Beyond Regulation: Alternative Ways to Guarantee of Privacy and Data Protection.

Margareth H. S. Kang

Master on Human Rights at University of São Paulo
Project Leader at Privacidade Brazil

Abstract

This article seeks to address the relationship between the personal data and the construction of a person´s identity. Thus, the theme runs through the regulation of personal data protection, and then reflects on emerging topics of the use of personal data by public and private sector. Finally, it reflects other means for a protection of personal data not by the law, thus contributing to the free construction of the person's identity.

Key words: Privacy, Data Protection, Human Rights, Law, Democracy

1. Introduction

After the end of the two world wars and the dismantling of the Soviet Union the borders that had been for several times limited, organized and re-organized seemed to find an arrangement, and the international political organization indicated a certain stabilization. Thus, especially after the 1940s it is possible to note the emergence and development of regional blocs and the increasing number of bilateral and multilateral agreements between countries.

Allied to these phenomena, the advancement of technology, the expansion and diversification of transport and mostly communication allowed the increasing mobility of people, goods and information in the modern society. Given this scenario of sharp transitions, society and its concepts were also and have been continuously and directly affected. A clear example regards the formation of identity.

The formation of identity can be seen from different perspectives, but we know that it is a construction. Among the many aspects that influence the construction of one's identity it is possible to mention, cultural references, religion, physical and racial characteristics, personal experiences, but mainly the set of information that the individual has access during his life, which ends up influencing all other references.

In the identity construction, the information about the person as well as the information available to the person are two aspects of utmost relevance. In ancient times the access and exchange of information were limited, often transmitted orally from generation to generation. Then, with the popularization of writing, books, newspapers and magazines had become an important tool of influence. But even with the popularization of printed materials, the full access of it was a class privilege that in addition to master the writing skill had also the status that enabled them to access the information.

Technological developments, the mass media such as the radio and the television disseminate the transmission of information. However, it was the Internet that brought the most impactful transformations, among the reasons for this phenomenon, we mention: the data storage capacity, the multiplication of "informers", the confusion between information generator and the information revceiver, and possibility of individualization of information for everyone.

In this sense, Spiros Simitis teaches us that modern forms of data collection have changed the discussion of privacy on three main points. First, questions about privacy express conflicts affecting everyone, and leaving therefore the merely individual sphere to the search for collective protection. Second, the monitoring has lost its exceptional character to become a routine. Third, the personal information is being used to enhance the standards of behavior, that is, the data processing is being developed as a strategy for handling of individual conduct. (SIMITIS, 1987. Pg 709-710)

We begin this article highlighting the regulation of personal data protection, we will go foward analyzing and exemplifying the issue of individualization of information and data, and how it can impact the formation of the identity of the individual as well as the consequences for society as a whole.

2. Privacy and Data Protection Regulation

The concept of privacy has not unisonous definition by the international community which ends up reflecting on the protection of personal data and its understanding, one of the reasons why although it is a global issue, there is a range of differences beyond the countries.

However, there is an international community consensus that the right to privacy and the protection of personal data protection must be guaranteed and respected, since it directly influences the exercise of other human rights. Privacy and personal data protection should be understood within a set of human rights that are interrelated with other rights like freedom of expression and transparency, for example.

Historically, the collection and management of personal data is not unique to the online world. For this reason, even before the emergence of the Internet, the importance of personal data was noted by the public and private sector which led to creation of the first personal data protection laws. However, it was the Internet that broaden the capacity of the collection, treatment and especially the individualization of the activities that previously had a limitation in face of the collective. In this sense, the use of Big data and algorithms have been increasingly seen not only in the private sector, but also in the public sector.

In Europe, the first generation of specific data protection laws was inaugurated by the German state of Hesse on September 30, 1970. In the same period it also began to emerge in the United States of America, the first laws regarding personal data protection. However, the United States had a different development of the rules comparing to Europe, as they preferred self-regulation. The majority of countries today, are highly influenced by EU model.

As observed by Viktor Mayer-Schönberger[1], personal data protection standards in Europe can be divided into four generations : (a) the first generation, characterized by rules that sought to regulate data processing technical aspects; (b) the second generation, characterized by rules that aimed to protect the individual's privacy rights by placing the person in the center, we highlight the emergence of consent; (c) the third generation marked by the possibility of the individual to determine not only if she/he wants, but how she/he wants to participate in the society, we highlight the publication of the concept of " Information Self-Determination "; and (d) the fourth generation, which brings greater empowerment to informational self-determination and non-negotiable mandatory individual legal protection and a preoccupation with the theme of the cross-border data flow.

Helen Nissenbaum[2] brings an alternative to the traditional understanding of the need for standards on this topic. In explaining her theory of "contextual integrity", she emphasizes that new technologies enable greater interaction with each other and also an overexposure of the individual, therefore, increasing the secret would then be a seductive answer, however imperfect, since the exchange of information is part the social being. So the hassle of the individual would not be with the exchange of information itself, but with the inappropriate exchange of information. The pursuit of "appropriate" exchange of information would not be in the division between public and private information and also not just by consent of the subject. The border between appropriate and inappropriate would be drawn from the context and the integrity of the flow of information. Having as parameter the actors involved, the type of information and the principles of transmission, then it would be asked for which interests serve the flow of information. In this sense, Nissenbaum explains that the proper flow of information must serve the social integrity and adds that respecting privacy is to respect the individual but also the role of information flow. So privacy would not be against the flow of information, but against the inappropriate flow of it. According to this theory, the development of the standard for an appropriate exchange of information should then basically observe its context and the integrity of that flow, remembering that the informational rules goes beyond the individual person , playing an important role in social institutions.

> "In the international scenario, this issue has generated guidelines, agreements and principles. We note that, in the 80s, we have the beginning of the regional regulation attempt, especially regarding the transfer of personal data between borders, starting with the OECD, Council of Europe and later the European Union. But only from the new millennium, since 2000, we noted the participation of other regions and blocks, such as APEC, and a greater integration between the regions, a result of the popularization of the Internet in developing countries. In the last five years we have seen that other blocks, such as the Organization of American States and the European Union, edited their first documents on the protection of personal data. Meanwhile, the EU and APEC are upgrading their instruments. Internationally, more countries enacted laws on the subject.
> We believe that this movement of countries and blocks around minimum standards of data protection reflects the very nature of the Internet. Therefore, we corroborate with the understanding of several authors, that minimum standards should be adopted throughout the world, since the person must be protected regardless of where it is found. "(KANG , 2016. Pg.156) [3]

However it should be stressed that about 40% of the countries do not yet have personal data protection law, not mentioning those who although have one, it doesn't protect effectively the citizen or sometimes legitimizes behaviors that contrapose data protection policies focused on the protection of person's rights.

For this reason, there is a long way to go in terms of personal data protection regulation. Regardless of the differences beyond the countries, protection of personal data is fundamental, and we agree with those that teaches us that for a proper analyses of matter we must consider some assumptions: a) public and private information classification has to be removed, b) its particular characteristics show the need of proper attention, c) the regulation of data protection should be used for the protection of the individual without forgetting the important role that information flows plays in the society, d) data protection regulation should seek to balance the asymmetry of power related to the control of information, e) data protection is closely associated with the free development of the personality and the construction of the person's identity. (KANG, 2016)

3. Identity and the Digital Era

Before entering in this topic we need to understand what is identity and its relation to personal data. Therefore we would like to bring here two definitions:

> The concept of identity is only vaguely clear to most people. It relates not only to names, which are easy to remember for human beings, but goes far beyond identifiers, which typically link an identity to a certain context and which usually are unique in that context. As an initial approach, the notion of identity is described as follows: *Identity is a set of attribute values related to one and the same data subject*.
> (…)Nevertheless, we allude here to attribute values being determined either by the identity holder himself or by others.

> Considering time aspects, we have to extend the above introduced definition. Accordingly, attribute values used to specify an identity may change over time. Since all values an identity-related attribute can take are essential to describe the identity of its data subject, it is necessary to add a timestamp to each attribute value for which that attribute value is valid. And, following this train of thought, we can further state: *An identity as a set of attribute values valid at a particular time can stay the same or grow, but never shrink.*[4]

For Manuel Castells[5],

> By identity, as it refers to social actors, I understand the process of construction of meaning on the basis of a cultural attribute, or a related set of cultural attributes, that is given priority over other sources of meaning. For a given individual, or for a collective actor, there may be a plurality of identities. Yet, such a plurality is a source of stress and contradiction in both self-representation and social action. This is because identity must be distinguished from what, traditionally, sociologists have called roles, and role-sets. Roles (for example, to be a worker, a mother, a neighbor, a socialist militant, a union member, a basketball player, a churchgoer, and a smoker, at the same time) are defined by norms structured by the institutions and organizations of society. Identities are sources of meaning for the actors themselves, and by themselves, constructed through a process of individuation."

Forward, in this same work, Castells observes that social construction of identity always takes place in a context marked by power relations. Thus, he separates three different origins in the construction of identity: a) Identity legitimizing, imposed by dominant Institutions of the society; b) Identity Resistance, generated to resist or oppose the logic of domination c) Project Identity, Which is built by social actors to redefine their position in the society seeking transformation in the social structure. (Castells, 2010, p. 6-8)

There are several definitions to the concept of identity, but mostly there is no disagreement that identity is constructed, formed by several elements that can be assigned by the individual or by others (society, state, etc). In this sense, today in the formation of our identity we have the interference of the public and private sector, which ultimately play an important role in shaping the identity of the individual but also in the transformation of the society.

3.1.The Identity Construction by the Private Sector

In the private sector, it seems that we are habituated to regard the data management made by them in a natural way, even if it is not. Nowadays personal data is commercialized and processed in many different ways and for several purposes. We have observed the monetization of data protection in the private sector.

The profile of who we are and our preference is openly being built by companies like Google (my account) and Facebook (Activity Log and News Feed Preferences). But, this profile construction is not as visible in many of the sites we navigate or by the services contracted in the Internet. In addition, the data collected by these companies could end up being accessed by the public sector. Depending on the country and the region, access to personal data can be obtained by court order or more directly with a simple request of the police authority or any other public authority.

However, it becomes more clear that regulation is not the only tool for the protection of privacy and data protection, the main reason is because the interest of the society about their data management is growing.

After the revelations of Edward Snowden, USA companies in technology and communication began to have revenue losses. Users from various fields related to communication started to look for companies not based in the United States territory as an alternative to the NSA surveillance. These losses were due to the lack of user's confidence, who preferred to seek their services in other countries capable of granting more protection of their data. [1](KANG, 2016)

[1] See: MILLER. Clair Cain. *Revelations of NSA spying cost US tech companies*. The New York Times. March 21, 2014. Available at: < http://www.nytimes.com/2014/03/22/business/fallout-from-snowdenhurting-bottom-line-of-tech-companies.html >. Accessed in: 04. Jul. 2015. GRIFFITHS, James. *Two years after Snowden , NSA revelatios still hurting US tech firms in China*: report. South China Morning Post. 03 July, 2015. Available at: < http://www.scmp.com/tech/enterprises/article/1831657/nsa-spy-revelations-damaging-us-tech-firmscompetitiveness-

Several factors can be assigned to this scenario: increasing public awareness of the importance of personal data, the rise of online incidents that endangers privacy, the insecurity felt by people regarding to tracking technologies and surveillance. In this scenario, the person felt insecure, and the market saw an opportunity, using privacy as product of competition. In this regard privacy-enhancing technologies (PETs), and transparency-enhancing technologies (TETs) as well as policy related to it are getting popular. The continuing growth of the Internet of Things will require more work from the private sector to enable innovation and its use without harming human rights such as right to privacy.

In the private sector therefore it is possible to observe that human rights like privacy and data protection are gaining monetary value. So even users from countries like USA that has several surveillance policies are opting for services elsewhere, which obliges the big service providers to take more measures in order to enhance data protection and transparency, like the recent WhatsApp encryption policy. Added to it, the companies are fighting for legislations that don't force them to give personal information to the government so easily. Through these choices, users, some consciously, but others unconsciously, are determining what type of policy and what kind of business will prevail, this consequently influences the forming of profiles and the over collection and processing of data by the private sector, and in the end of the road it will impact on the person's identity construction by companies.

3.2 The Identity Construction by the Public Sector

In the public sector, Governments are increasingly using personal data to tackle several issues, from national security issues like terrorism defense and cybercrime to public policy development such as unified identity management. However many of this movements have been done without taking the proper care and analyses of possible impacts of technology on social exclusion, increased social stratification, and on the democracy, for example.

In this section we analyze the two most recent ways of use of personal data by the public sector which the potential of consequences to the person´s identity construction has not been measured yet, namely the use of algorithms in public policies and the renewal of traditional identification documents.

A. Algorithms in the Public Sector

The use of algorithms by the public sector is not novelty, several States are making use of this tool primarily for issues related to combating violence and security. While in some countries, such as Brazil, this tool is in the early stages and it is still not clear how to use it, in the United States for example, police[2] in Chicago and other cities have increasingly made use of algorithms to predict possible criminals or most likely places for a crime, therefore acting preventively, this is known technique the *predictive policing*[6].

> "The strategy, known as predictive policing, combines elements of traditional policing, like increased attention to crime "hot spots" and close monitoring of recent paroles. But it often also uses other data, including information about friendships, social media activity and drug use, to identify "hot people" and aid the authorities in forecasting crime. (…)
> The use of computer models by local law enforcement agencies to forecast crime is part of a larger trend by governments and corporations that are increasingly turning to predictive analytics and data mining in looking at behaviors. Typically financed by the federal government, the strategy is being used by dozens of police departments - including Los Angeles, Miami and Nashville – and district attorneys' offices in Manhattan and Philadelphia."

[2] "Many government agencies and private entities are using data to try to predict outcomes, and local law enforcement organizations are increasingly testing such algorithms to fight crime. The computer model in Chicago, though, is uniquely framed around this city´s particular problems: a large number of splintered gangs; and ever younger set of gang members, according to the police; and a rash of gun violence that is connected to acts of retaliation between gangs." DAVEY, Monica. *Chicago Police Try to Predict Who May Shoot or be Shot.*The New York Times. May 23, 2016. Available at: < http://www.nytimes.com/2016/05/24/us/armed-with-data-chicago-police-try-to-predict-who-may-shoot-or-be-shot.html?_r=0 >.

Despite looking like a modern and reliable tool that can bring more efficiency to state activity, too much confidence in the use of algorithms is also criticized, "(...) activists and advocates of civil liberties are not convinced. Karen Sheley, the director of the Police Practices Project of the American Civil Liberties Union of Illinois, has pointed out that these innocent people are being flagged based on criteria that haven't even been publicly established."[7]

These criticisms are partly because algorithm uses (in the modern form) is still recent, with little evidence of its effectiveness but mainly due to its potential for bias analyzes and portray the problems which we live today, such as prejudice based on race, culture or social class for example. We emphasize that despite the algorithms, being operated on computers, they are created, analyzed and managed by people[3].

Spiros Simitis pointed out that there are some general consequences of the automated processing of data, not related to a specific country. In the public sector, data crossing can help the formation of "suspicious people", and concomitantly the reversal of the burden of proof, making the burden of proof fall on the individual, which would have the obligation to explain and justify about her/his behavior: "The accusation becomes much closer to a conviction. " The second consequence is the loss of context, since the data is disconnected from the original situation and transformed into items. As a result of this de-contextualization, intensified by the routine processing of the data, there is an increased risk of misinterpretations and false conclusions. The third consequence would be the categorization, especially when the processing is aimed at a particular topic. The individual becomes labeled and forcibly placed in a group[8].

B. Registration Document and Identity

When we think of state identification the first image that comes to our mind are the identification documents. The public sector identifies their citizens by numbers (registration numbers). In this sense, the document that among other information contains the unique number given to the individual serves to identify her/him beyond the society. The individualization of the subject by the State is not new, but it was through the organization of States in the modern world that the documents took the form they have today. On this subject Mariza Peirano clarify that:

> The fact that the documents most commonly used today were introduced at the beginning of the 20th century reinforces the idea that they have their origin with the implementation of the modern state – "this horrible time of papers" -, representing an effort to combine particular elements and general knowledge. A legal document, a "paper", concedes citizenship to its holder. (Since each document has its own history, allowing for many changes over the years, and also a place in a specific configuration of documents, it is possible to think of the history of documents as an "archaeology of the state" in different contexts.)
> (…)
> The document has a force that transforms the individual into a citizen of a specific nation-state and qualifies an individual for defined activities. The relationship between the individual and the document that identifies someone is thus not only of representation, but also of contiguity and/or extension. When an individual looses his/her "identity," that experience is true in many senses. There is an element of magic of contiguity in this association: the individual becomes a citizen through his/her identity card, but when an individual finds him/herself without a card, he/she no longer has an identity (that is civil and public). The identity card produces the citizen. Those that have seen their identity forged or recognized their signature falsified on a check, for example, know the discomfort of the copy of their "self". (Peirano, 2002)

In fact the records and documents bring many benefits to the society They " facilitate the act of counting, adding, aggregating the population (as well as to tax wealth and to control production) and identifying the individual in order to confer rights and demand duties. Thus, both particular elements and knowledge about the collectivity ‐ these two inseparable components of the "modern fact" (Poovey 1998) ‐ are united in the document, in "papers" that, recognized and regulated, also identify the individual as unique and particular. The document legalizes and authorizes the citizen, making him/her visible, liable to control, and legitimate for the state. The document makes the citizen in performative and obligatory terms. This legal obligation of having a document has, of course, its underside: to remove, to dispossess,

[3] The recent discussion hosted by Robert L. Bernstein Institute for Human Rights, in march 2016, is recommended because it brings case studies but also more conceptual discussions permeating areas like law, social science and computer science. *Tyranny of the Algorithm? Predictive Analytics & Human Rights*. Bernstein Institute for Human Rights. NYU LAW. Available at: < http://www.law.nyu.edu/bernstein-institute/conference-2016 >

to deprive and to deny the social recognition of the individual who does not have a required paper in certain contexts." (PEIRANO, 2002)

The identification of the person is important since it first ensures that individual exists in the legal world, and consequently ensures the guarantee of the fundamental rights to the person. According to ID2020[9] organization, about a fifth of the world population is not properly registered. Thus, in according to UN SDG target 16.9 which aims to "*provide legal identity to all, including birth registration, by 2030.*" intends to register all by 2030.

As previously mentioned, we note that several countries have sought new solutions for their records of citizens. India, Brazil and Estonia[10] are some examples. The State policies of person identification trough biometrics and other similar mechanisms seems to be increasing as well as the identity policies that aggregate information from the several sectors of government. The E-Estonia card influenced the creation of the My Number Identification System in Japan[11]. The Aadhar implemented in India a few years ago, has attracted the attention of other countries such as Russia, Morocco, Algeria and Tunisia[12].

These new forms of identity have in most cases a mass aggregation of various personal data that used to be separated. The citizen then get a single number that represents most, if not all, government offices, this is possible when you combine all the individual data from the different public agencies into one single number. However, if the State wants to review its identity politics, aggregating data from various public sector agencies, it is necessary to check if this action is really needed and what is the purpose to be achieved.

Common justifications by the government to justify aggregation and/or combining of personal data as part of these new forms of identity is the reduction of bureaucracy, reduction of corruption, the economy in the state administration, among others. But it is necessary to remember that the overload, inappropriate, incorrect or inaccurate aggregation of personal data brings with it the danger not only of the State turning into the biggest data leakage target but also unwanted and inaccurate formation of personal categorization and interference to the individual´s identity by the state which lead to deep consequences to the society, reason why state may not be able to retain all the data of the citizen, and do it unjustifiably.

I do not criticize here the data management policies that aggregate and cross data from different sectors to a better policy to the society. If well used and managed, it can be extremely useful in designing public policies that are reliable and benefits the society as a whole. If the collect and treatment of the data have specific purposes and guarantees the protection of the person and her/his basic rights, the information generated could serve for a better planning and implementation of public policies with lower costs and lower waste of public resources, which in the end will be felt and appreciated by citizens.

However as we saw there are not just good scenarios, and to prevent the harm regarding the fundamental rights like privacy and data protection there are other ways beyond the law. If the consumer choices influenced the private sector to be concern about privacy and personal data (as we saw on item A), we argue that the public sector should bring this concern to the discussion in the pools. Policies related to privacy and freedom of the individual in the network should be in the central discussions when we are choosing our leaders, and this will be discussed in the next topic.

4. Privacy and Personal Data Protection in the Center

The privacy of data was one the issues during the recent presidential campaign of the USA. Despite not being the central theme during the discussions, the fact of being addressed by the candidates shows the potential for discussion and the growth of knowledge by the American society. According to the evaluation of Ad Age magazine , "While issues such as commercial and government data security and privacy probably won't be front and center for candidates, this appears to be the first election season in which privacy has spawned much, if any, discussion among presidential hopefuls."[13].

It was observed that the candidates Bernie Sanders, Martin O'Malley (both Democrats) and Ted Cruz (Republican) were the biggest supporters of the right to privacy, and against mass surveillance. On the other hand, Donald Trump, Marco Rubio, Jeb Bush (all of the Republican Party) were in favor of mass surveillance policies. Hillary Clinton, current candidate, is in the middle because despite having voted for the Patriot Act has been involved in the scandal of personal email use in governamental issues. We see therefore that the candidates were forced to stand on the matter, and may fall more to protect the right to privacy or support surveillance policies.

These accomplishments are not an accident since this issue has increasingly growing on the agenda. The reason is due to the increasingly presence of the internet and technology in our lives. So the discussions in this field impact us directly.

Recently in Brazil, there was an attempt by broadband providers, VIVO, OI, GVT, NET, CLARO to implement limited internet usage packages for fixed broadband (which is now unlimited)[14]. This would primarily impact the poorest who could not afford to pay for the Internet that they use today, due to the high rates. This unilateral action by the companies made civil society, consumer associations and various organizations come together to preserve the user's rights. However the most interesting was that there was a commotion not only by the experts in the field, but by many Internet users, which resulted in the collection of about 1,66 million signatures at the Avaaz´[15] petition. Consequently, on April 22, 2016, Anatel (National Telecommunication Agency), the telecom regulator in Brazil, banned indefinitely the limitation of fixed broadband usage packages. Until now this is not fully resolved.

The attempt of the telecom operators to limit the fixed broadband made the discussion reach the media and the different channels of information dissemination, which today largely depends on the Internet. Students who attend classes through the Internet, restaurant owners who offer internet in their establishment, bloggers and youtubers that work over the Internet, television networks, radio and newspapers, which offer their content and depend on the internet users, and the society at large which uses aa fixed broadband in their work and home understood the importance of their manifestation.

In this sense, issues related to the Internet, such as the issue of broadband usage limitation, net neutrality, personal data protection, may gain more attention and enter in the agenda of the upcoming election candidates. I emphasize that decisions like these that impact the formation of society and the construction of the person must be taken along long discussions by the society and not imposed by the government or the private sector.

The examples outlined above reveal that the choice of society does not always comes from the initiative of our representatives in the congress. The internet allows bottom-up decisions and within the list to be decided are the choices that society make regarding the limits of interference from the public and private sector in the construction of our identity through the manipulation of personal data.

So the construction of identity, as well as personal data and privacy protection, and all other topics related to the Internet - such as network neutrality, unlimited access, freedom of expression, etc. – are able to bring an impact in some way. Hence it is very relevant to us to understand the ecosystem of the Internet and require our government to do so.

Final Considerations

Given the above we find that identity is a construction, and in the society which we live the guarantee of the right to privacy and personal data protection is essential to the free construction of person's identity. In fact, there are many countries that have national and international instruments for the protection of personal data, like laws, regulations and treaties.

However, in addition to the traditional instruments cited in the previous paragraph to guarantee these rights, there are other ways that can also contribute not only to the protection of these human rights, but also influence the formation of laws and regulations. Among the various alternative mechanisms that can be used to ensure the right to privacy and personal data protection, we brought two examples that are growing nowadays and have a bigger potential to be widely used. The first is the monetization of protecting of privacy and data protection, as observed in the private sector. The second is the inclusion of the topic in the agenda of public policies discussed in the running of the election of our government representatives. Both of the alternatives should be used inside a set of other instruments, like the law, that influence and strengthen each other in order to protect and guarantee these rights.

So, it is really important that Internet related rights get in the agenda of discussions and public policies, the society needs to follow and participate in public policy construction and implementation verifying its transparency and the concern to protect the personal data of individuals beyond other rights. In this sense, education and awareness of issues related to the Internet is required, hence the grow of the discussions in the media and in daily talks. We can choose the society that we want, but in order to make a reasonable decision it is needed to have tools for it, since the choices have the power to directly influence the construction of our personal identity and our identity as a society.

The right to an identity as well as the right to privacy and protection of personal data are human rights declared in several laws and treaties and they must be protected and guaranteed. The protection of privacy and personal data is related to other human rights and even democracy. Society must choose how it would like to be built and this choice cannot come from the privileged sectors of society. So for a natural construction of identity, not determined in advance by the State or the private sector the appropriate protection of personal data and privacy is essential.

REFERENCES

[1] MAYER- SCHÖNBERGER, Viktor. *General development of data protection in Europe, in: Technology and privacy: The new landscape*. AGRE, Philip; ROTENBERG Marc.(orgs.). Cambridge: MIT Press, 1997.

[2] NISSENBAUM, Helen. *Privacy in Context: tecnlogy, policy, and the integrity of social life*. California: Stanford University Press, 2010.

MILLER. Clair Cain. *Revelations of NSA spying cost US tech companies*. The New York Times. March 21, 2014. Available at: < http://www.nytimes.com/2014/03/22/business/fallout-from-snowdenhurting-bottom-line-of-tech-companies.html >. Accessed in: 04. Jul. 2015.

GRIFFITHS, James. *Two years after Snowden , NSA revelatios still hurting US tech firms in China*: report. South China Morning Post. 03 July, 2015. Available at: < http://www.scmp.com/tech/enterprises/article/1831657/nsa-spy-revelations-damaging-us-tech-firmscompetitiveness-china>. Acessed in: 04 jul. 2015.

[3] KANG, Margareth H.S. *Personal data protection and the South Korean legal system*. 2016. Master Dissertation – Faculty of Law, São Paulo University, Sao Paulo, Brazil, 2016.

[4] PFITZMANN, A. BORCEA-PFITZMANN, K. CAMENISCH, J. *PrimeLife* – Chapter 1 . *in* CAMENISCH, J. FISCHER-HÜBNER, S. RANNENBERG, K - Editors. *Privacy and Identity Management for Life*. Springer-Verlag Berlin Heidelberg. 2011. Pg.10,11

[5] CASTELLS, Manuel . *The Information Age: Economy, Society and Culture. Vol.II: The Power of Identity*. Second Edition. Malden MA. Oxford UK: Blackwell Publishers. 2010.

[6] ELIGON, John. WILLIAMS, Timothy. *Police Program Aims to Pinpoint Those Most Likely to Commit Crimes.* Sept. 24, 2015. The New York Times. Availabe at: < http://www.nytimes.com/2015/09/25/us/police-program-aims-to-pinpoint-those-most-likely-to-commit-crimes.html >

[7] VIBES, John. *Police Now Using "Pre-Crime" Algorithm To Target And Label Innocent Citizens As Criminals*. Activist Post. Chicago, May 26, 2016. Available at: < http://www.activistpost.com/2016/05/police-now-using-pre-crime-algorithm-to-target-and-label-innocent-citizens-as-criminals.html >

[8] SIMITIS, Spiros. *Reviewing privacy in an information society*. 135. University of Pensilvania Law Review 707. 1987. Pg.709 – 71

[9] ID2020. Available at: < http://id2020.org/>

[10] HAMMERSLEY, Bem. *Why you should be na e-resident of Estonia*. Wired. 04 feb. 2015. Available at: < http://www.wired.co.uk/article/estonia-e-resident>

[11] JAFFE, Eric. How Estonia became a global model for e-government. Side Walk Talk.20 Apr, 2016. Available at: < https://medium.com/sidewalk-talk/how-estonia-became-a-global-model-for-e-government-c12e5002d818#.9frlcib2d >

KYODO. Japan, Estonia vow to strengthen cybersecurity cooperation. The Japan Times news. 8 Apr, 2016. Available at: < http://www.japantimes.co.jp/news/2016/04/08/national/politics-diplomacy/japan-estonia-vow-strengthen-cybersecurity-cooperation/#.V43lyfkrLIV >

[12] RAJ, Amrit. JAIN, Upasana. *Aadhaar goes global, finds takers in Russia and Africa*. Live mint. 09 Jul 2016. Available at : < http://www.livemint.com/Politics/UEQ9o8Eo8RiaAaNNMyLbEK/Aadhaar-goes-global-finds-takers-in-Russia-and-Africa.html >

[13] KAYE, Kate. *Why Data Privacy Is a Real Campaign Issue in 2016. Cruz, O'Malley, Sanders and Others Have Weighed in.* AdvertisingAge. June 17, 2015. Available at: < http://adage.com/article/privacy-and-regulation/data-privacy-a-real-campaign-issue-2016/299081/ >

DAVEY, Monica. *Chicago Police Try to Predict Who May Shoot or be Shot*.The New York Times. May 23, 2016. Available at: < http://www.nytimes.com/2016/05/24/us/armed-with-data-chicago-police-try-to-predict-who-may-shoot-or-be-shot.html?_r=0 >.

Tyranny of the Algorithm? Predictive Analytics & Human Rights. Bernstein Institute for Human Rights. NYU LAW. Available at: < http://www.law.nyu.edu/bernstein-institute/conference-2016 >

[14] BORN, Robert. *Brazilian broadband providers want to limit usage*. BRIC+ New World News.04, may, 2016. Available at: < http://www.bricplusnews.com/business/brazils-usage-limits-broadband/>

[15] *Vivo, GVT ,OI, NET, Claro, Anatel, Ministério Publico Federal: Contra o Limite na Franquia de Dados* na Banda Larga Fixa. Available at: < https://secure.avaaz.org/po/petition/Vivo_GVT_OI_NET_Claro_Anatel_Ministerio_Publico_Federal_Contra_o_Limite_na_Franquia_de_Dados_na_Banda_Larga_Fixa/?pv=49 > . Accessed in : 15, Jul. 2016.