referred to as "ECTHR", "the Human Rights Convention" or (when there is no risk

protection of personal data[49], it is guaranteed the protection and legitimate use of personal data, and their treatment by public authorities. In most countries, the right to the protection of personal data and information is part of the constitution, the provisions of which, as a minimum, provide for the right to home protection and the protection of correspondence.
In terms of these instruments, data protection therefore operates between the right to respect for private life (privacy) and the possibility to suppress the extent of privacy or itsprevalence.
In the context of the technology development, the possibility of collecting, storing and conciliation of large pools of data mightresult in the infringement to the right of privacy. The underlying notion behind the aims of the data protection regulatory framework is the insufficiency of secrecy protection: within the new context protection should apply to all data: "data protection should be differentiated from the interpretation of privacy as intimacy."[50]. The concept of private life is a broad concept that does not need a complete definition, since none of them would be inclusive[51].
Meanwhile,corresponding to the idea of general personality right, the EU legislation the privacy can be interpreted and regarded:
as a claim, entitlement or right of an individual to determine what information about himself (or herself) may be communicated to others;
as the measure of control an individual has over information about himself,
as intimacies of personal identity, or who has sensory access to him;
as a state or condition of limited access to a person, information about him, intimacies of personal identity.
The aim of data protection law is the protection of privacy. The protection of personal data within the new circumstances can offer the protection of privacy. These statements are true;However, they say little about what privacy is and why it needs protection.
The impact of public security in the information privacy will be analyzed in the context of the goal and the interest protected under data-processing regulations on one hand and the interest protected in case of disclosure of personal information or violation of secrecy of privacy.

Models of data protection

As was mentioned before, the right to pretend protection of privacy has been regulated from more concerete provisions and requirementsl, in case of exceed of restrictions.
Different governments respond in different ways to these requirements, and according to the existing systems of safeguards for personal data protection and their application, have defined the global trend on privacy protection. According to Banisar and Davies[52]in their international survey of privacy, data protection, and surveillance laws and developments, can be defined four different

---

of confusion, in particular with the Data Protection Convention) as just "the Convention".

[49]https://www.dlapiperdataprotection.com

[50] Intimacy generally refers to the feeling of being in a close personal association and belonging together.

[51]Van Kück kundër Gjermanisw, 12 qershor 2003, seksioni i tretë, nr 35968/97, Strasbourg.

[52] David Banisar& Simon Davies, Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments, 18 J. Marshall J. Computer & Info. L. 1 (1999)

models for personal data protection, which are indicated from the necesity to enforce the surveillance or the monitoring of special operations through technology system.
The models are classified throught the main mechanism or the distingueshed element of the protection system (legislation, internal rules or technique equipments). So, can be distinguished the model of *comprehensive legislation, sectoral legislation, self-regulation and technology protections*. Depending on their application, these models could have impact by ensuring the complemented components among models or by containing opposed elements. In those countries that best guarantee the right to data protection, all these models work together and complement each other[53].
Comprehensive legislation consists of a model that builds on common laws that regulate the collection, use and dissemination of personal data by both public law institutes and private companies. Today around the world, over 100 countries[54]and independent jurisdictions and territories around the world have now adopted data protection laws that guarantee the right to protection of personal data by adopting special legislation and adopting the principles of correctness of personal data.
In Europe, an important point for countries with such a model of protection the unification act or rules and standarts.[55] The Data Protection Directive 95/46 created an obligation for Member States to ensure an common level of protection of personal data when transferred or processed in non-EU countries, seting a point of reference for national law and enforcmet of data protection through the harmonization nor only to the provisions, but also to the way they have to be interpreted. Also, during 1980, the Organisation for Economic Cooperation and Development (OECD) developed its privacy guidelines that included 'privacy principles', and shortly thereafter the Council of Europe's convention came into force.
Under this approach, data protection rules are developed and enforced by the private sector, and a special agency or commission monitors their implementation.
This is the preferred model for most countries to ensure an effective data protection mode. In most of these countries, there is also an official or commission that analyzes and carries out comprehensive control over compliance with data protection laws. The Republic of Kosovo, and other countries in the region are among the countries with comprehensive legislation.
In some countries, with the aim to provide more detailed protections and based on specific aspects of certain categories of information or sectors, they have avoided the general privacy protection rules set out in the first model, favoring the proper sectoral legislations. This model is base on the provisions for the protection of personal data according to the areas in which the latter are taken and existed as answer of the necessary measures and risques. They cover areas of particular complexity, such as financial protection of personal data, telecommunications, medical or health information, intelligence services, e-commerce, etc. The dynamics of the development of the different sectors are turning into a huge drawback for this model, which is why it is in constant change.
Another model for protecting the right to privacy is through self-regulation by companies and in various spheres of economic and social activity, different organizations set limitations on their specifications and most possible violation. Specifc sectors of an industry or company's bodies are

---

[53] *Idem*

[54] Banisar, David, National Comprehensive Data Protection/Privacy Laws and Bills 2016, November 2016

[55] Council Directive 95/46/EC, 1995, The directive, issued by the European Parliament and by the Council on 24 Oct. 1995, addresses the protection of individuals with regard to the processing of personal data and on the free movement of such data.

best aware of exactly what personal information they collect and how they use it. In order for data protection to be effective in one system, companies have the predisposition to cooperate because there are financial and political constraints on governments and other supervisors to impose coercive cooperation. For this reason, this approach has some positive aspects, but in general, protection is becoming a victim of the desire to maximize profits.

The development of information technology is making the processing and exchange of personal data considerably easier and partially passed into the hands of the individual consumers themselves. These new challenges are related to the fourth model –technology personal data protection.Through the use of a range of technical tools,every useres can provide different levels of communication and privacy protection. Such systems can be used to limit the transmission of personal data by giving the user access to his or her data and providing communications surveillance. These include encryption, proxy servers, forwarding of messages, e-money and smart cards[56].

The most applied model is the first one, which garanties in fact from legislation and the set of requirements designed from the state policy to ensure that the state's duty to protect personal information collected or stored in the course of its activities is respected by ensuring high standards. The set of requirements in most of the legislation are defined in two directions.

The first one is the list of principles relating to data quality and criterias, for making data processing legitimate. It can be easilty distinguished that this list of principles and criterias give substance to and amplify those contained in the Council of Europe Directive 95/46 EC on the protection of individuals with regard to the processing of personal data and on the free movement of such personal data must be:

processed fairly and lawfully;

collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

It can be clearly identified the fact that the principles of protection reflect the different perspectives, from which can be realized the control of data and their protection. On the one hand, they are embody in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the subject of data, who have the right to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances.

Furthermore, Article 7 of the Directive 95/46 define precisesly conditions for legitimated processing of personal data covering :

the unambiguously consent of the data subject;

the necessity of entering into a contract relation, to which the data subject is party or in order to take steps at the request of the data subject prior to;

the necessity for the compliance with a legal obligation to which the controller is subject; or

[56]Privacy in the Modern Age: The Search for Solutions, edited by Marc Rotenberg, Julia Horwitz, Jeramie Scott, April 2015

the necessity to protect the vital interests of the data subject; or the necessity for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or the necessity of accomplishment of the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests require protection of at the same level.

Despite their legal framework clarity related to information privacy, the confrontation of information privacy with other fundamental rights or interests puts law enforcers before a very tender dilemma. This dilemma can be resolved on criteria, determined as "the most important interest" or "the right, which prevails"[57]. Concretely, the right to privacy as a private interest is juxtaposed with the groupof those interests, which are related to the national security, public security and prosecuting of criminal offences, putted under the umbrella of public interest[58]. Can be noted that the balance, usually, has dominated by the public interest, which relies on the public welfare and the proper administration of justice.

Facing these important guaranteed constitutional values59 is of interest because of interference or mutual intervention in a number of practical cases.Therefore, it has to be emphasize the standards, which have to be considered case by case60 in the practice and to establish with of the before mentioned interest will have priority over the other. To establish this report or to resolve the issue of legitimacy or of not interference, first of all, should be refer to the constitutional principle of proportionality, which is particularly effective in the area of human rights. This means that any intervention on behalf of the public interest is necessary, appropriate, proportionate and effective.

Therefore, the respect of information privacy requires in principle non-intervention or restriction access on the information about the way a person organize his life.We consider that, the margin of assessment for personal data, in the case of the existence of a relationship between the right to access to personal data and the public interest has to be strongly based on the necessity of disclosure, which sufficient,in measures and categories of personal data, to guaranty effective use of them

---

57 Decision no.16/ 11.11.2004 of Constitutional Court of Albania

58 In accordance with different definitions or sources on "Public interest" we find the appropriate definition of the *General Statement of Principles* from the Australian Press Council, which defines public interest as "*involving a matter capable of affecting the people at large so they might be legitimately interested in, or concerned about, what is going on, or what may happen to them or to others", available at https://www.alrc.gov.au/publications/8-balancing-privacy-other-interests/meaning-public-interest#_ftn25*

59Referringespecially to the European Convention of Human Rights and other international acts.

60The margin of this assessment, and consequently the ratio between the hedged interest and the one affected, varies in each case. It depends on a number of circumstances and conditions that vary from one country to another, from one period of time to another, from the range of rights that are imposed on the balance and the consequences that would have the advantage of each of them.

Analyze of the ECTHR Decisions

The tendency to take measures towards the fight against organized crime and the prevention of other criminal offenses, preventing cases of abuse of state power or national interests has often created a relationship between public and private interest.

The allegation of respect for the information privacy has been constantly expanding not only through the European Court of Human Rights's jurisprudence, but also from the differing legal and jurisprudential developments of the states parties to the ECTHR. However, in general, it is acknowledged that the right to respect for privacy in general lies in essence of the data protection[61], and it provides the individual with a space within which he could independently develop and complement his personality, or maintain his relationships with the others[62].

Through ECTHR judgments we have analyzed in what cases the public interest has justified the use of personal data and under which criteria the court has decided neither proportionate with this right.

Accordingly, to the arguments Court in the case Uzun v. Germany[63] the processing and use of the data obtained through authorized surveillance on one had interfered with the applicant's right to respect for his private life. The Court considered that "…adequate and effective safeguards against abuse had been in place. The measures had pursued the legitimate aims of protecting national security, public safety and the rights of the victims, and of preventing crime". It is also emphasized that the used methods of investigation had been carried out for a relatively short period…. given that the investigation had concerned very serious crimes, the applicant's surveillance by GPS had thus been necessary in a democratic society".So, can be noted that the criteria used by the Court are focused on the legitimate aims of protecting national security, public safety and the rights of the victims, and of preventing crime, which had also been proportionate.

Another discussed case judged by the ECtHR has been the restricting of the cross-border movement in the context of the implementation by the state of counter-terrorism resolutions[64].

---

61 Van Kück v. Germany, no. 35968/97, ECtHR (Fourth Section), Decision of 18.10.2001

62 Scherpe, Jens M., Family and Private Life, Ambits and Pieces - M. v. Secretary of State for Work and Pensions, 2011. Child and Family Law Quarterly, Vol. 19, No. 3, pp. 390-403, 2007

63 In October 1995 the applicant and another man (S.) were suspected of involvement in bomb attacks by a left-wing extremist movement, complained in particular that his surveillance via GPS and the use of the data obtained thereby in the criminal proceedings against him had violated his right to respect for private life (*private life includes the privacy of communications, which covers the security and privacy of mail, telephone, e-mail and other forms of communication; and informational privacy, including online information -Copland v. the United Kingdom, no. 62617/00, ECTHR 2007-I).* Realizing that they were under surveillance, the two men sought to escape detection by destroying transmitters that had been installed in S.'s car and by avoiding use of the telephone. To counteract this, in December 1995 the Federal Public Prosecutor General authorized their surveillance by a Global-Positioning System device (GPS) which the authorities arranged to be fitted in S.'s car. The applicant and S. were arrested in February 1996 and subsequently found guilty of various bomb attacks between January and December 1995 on the basis of the evidence obtained through their surveillance, including GPS evidence linking the location of S.'s car to the scene of one of the attacks.

64 Nada v. Switzerland, judgment of 12 September 2012 (application no. 10593/08), according to which implementation by Switzerland of United Nations counterterrorism resolutions introducing a travel ban for all individuals, groups, undertakings and associated entities on the sanctions list. The applicant was revoked the permit to cross the border of the country. When he visited London in

The Court observed that Switzerland could not simply rely on the binding nature of the Security Council resolutions, but should have taken all possible measures, within the latitude available to it, to adapt the sanctions regime to the applicant's individual situation. As Switzerland had failed to harmonize the international obligations that appeared contradictory, the Court found that there had been a violation of Article 8.

As to the necessity of the measures, the Court was prepared to take account of the fact that the threat of terrorism was particularly serious at the time of the adoption of the resolutions imposing the sanctions. However, according the decision "*the maintaining or reinforcement of those measures had to be justified convincingly*".So, by this case can be interpreted that the principle of proportionality…." *should have taken all possible measures, within the latitude available to it, to adapt the sanctions regime to the concrete situations".* It is necessary to be taken into account the realities of the case, especially the duration of the measures imposed has to be implemented in its legal order.

Results

Referring to the constitutional principles in most of the countries and the European directives, it is necessary that any intervention on behalf of the public interest has to be necessary, appropriate, proportionate and effective.

For the ECtHR, the point at issues is the use of personal data and restriction of privacy has to be in accordance with the law.The Court consider that the measures has to pursued an adequate and effective safeguard, which correspond to legitimate aims of protecting national security, public safety and the rights of the victims, and of preventing crime. For more security, it can be cause lessprivacy, which on the other hand means stronger security and more state control and visibility.

Necessity of specified priorities criteria in case of balance between privacy and other legitimate interest or fundamental subjective rights, based on the nature and their status. Also, it is necessary to be taken into account the realities of the case, especially the duration of the measures imposed has to be implemented in its legal order.

Effectively combining the sectorial and self ─regulation model, for each branch of institutions, which collect and process personal information; More special legal instruments on data protection in police and law-enforcement cross- border cooperation to improve self - protection model of data protection information, especially for the purpose of preventing and combating crime in three actually fields: terrorism, cross- border crime and illegal migration.And also, for different types of data subjects, such as suspects, convicted persons, victims and witnesses; and data considered to be hard facts and those based on suspicions or speculation.

November 2002, the applicant was arrested and deported back to Italy, his money also being seized. In October 2003 the Canton of Ticino revoked the applicant's special border- crossing permit. Relying on Article 8 (right to respect for private and family life), the applicant argued that the ban imposed on him, preventing him from entering or transiting through Switzerland, had breached his right to respect for his private, professional and family life. As a result of the ban, he had been unable to see his doctors in Italy or in Switzerland or visit family and friends. The addition of his name to the list annexed to 3 the Taliban Ordinance had damaged his honor and reputation. The aim of the restrictions was to prevent crime and, as the relevant Security Council resolutions had been adopted to combat international terrorism under Chapter VII of the United Nations Charter, they could also contribute to Switzerland's national security and public safety.

References

1. David Banisar& Simon Davies, Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments, 18 J. Marshall J. Computer & Info. L. 1 (1999)
2. Banisar, David, National Comprehensive Data Protection/Privacy Laws and Bills 2016, November 2016
3. Etzioni, A.) The Limits of Privacy. New York: Basic Books,1999
4. Feldman, DSecrecy, Dignity or Autonomy? Views of Privacy as a Civil Liberty, 1994
5. Privacy in the Modern Age: The Search for Solutions, edited by Marc Rotenberg, Julia Horwitz, Jeramie Scott, April 2015
6. Scherpe, Jens M., Family and Private Life, Ambits and Pieces - M. v. Secretary of State for Work and Pensions, 2011. Child and Family Law Quarterly, Vol. 19, No. 3, pp. 390-403, 2007
7. Nada v. Switzerland, judgment of 12 September 2012 (application no. 10593/08), Van Kück v. Germany, no. 35968/97, ECtHR (Fourth Section), Decision of 18.10.2001
8. Decision no.16/ 11.11.2004 of Constitutional Court of Albania