PERSPECTIVES REGARDING DATA PROTECTION ACCOUNTABILITY

Liana-Iulia PAUL [*]

Abstract

In this article we have presented the main aspects concerning data protection accountability. The manner in which companies and regulators sustain the activity concerning the protection of individuals has also been exposed. Moreover we have discussed about the necessary instruments in providing three important goals: privacy, reliability and availability.

Further we have underlined the importance of protecting the cross-border information transfers and the role of risk management in data protection. Finally we have emphasized the principal categories of threats, harms and risks concerning data protection and also our conclusions.

Key Words: *data protection, accountability, risk management, cybercrime.*

1. Introduction

During the last years the information transfers had achieved a high level with a great impact upon our society. Starting with the internal transfers and ending with the cross-border ones, we may say that people are very exposed to different types of threats concerning their personal data.

Computer crimes had increased a lot over the last years and this phenomenon shall be at least diminished if not completely eradicated.

In this circumstance an important issue focuses on the accountability concept.

"Accountability is the fact of being responsible for your decisions or actions and expected to explain them when you are asked."[1]

According to a computer definition, accountability represents the readiness to have one's actions, judgments, and failures to act to be questioned by responsible others. It also means to explain why deviations from the reasonable expectations of responsible others may have occurred and to respond responsibly when errors in behavior or judgment have been detected. Accountability which could be defined as a critical component of professionalism is closely related to the principles of morality, ethics, and legal obligations. In a computer sense, this term associates computer with their actions while online.[2]

According to another opinion, accountability is an essential information security concept. This means that every individual who works with an information system should have specific responsibilities for information assurance. We may say

[*] M.A. "Dimitrie Cantemir" Christian University.

[1] See http://www.oxforddictionaries.com/definition/learner/accountability, accessed on april 4th 2015.

[2] See http://www.yourdictionary.com/accountability¸ accessed on april 7th 2015.

that every company should have an information security plan and each employee should respect it. The tasks for which an individual is responsible are part of the overall information security plan and are readily measurable by a person who has managerial responsibility for information assurance. An example in this area is the policy statement that all employees must avoid installing outside software on a company-owned information infrastructure. In order to check if the policy is being followed the person in charge of information security should perform periodic checks.

The duties and responsibilities of all employees, as they relate to information assurance, need to be specified in detail. Otherwise, the attempt of establishing and maintaining information security is haphazard and virtually absent. [3]

2. The Protection Offered to Individuals

The information on digital platforms is very vulnerable. From this point of view we may notice two types of protection: one offered by companies and other offered by regulators.

Starting with the first type of protection we may distinguish, according to an opinion, five important rules for accountability in cyberspace, also known as the five golden rules:

a. the board members must hold senior management accountable for cyber-security and privacy as they do for financial integrity. They should know all the right questions even if they don't know all the right answers;

b. CEOs also sustain integral to profitability, effective management, workplace ethics and consumer trust;

c. CPOs and CIOs work together understanding their inherent overlap: if personal information resides in cyber-infrastructure, privacy resides in cyber-security;

d. business line managers ensure implementation of cyber-security and privacy policies through staff supervision and training;

e. staff endorse cyber-security strategies as a matter of ethics, honouring consumer trust."[4]

Our country, Romania, has managed to achieve a good regulation in accordance with the criteria imposed by the European Convention on Cybercrime from 2001.[5] Our new Penal Code contains in Chapter IV the regulation for this spectrum.

The concept of accountability was first established in data protection by the Organization for Economic Co-operation and Development ("OECD") and it encourages robust data flows and offers protection and responsible use of information, wherever it is processed. [6]

[3] See http://www.computer-security-glossary.org/accountability.html, accessed on april 10th 2015.

[4] See http://www.dentons.com/en/insights/alerts/2015/january/26/five-golden-rules-for-accountability-on-privacy-and-cyber-security, accessed on April 17th 2015.

[5] I. Vasiu şi L. Vasiu, *Criminalitatea în cyberspaţiu*, Universul Juridic Publishing House, Bucureşti, 2011, p. 137.

[6] See http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf, accessed on April 21th 2015.

If we think about the protection of the cross-border information transfers we may notice that the practical aspects of accountability and the manner in which it can be used should suffer future improvements as they are not to well pointed out.

Moreover, "principle-based data privacy laws often leave room for interpretation."[7] This is how organizations are left to make appropriate decisions on how to implement these principles and to regulators on how to interpret and enforce the law.

It is very important that organizations develop a methodology in order to apply, calibrate and implement abstract privacy obligations based on the actual risks and benefits of the proposed data processing.

3. Instruments for 3 Goals

The fundamental computer attributes are privacy, reliability and availability.

Privacy regards several aspects starting with the localization of private data. We can say that this kind of data can be found everywhere: on "applications for schools, jobs, clubs, loans charge accounts, magazine subscriptions, tax forms, insurance claim, hospital stay, military draft registration, court petition"[8] and several others.

Therefore data should be accessed only by authorized persons.

Reliability, the second computer attribute underlines the importance of unchanging transferred data between the transmitter and the receiver.

Finally the accountability refers to computer data and systems that are reliably and timely obtainable and usable or accessible for all legitimate users in accordance with their privileges.[9] Transferred data must be available on demand.

4. The Role of Risk Management in Data Protection

In order to fulfil their daily duties, including those concerning data protection, employees must understand exactly what it is asked of them. The person in charge with this task is the security manager. Nowadays the common practices of defining generic responsibilities through employment contracts and the programs which are delivered via the intranet are not sufficient and not quite adequate. So, the employees' skills should be developed through training programs and the stakeholders should become aware of the importance of e-Education and the investments they should do in this area for their own benefit. We could also say that it is very important to analyze this issue from the security's manager point of view, but also from the controlled persons' perspective.

[7] See https://www.hunton.com/files/upload/Post-Paris_Risk_Paper_June_2014.pdf, accessed on April 30th 2015.

[8] See http://www.google.ro/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&ved=0CEgQFjAF&url=http%3A%2F%2Fwww.csie.ntu.edu.tw%2F~kmchao%2Fbcc03spr%2FChap11.ppt&ei=VLZnVY-HoHzUuDegPgJ&usg=AFQjCNGjN-SJErlSpMG2guw1sFjn949ljw , accessed on May 5th2015.

[9] I. Vasiu and L. Vasiu, *Break on Through: An Analysis of Computer Damage Cases*, Journal of Technology Law & Policy, Volume XIV – Spring 2014, Pittsburgh, p. 160.

Another important aspect regarding risk management in data protection from the employees' point of view is the everyday approach in this field through their daily tasks. Everyone is responsible of the manner in managing a vital component through the everyday activities.[10]

Lately the intruders frequently succeed in attaining their objectives by exploiting weaknesses. With persistence they can perpetrate also without sophisticated methods.

Often enterprises present inadequately secured or completely vulnerable points of entry.

Cyber attacks can produce isolated or devastating damages because of the lack of preparation and investment of the victims.

In accordance with the facts presented above a paradox is rising: despite the great efforts of the smartest specialists in this area "the security industry struggles to keep pace." [11]

There are numerous privacy management programs concerning different types of risk but it is also very important for all this programs to become more and more developed.

One of the most important aspects is to create an adequate framework to "identify, prioritize and mitigate such risks so that principle-based privacy obligations can be implemented appropriately and effectively."[12]

5. The Principal Categories of Threats, Harms, Risks Concerning Data Protection

The advanced and persistent threats in cyberspace are complex and constant attempts to "breach and bring down systems." [13]

The only effective strategy for maintaining parity with the legions of cybercriminals is to own an intelligence driven approach to security.

The threat surface is very extended and on an ongoing basis. It is so important to understand the techniques, habits and motivations of threat factors in order to eradicate and prevent cyber attacks.

[10] See http://www.computerweekly.com/opinion/Accountability-is-key-to-security, accessed on May 15th 2015.

[11] See https://blogs.rsa.com/wp-content/uploads/2015/03/h14039-failures-of-the-security-industry-wpFINAL.pdf accessed on May 16th 2015. The number of reported information security incidents around the world rose 48 percent to 42.8 million, to the equivalent of 117.339 attacks per day, according to The Global State of Information Security® Survey 2015, published in September 2014 by PwC in conjunction with CIO and CSO magazines. Detected security incidents have increased 66 percent year-over-year since 2009, the survey data indicates. The same study reports that as security incidents become more frequent the associated costs of managing and mitigating breaches are also increasing. Globally, the estimated reported average financial loss from cybersecurity incidents was $2.7 million – a 34 percent increase over 2013. Big losses have been more common this year as organizations reporting financial hits in excess of $20 million nearly doubled.

[12] See https://www.hunton.com/files/upload/Post-Paris_Risk_Paper_June_2014.pdf accessed on May 17th 2015.

[13] See https://blogs.rsa.com/wp-content/uploads/2015/03/h14039-failures-of-the-security-industry-wpFINAL.pdf , accessed on May 18th 2015.

"One truth the security industry has learnt is that cybercriminals value the element of surprise."[14]

A few recommendations were born from the necessity of facing this phenomenon:

a. be prepared - today's cyberwars are dynamic. Vigilance and readiness must be inherent in any information security plan. Vulnerability testing and monitoring should be operationalized and ongoing. A holistic response plan incorporating people, process and technology must be established, understood and embraced by all constituents. And the plan itself should be regularly evaluated;

b. prioritize – not all information assets and infrastructure are equal. Decide which are mission-critical and which are business-critical. Identify systems that cannot, for any reason under any circumstance, be breached or taken down;

c. adapt to changes in IT Infrastructure – the composition of modern IT infrastructure is increasingly open and amorphous. Cloud computing delivers tremendous business benefits – agility, future proofing, reduced IT infrastructure and support requirements, lower costs. Similarly, ecommerce, digital supply chains, and mobile networks are indispensable elements of contemporary commerce and communication. Security professionals must understand, embrace and be prepared to defend them with plans and tactics that account for the new, unique security challenges they present;

d. eliminate blind spots – in the emerging security paradigm, prevention gives way to detection. Granular visibility is paramount to spotting and stopping modern threats. Fully optimize toolsets and orient them to emerging threats, incorporating human intelligence and open source intelligence;

e. account for human weakness; accommodate the modern workforce – humans are imperfect. They are the single softest target for threat actors. Phishing, spyware and other attacks target individuals within an organization. Social media has changed the workplace and opened new entry points for malicious software. Many employees use Facebook, LinkedIn and Twitter to perform their jobs. An increasingly collaborative workplace means that people are sharing information regularly across offices, time zones and geographies, introducing new sources of risk that must be accounted for.

f. trust but verify – information security providers bring to market more advanced software and services than ever before. Confidence in security technology is well founded. However, insufficient, incorrect or non-existent human-based analysis of security events can render it ineffective. Enterprises must maintain a high state-of-alert and continue to test and strengthen security processes and technology. [15]

The most common threats which arise from data protection are as it follows:

- unjustifiable or excessive collection of data;
- use or storage of inaccurate or outdated data;
- inappropriate use of data, including;
- use of data beyond individuals' reasonable expectations;

[14] See https://blogs.rsa.com/wp-content/uploads/2015/03/h14039-failures-of-the-security-industry-wpFINAL.pdf , accessed on May 18th 2015.

[15] See https://blogs.rsa.com/wp-content/uploads/2015/03/h14039-failures-of-the-security-industry-wpFINAL.pdf , accessed on May 19 th 2005.

- unusual use of data beyond societal norms, where any reasonable individual in this context would object;

-unjustifiable inference or decision-making, which the organization cannot objectively defend;

-lost or stolen data;

-unjustifiable or unauthorized access, transfer, sharing or publishing of data.

There are three types of harm that any of the identified threats could present:

-tangible damage to individuals;

-intangible distress to individuals;

-societal.

Tangible damage includes:

-bodily harm;

-loss of liberty or freedom of movement;

-damage to earning power;

-other significant damage or economic interest.

Intangible distress:

-detriment arising from monitoring or exposure of identity, characteristics, activity, associations or opinions;

-chilling effect on freedom of speech, association, etc;

-reputational harm;

-personal, family, workplace or social fear, embarrassment, apprehension or anxiety;

-unacceptable intrusion into private life;

-discrimination or stigmatization.

For both tangible damage and intangible distress, the harm may be potential (it could or would have this effect) or actual (it will, is having or has had this effect).[16]

The main risks in data security are:

- theft – especially by using the Internet criminals can cause harm through attacks on vulnerable systems;

- loss – of laptops, for example, represents a way for unauthorized people to possess that data;

- neglect – usually after selling or recycling old computers which contain information that was not properly deleted;

- insecure practices – while collecting, storing, sending, encrypting, finding and removing data may all have implications for the persons safety. [17]

An important issue is the consumers' education regarding the risks presented above, but also the adequate security of information systems. There have been cases in which companies didn't protect in an adequate manner its informational network against predictable and reasonable cyberattacks and the authorities began investigations in that cases. [18]

[16] See https://www.hunton.com/files/upload/Post-Paris_Risk_Paper_June_2014.pdf, accessed on May 20th 2015.

[17] See https://ist.mit.edu/security/data_risks , accessed on May 20th 2015.

[18] I. Vasiu şi L. Vasiu, *Frauda cu carduri de credit şi debit: O schemă de clasificare,* Drept penal anul XIX Nr. 1, Ianuarie-Martie 2012, Bucureşti, 2011, p. 28.

6. Conclusions

In this article we have presented the main aspects concerning data protection accountability. During the last years the information transfers had achieved a high level with a great impact upon our society. Starting with the internal transfers and ending with the cross-border ones, we may say that people are very exposed to different types of threats concerning their personal data.

Computer crimes had increased a lot over the last years and this phenomenon shall be at least diminished if not completely eradicated.

In this circumstance an important issue focuses on the accountability concept.

The manner in which companies and regulators sustain the activity concerning the protection of individuals has also been exposed. The information on digital platforms is very vulnerable. From this point of view we may notice two types of protection: one offered by companies and other offered by regulators.

Moreover we have discussed about the necessary instruments in providing three important goals: privacy, reliability and availability. The fundamental computer attributes are privacy, reliability and availability.

Further we have underlined the importance of protecting the cross-border information transfers and the role of risk management in data protection. There are numerous privacy management programs concerning different types of risk but it is also very important for all this programs to become more and more developed.

Finally we can say that cybercrime is hurting the global economy. Obviously the principal categories of threats, harms and risks concerning data protection have become more advanced and persistent in cyberspace.

We may say that the doubtless failures in the system must be identified and rectified and we must also understand that cyber attacks are inevitable.

The good news is that risk can be managed in accordance with an advanced and operational planning.