COMPUTER LAW & SECURITY REVIEW 30 (2014) 179–189

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Protecting the communication: Data protection and security measures under telecommunications regulations in the digital age

*Gönenç Gürkaynak**, *Ilay Yilmaz*, *Nazli Pinar Taskiran*

ELIG Attorneys-at-Law, Istanbul, Turkey

Keywords:
Telecommunication
Security
Cyber security
Data protection
Privacy
EU
Turkey

ABSTRACT

This paper aims to provide a comparative overview and evaluation of various legal frameworks for electronic communications security in light of the recent developments in the electronic communications sector. The article also includes an insight on European Union and Turkish legal environment for data protection security in electronic communications sector.

The dynamic and ever-changing nature of electronic communication technologies brings brand new opportunities for quick access to extensive information and communication through integrated channels. On the other hand such dynamic nature paves the way for new challenges and concerns regarding electronic communications security. Both national and international sector regulators and policy-makers are encountering new threats for security of electronic communications while trying to adapt to convergence and the ongoing tendency for Internet Protocol ("IP") based digital networks.[1] Various legal frameworks come into force accordingly and legal security measures are created by the regulators and the sector actors, in order to overcome security concerns. Evolution of electronic communication technologies and new challenges that it yields, forces national and international authorities to work for unified solutions and cooperation in fighting against these challenges.

1. Introduction

The history of communication begins with the history of humanity. Invention of the optical telegraph in the year of 1792 is accepted as a corner stone of the communication systems.[2] In 1862 first fax was sent by an Italian physicist's pantelegraph and it was only 15 years before Alexander Graham Bell patents the telephone.[3] A rapid development in communication systems and invention of fax machine with the ability of scanning, invention of telautograph, audio and radio transmission took place after the following years since the worldwide communication systems emerged by virtue of Internet in1991.[4] This

* *Corresponding author*. ELIG Attorneys-at-Law, Citlenbik Sok. No: 12, Besiktas, Istanbul, Turkey. Tel.: +90 212 327 1724.
E-mail address: gonenc.gurkaynak@elig.com (G. Gürkaynak).

[1] Centre for European Policy Studies (CEPS), E-communications: Regulatory Challenges for the Post-Lisbon Era, available at http://www.ceps.eu/taskforce/e-communications-regulatory-challenges-post-lisbon-era.

[2] William von Alven, Bill's 200-Year Condensed History of Telecommunications, http://www.cclab.com/billhist.htm.

[3] Id.

[4] Telecommunications and Industrial Development, United Nations Industrial Development Organization, Research and Statistics Branch Working Paper 14/2009, Anders Isaksson, Research and Statistics Branch Programme Coordination and Field Operations Division UNIDO, available at http://www.unido.org/fileadmin/user_media/Publications/Research_and_statistics/Branch_publications/Research_and_Policy/Files/Working_Papers/2009/WP%2014%20Telecommunications%20and%20Industrial%20Development.pdf.

0267-3649/$ – see front matter © 2014 ELIG Attorneys-at-Law, Istanbul, Turkey. Published by Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.clsr.2014.01.010

was the beginning of a new era which boosted the communications' pace of improvement. Previously, before the transition to the electronic communication, communication was limited with distance and speed.[5] Electronic communications enabled people to communicate nearly as quickly as the speed of a light, over much greater distances with scores of people and vast amount of data can be transferred.

Electronic communications term encompasses all forms of communications through electronic means, including but not limited to communications via fixed line, mobile telephone, facsimile, Internet, cable or satellite. In the age of converged technologies gathering various kinds of communications in the widest possible description has significant importance due to the information technologies' rapid development. Therefore, "electronic communications" term shall be regarded as comprehensive description covering existing means of electronic communications as well as the future technologic innovations.[6]

Public Switched Telephone Network ("PSTN") and Integrated Services Digital Network ("ISDN") were considered as the most traditional and widely-used networks which are known as secure and reliable. However, by virtue of the Internet's recent improvement, electronic communications services steered for the IP based systems, as of mid-nineties.[7]

Next are the Next Generation Networks ("NGNs"), which are IP based systems providing telecommunication systems by using broadband. NGNs enable all information and services such as voice, data and media transferred through the same network. Rapidly emerging communication technologies are compatible with both IP based and new generation applications. In this respect NGN is a platform wherein all kinds of electronic information and communications are combined.[8] According to the International Telecommunication Union ("ITU"), NGNs may be described as packet switching networks providing high standards of electronic communication services and supporting various broadband technologies. As the NGNs provide mobility, services become accessible and consistent for all users. Therefore NGN enables the convergence of various networks compatible with the developments in telecommunication sector by way of providing various kinds of services through an IP based network to the end-users or in other terms the consumers.

Convergence is a concept providing all voice, data, video, imagery, and other applications and all access, transport, and other service requirements through a single telecommunications facility.[9] Convergence makes traditional regulatory approaches of telecommunication sector insufficient, since it is difficult to foresee the future issues related to electronic communications.

Electronic communications operators focus on delivering convergent services in order to keep up with the needs and requirements of the consumers.[10] The Organization for Economic Co-operation and Development ("OECD") defines convergence in two other aspects; first one is the overlapping of technology, service and companies of different sectors.[11] The other definition given by OECD for the term "convergence" is the vanishing of the technical and regulatory borders between the sectors.[12] In this respect, NGN and the term "convergence" are compatible with each other. Thus, European Telecommunications Standard Institute ("ETSI") refers NGN as convergence of PSTN, mobile networks and Internet.

It can also be argued that "convergence is expected to foster a multimedia environment where voice, audio, video, and data can be seamlessly exchanged between users".[13] Along with the social, economic, and technological developments, the need of transforming the traditional competencies and responsibilities of national regulatory authorities for the electronic communications emerged.

As a result of a legal need with respect to the above mentioned developments in telecoms world, Directive 2002/21/EC of the European Parliament and the European Union Council, stipulates that each member state shall take necessary measures to safeguard its electronic communications security, including the national regulatory authorities' establishment of specific and proportional obligations applicable to the providers of electronic communications services.[14]

2. Governmental regulators for electronic communications

The urge to establish the data protection and security measures for electronic communications sector, certain governmental bodies are established under national and international laws. Bearing in mind that mere governmental efforts are not sufficient to fight against data protection breaches and that a public private cooperation needs to be established, a number of data protection authorities have been constituted.

The Body of European Regulators for Electronic Communications ("BEREC") is an umbrella organization which is actively initiated in January2010[15] and the main authority in the Europe which serves for the development and better functioning of the European electronic communications. BEREC advises the European Commission ("EC") and national regulatory authorities on issues related to the application

[5] Id.

[6] European Commission – MEMO/05/255 14/07/2005, available at http://europa.eu/rapid/press-release_MEMO-05-255_en.htm.

[7] J. Lintao, 2005, Concern over the Security of Communication Networks, Huawei Technologies Issue 16.

[8] Available at http://www.etsi.org/technologies-clusters/technologies/next-generation-networks.

[9] J. A. Pecar, D. A. Garbin, The New McGraw-Hill Telecom Factbook, 2000, p. 722.

[10] A. D. Çaycı, Convergence Of Information And Communication Technologies With A Regulatory Point Of View: Turkish Case, 2009, available at http://www.tk.gov.tr/kutuphane_ve_veribankasi/tezler/diger_tezler/Aysel_Deniz_CAYCI.pdf.

[11] Convergence and Next Generation Networks, available at http://www.oecd.org/sti/40761101.pdf.

[12] Id.

[13] C. Saxtoft, Convergence User Expectations, Communications Enablers and Business Opportunities, 2008, England, John Wiley & Sons Ltd., p.101.

[14] Directive 2002/21/EC, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0033:0033:EN:PDF.

[15] Available at http://berec.europa.eu/eng/about_berec/what_is_berec/.

of the EU regulatory framework for electronic communications.[16]

Another important international regulator is the Independent Regulators Group ("IRG") which was established under Belgian law in 2008.[17] At the present time, IRG has 37 members which correspond to 28 European Union ("EU") member states, 4 European Free Trade Association ("EFTA") members and 5 candidate countries to the EU whereas BEREC has 28 EU member states.[18] Therefore IRG's focus might be deemed broader than BEREC due to its diverse structure.

In the United Kingdom ("UK") a separate regulatory Office of Communication ("Ofcom") was established for discussions on convergence of electronic communication technologies and infrastructures following the enactment of the Office of Communication Act in 2002.[19] The second step was made in November 2002 by introducing the Communication Bill to the parliament that will set the new regulatory framework. Before, establishment of Ofcom responsibilities in the communication sector were shared between five different bodies: The Broadcasting Standards Commission, Office of Telecommunications ("Oftel"), the independent Television Commission (licensing and regulating independent television services), the Radio Authority (licensing and regulating the independent radio services) and the Radio Communications Agency within the UK Department of Trade and Industry. The general duties of the Ofcom are set as consumer interests in relevant markets, where appropriate by promoting competition, to secure the optimal use of the radio spectrum, a wide range of TV and radio services available in the UK, and to secure that standards are applied in the communications sector.[20]

In Turkey, Information and Communications Technologies Authority ("ICTA") is the main governmental authority for regulating, controlling and developing electronic communications sector. Among its other competencies and responsibilities, ICTA is responsible for taking necessary measures and performing coordination to ensure the continuity of electronic communications in case of any threats or vulnerabilities.

The electronic communications networks' fast-growing and fast-changing nature and increase of interconnectivity, information systems and networks[21] is inevitably exposed to a growing number and variety of threats and vulnerabilities which lead to new legal problems for electronic communications security each day. Accordingly, the need for enhancing awareness and understanding of security issues within the society and to develop a culture of security has emerged. In 2012, eighteen (18) countries reported seventy nine (79) significant incidents of electronic communications security breaches to the European Union Agency for Network and Information Security ("ENISA"), in which most of them were the affected mobile telephones or mobile Internet.[22] ENISA is a network and information security center for the EU, its members, among the private sector and European citizens, assisting EU members in the application of relevant EU legislation and developing Europe's critical information infrastructure and networks.[23]

3. Standards for security in telecommunications sector

Electronic communications security aims to prevent unauthorized access to secure areas related to electronic communications, to mitigate the risks of the circumstances beyond control (e.g. natural disasters), to prevent inaccurate or incorrect information and to prevent halt of electronic communications services. In order to achieve these objectives, both the organizational and the technical aspects of security shall be taken into consideration.[24]

The most comprehensive regulation regarding the security of electronic communications in Turkey is the Regulation on Electronic Communications Security which sets out the procedures and principles for the measures which must be taken by operators in an effort to prevent the risks caused by threats and/or weaknesses by ensuring;

(i) Physical area security,
(ii) Data security,
(iii) Hardware and software security and reliability and
(iv) Personnel reliability[25]

Regulation on Electronic Communications Security covers quantitative and qualitative continuity, equal treatment, regularity, transparency and effective use of resources unless objective reasons require otherwise, protection of consumer rights and promotion of service quality and national and/or international standards and regulations.[26]

According to Regulation on Electronic Communications Security, authorized operators are obliged to make sure that they fulfill either TS ISO/IEC 27001 or ISO/IEC 27001

[16] BEREC adopts revised broadband common positions, net neutrality reports, and the 2013 work programme, available at http://berec.europa.eu/eng/document_register/subject_matter/berec/press_releases/1131-berec-adopts-revised-broadband-common-positions-net-neutrality-reports-and-the-2013-work-programme.

[17] IRG, available at http://www.irg.eu/render.jsp?categoryName=CATEGORY_ROOT.

[18] Available at http://www.irg.eu/render.jsp?categoryId=260504.

[19] Ofcom, available at www.ofcom.gov.uk.

[20] Ofcom Annual Plan 2013/14, available at http://www.ofcom.org.uk/about/annual-reports-and-plans/annual-plans/annual-plan-2013-14/.

[21] OECD Guidelines for the Security of Information Systems and Networks, Ministerial Background Report DSTI/ICCP/CISP (2007)2/Final available at http://www.oecd.org/sti/ieconomy/15582260.pdf.

[22] Dr. M. Dekker, C. Karsberg, M. Lakka, Annual Incident Reports 2012, Analysis of Article 13a annual incident reports, 2013, available at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/article-13a-annual-report-2012.

[23] About ENISA, available at http://www.enisa.europa.eu/about-enisa.

[24] R. Jay, Data Protection Law and Practice, 2012, Sweet &Maxwell, 7-02, p.302.

[25] Article 2 of the Regulation on Security of Electronic Communications, available at http://eng.btk.gov.tr/mevzuat/yonetmelikler/dosyalar/BY-LAW%20on%20Security%20of%20Electronic%20Communications.pdf.

[26] Article 5 of the Regulation on Security of Electronic Communications.

standards.[27] ISO/IEC 27001 standard is an information security standard published in October 2005 by the International Organization for Standardization ("ISO") and the International Electro-technical Commission ("IEC"), which specifies the requirements to be met by information security management systems ("ISMS")[28] and which is currently in the process of revision and expected to be published at the end of 2013.[29] This standard is an internationally recognized code which has 100 certifications 17,509 ISO/IEC 27001 issued in a hundred (100) countries at the end of December 2011. On the other hand, TS ISO/IEC 27001 is the equivalent of ISO/IEC 27001 adopted by Turkish Standards Institute in order to establish an effective information security system and to provide certification for the operators.[30] The security standards set out in ISO/IEC 27001 are generic and are convenient to all organizations, regardless of type, size and nature and all sectors, with minor modifications.

Imposing upon the operators the obligation of complying with international standards with national regulations is inevitable and crucial due to the dynamic needs of the telecommunications sector. Moreover, harmonized standards are mandatory for the operators as this sector is borderless.

The Security of Electronic Communications Regulation obliges the operators to comply with these standards within a year as of their authorization date and this period can be extended, should the Information and Communication Technologies Board ("Board") find it necessary. The Board extended this period to two years as of the authorization date for all operators, which are authorized after publication of the regulation (i.e. July 20, 2008), with its decision of June 24, 2009.[31] If an operator does not comply with this requirement within its legal period, it might be subject to administrative fines by the Board according to the Article 34 of the Regulation on Administrative Fines and Other Sanctions and Measures to be Imposed upon Service Providers by the Telecommunication Authority ("Sanctions Regulation"). These administrative fines might vary according to the circumstances such as type of the breach, size of the loss, the financial gain in return and its magnitude, reoccurrence, previous breaches and good faith, pursuant to the Article 32 of the Sanctions Regulation.[32]

On the other hand, a new regulation to replace the Regulation on Electronic Communications Security is open to public opinion since September 9, 2013. This new Regulation on Electronic Communications Security obliges the operators to comply with these standards within a year as of their authorization date. This period may be extended, should the Information and Communication Technologies Board ("Board") find it necessary. The Board extended this period to two years as of the authorization date for all operators, which are authorized after publication of the regulation (i.e. July 20, 2008), with its decision of June 24, 2009.[33] If an operator does not comply with this requirement within its legal period, it might be subject to administrative fines by the Board according to the Article 34 of the Regulation on Administrative Fines and Other Sanctions and Measures to be Imposed upon Service Providers by the Telecommunication Authority ("Sanctions Regulation"). These administrative fines might vary according to the circumstances such as type of the breach, size of the loss, the financial gain in return and its magnitude, reoccurrence, previous breaches and good faith, pursuant to the Article 32 of the Sanctions Regulation.[34]

The new Regulation brings some significant changes to the Regulation on Electronic Communications Security which was published on Official Gazette on July, 20, 2008. The new regulation introduces certain brand new definitions, concepts and governmental bodies to the Regulation on Electronic Communications Security which are mostly new definitions, concepts and governmental bodies for Turkish law (e.g. certificate of authority, information security management system ("ISMS"), information security management system standard, information system, information integrity, accessibility, critical infrastructure, critical information, risk evaluation, risk processing, risk based analysis and Cyber Security Board, etc.).

As a governmental step for maintaining cyber security in Turkey, a cabinet decision regarding conducting, managing and coordinating national cyber security activities came into force on October 20, 2012. Moreover, on June 20, 2013, another decision on the national cyber security strategy and action plan for the years 2013–2014 came into force. Under the decision of October 20, 2012, a Cyber Security Board was established in Turkey. The Cyber Security Board of Turkey is entitled to determine the governmental precautions regarding cyber security, to approve national cyber security strategies and procedures and principles within this scope and to maintain the national cyber security and coordination.

The new Regulation on Electronic Communications Security also extends obligations of the operators. Moreover, some of the operators defined under Article 5/2 of this new regulation, i.e. operators providing infrastructure operation services, operators which are operating under concession agreements,

[27] Article 11 of the Regulation on Security of Electronic Communications.

[28] ISO/IEC 27001:2005 Abstract, available at http://www.iso.org/iso/catalogue_detail?csnumber=42103.

[29] Katie Bird, New version of ISO/IEC 27001 to better tackle IT security risks, 14.08.2013, available at http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1767.

[30] Available at http://www.tse.org.tr/hizmetlerimiz/belgelendirme-hizmetleri/sistem-belgelendirme/belgelendirme-yap%C4%B1lan-y%C3%B6netim-sistemleri/ts-iso-iec-27001-bilgi-g%C3%BCv-y%C3%B6netim-sistemi.

[31] Available at http://www.btk.gov.tr/mevzuat/kurul_kararlari/dosyalar/kkehgy.pdf.

[32] Available at http://www.btk.gov.tr/mevzuat/yonetmelikler/dosyalar/05_09_2004%20.pdf.

[33] In January 23, 2013 the Board issued a fine in the amount of TRL 589,967.97 (which corresponds to %0.008 of the operator's net sales for the year 2011) for one of the leading communication and convergence technology operators in Turkey, regarding its failure to meet certain standards stipulated under TS ISO/IEC 27001 and ISO/IEC 27001 during configurations of a device.

[34] In a recent decision, the Board decided to send an official warning letter to two telecommunications companies, which did not certify their conformity with the Standards, and requested them to obtain and submit their certificates of conformity within six months. On the other hand, in the same decision, the Board decided to merely send an official warning letter to the other two telecommunication companies, which certified their conformity with a delay. This decision demonstrates the Board's approach on certification of conformity and variety of its sanctions based on the circumstances. Available at http://www.btk.gov.tr/mevzuat/kurul_kararlari/dosyalar/2013%20DK-BTD-348.pdf.

mobile phone service operators, mobile phone operators providing services for air vehicles, Internet service providers, mutually used radio service operators, fixed phone service operators, virtual mobile network service operators, satellite communication service operators, satellite and cable TV service operators have additional obligations, provided that their annual sales are above 15.000 (fifteen thousand) Turkish Liras.

All operators are obliged to establish ISMS, containing all services, infrastructures and networks of such operator. Management body of the operator is obliged to publish an ISMS policy including the understanding of such operator regarding information security under Article 7 of the new Regulation. Operators shall monitor and keep the system record files for two years including but not limited to user identities, login and logout history of the users, system changes, special authorizations of certain users.

Non-disclosure agreements will be also mandatory once the new Regulation becomes effective. The amending Regulation stipulates the minimum requirements for the non-disclosure agreements which will be signed in between the operators and its employees and operators and third parties.

The new Regulation on Electronic Communications Security, with its Article 36, requires operators to obtain a certificate of conformity from the certification authorities. The operator, if obtaining certificate of conformity for the first time, should obtain it in one year following the end of the year of which the obligation status of the operator has changed. Operators are obliged to inform ICTA within two months, in case there is a certain amendment on the certificate of conformity or in case of the certificate of conformity is renewed.

Operators are also obliged to prepare an electronic communications security report by the end of March of each year and to send such a report to ICTA through electronic means. The hardcopy of the electronic communications security report shall be kept for five years by the operator. The content of the electronic communications security report is set out under Article 37 of the new Regulation. Under Article, the operator is obliged to inform ICTA in case there is a full-scale breach against electronic communications security.

Amending the Regulation on Electronic Communications Security introduces definition of anonymizing data. On the other hand, it prohibits export of both traffic data and location data abroad which might affect the relations of the operators with international business partners. Therefore, amending the regulation brought more strict rules on data protection which might affect business structures of operators in Turkey.

4. Security measures

In December 2010, ENISA drew up a guideline on security measures for electronic communications within EU.[35] This guideline titled "Technical Guideline for Minimum Security Measures" sets out security measures that categorized in different sections. These categories are (i) governance and risk management, (ii) human resources security, (iii) security of systems and facilities, (iv) operations management, (v) incident management, (vi) business continuity management, (vii) monitoring, auditing and testing.[36] The guideline provides security measures operators and providers of public communications networks should take to ensure security and integrity of these networks, and lists down the minimum security measures that national regulatory authorities of the EU members should take into account for their assessment of public communications network providers' compliance with the relevant legislation.[37]

Current Turkish electronic communications legislation imposes various obligations on the electronic communications operators for taking all possible measures and actions to prevent electronic communications security breaches, in order to provide integrity, confidentiality, continuity, reliability, nonrepudiation, thus the security in the electronic communications services.[38] The foregoing objectives might be achieved by ensuring (i) physical area security, (ii) data security, (iii) hardware-software security and reliability and (iv) human resources security. Data protection policies of Turkey are in line with the data protection policies of the EU. Amendments on Turkish data protection legislation mostly refer to EU regulations. On the other hand, EU's data protection policy does not prohibit transfer of data abroad if the country to which the data will be transferred has a specific data protection law.

4.1. *Physical area security*

Under Turkish laws, the physical area security measures to be taken by the operator may be grouped as indoor security sensitive area measures, outdoor security sensitive area measures and measures for both security sensitive areas.

The indoor measures set out in the Regulation on Electronic Communications Security are the operators' obligations (i) to specify the authorities for entrance and access and permit entrance and access of only authorized persons, (ii) to keep records of the visitors' information entering the building and ensuring that they enter the permitted sections of the premises, (iii) to make sure that all persons in the building carry identity or entrance cards in view, (iv) to keep the entrance and access authority information up-to-date.[39] On the other hand, as for the outdoor measures, the operators are obliged to control access to the facilities including infrastructure items and to put warning signs where necessary.

[35] Technical Guideline for Minimum Security Measures, available at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/minimum-security-requirements/copy_of_minimum-security-requirements/technical-guideline-on-minimum-security-measures.

[36] Executive Summary, Technical Guideline for Minimum Security Measures, available at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/minimum-security-requirements/copy_of_minimum-security-requirements/technical-guideline-on-minimum-security-measures.

[37] Technical Guideline for Minimum Security Measures, available at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/minimum-security-requirements/copy_of_minimum-security-requirements/technical-guideline-on-minimum-security-measures.

[38] Article 19 of the Regulation on Authorization in the Electronic Communications Sector.

[39] Article 7 of the Regulation on Security of Electronic Communications.

Besides, operators are obliged to refrain from conducting unscheduled activities, prevent entrance of unauthorized devices to and create physical area security schemes in all security sensitive areas (i.e. indoor and outdoor) in order to prevent any malicious activities.

Physical area security includes the measures to be taken for prevention of unauthorized access to the work area and to the information therein. One can easily control and take hold of the electronic communications devices and exploit them for illicit purposes, if he/she has physical access to them. Therefore in order to ensure security of electronic communications it is necessary to primarily secure the physical environment. For these purposes it is necessary to keep electronic communications devices locked, to use passwords or keep devices off, when they are not used. Also it is necessary to ensure that the authorized person has access to the information therein and to monitor the entrance to the areas in which the electronic information is kept.

On the other hand, as previously indicated above, there is always the risk of encountering natural disasters such as earthquakes, hurricanes, flood or terror attacks which are beyond one's control. The measures to be taken with respect to such unforeseeable circumstances should also be considered a part of physical area security. Establishing a secure information system infrastructure is necessary for providing uninterrupted flow of information and to prevent the halt of communications.

On September 9, 2009 there was a flash flood in Istanbul, Turkey which killed at least thirty one people[40] and was regarded as "the worst flooding in decades".[41] The flood led to a huge damage to the infrastructure and it destroyed a leading global telecommunications company's data center in Istanbul. The company suffered both physical losses and, as a side effect, technical difficulties[42] which had a negative effect on the company's reputation. This event was brought to the Board's attention and the Board decided to send an official warning letter to the telecommunications company for causing damages to its data center by acting in a negligent and inattentive manner, and not taking the necessary actions with respect to physical area and environment despite the fact that there were similar floods in the same area previously, and to investigate the case at hand.[43]

4.2. *Data security*

Data security defines protection of data from all threats and jeopardies, including but not limited to unauthorized access to, use, disclosure, disruption, modification, perusal, inspection, recording or destruction of data, while collecting, communicating it to the end users, retaining and using, and all measures to be taken in advance and actions to be taken during any attempts to commit security breaches so as to preserve confidentiality, integrity, non-repudiation, reliability and availability of information.[44]

Data security breaches may give rise to financial loss, loss of customer confidence and lead to regulatory action.[45] It appears that challenges in this area are going to get harder rather than easier in the future as the technology changes rapidly.[46] Hence it is not possible to ensure data security by using merely one security solution. In order to make sure that the data is completely secure one must use multiple measures to have the sufficient precautions for threats.

According to the European Parliament's and the European Union's Council's Directive 2002/58/EC (i.e. EU directive on privacy and electronic communications) electronic communications service operators should take both technical and organizational measures to safeguard security of its services and network security and these measures shall ensure a level of security adequate for the risk encountered.[47]

Points to take into consideration in order to provide electronic communication security are listed in ISO/IEC 17799 (Information technology- Code of practice for information security management) as data confidentiality, integrity and availability. ITU broadened the scope of electronic communication security elements in its X.805 Recommendation.[48] According to ITU's relevant recommendation, the security elements are classified as access control, authentication, non-repudiation, data confidentiality, communication security, integrity, availability and privacy.[49]

In Turkey, Regulation on the Amendment of Regulation on Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector ("Electronic Communications Data Protection Regulation") was published in the Official Gazette on July 11, 2013. There have been some significant changes made to the previous electronic communications regulation.

Recent amending Electronic Communications Data Protection Regulation also serves for such harmonization process with the European Union legislation, and aims to keep up with recent technological developments. Electronic Communications Data Protection Regulation sets forth certain protective measures for the personal information of subscribers or users of the electronic communication services, including but not limited to the following ones. Article 5 of the amending Electronic Communications Data Protection Regulation stipulates that traffic data required for marketing of the electronic

[40] Available at http://www.nytimes.com/2009/09/10/world/europe/10turkey.html?_r=0.

[41] Available at http://www.hurriyetdailynews.com/default.aspx?pageid=438&n=flash-floods-immerse-istanbul-highway-stranding-dozens-of-2009-09-09.

[42] Available at http://www.datacenterknowledge.com/archives/2009/09/14/video-data-center-floods-in-istanbul/.

[43] Information and Communication Technologies Board's decision of 07.01.2010 numbered 2010/İK-12/04, available at http://www.tk.gov.tr/mevzuat/kurul_kararlari/dosyalar/2010%C4%B0K-12-04.pdf.

[44] ISO/IEC 17799:2005.

[45] Rosemary Jay, Data Protection Law and Practice, 2012, Sweet &Maxwell, 7-01, p.301.

[46] Sir Gus O'Donnell, Data Handling Procedures in Government, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60966/final-report.pdf.

[47] Article 4 of Directive 2002/58/EC, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF.

[48] Zachary Zeltsan, ITU-T Recommendation X.805 and its application to NGN, available at http://www.itu.int/ITU-T/worksem/ngn/200505/presentations/s5-zelstan.pdf.

[49] Id.

communication services and providing value added electronic communication services, may be processed only by anonymizing the data or obtaining the consents of subscribers or users after they are properly informed. Such processing may only be performed in accordance with the consent obtained from the user or subscriber and in the amount and for the time required by the electronic communication services, marketing activities and similar services.

Location data and identity of the relevant persons may only be processed in case of a disaster, a state of emergency and an emergency call, in the absence of consent by the subscriber or user, other than the cases designated under relevant legislations and judicial decisions.

The term "anonymizing" is described under Article 1 of the Electronic Communications Data Protection Regulation as processing data in a way that they cannot be associated with any real person or legal entity who is identified or identifiable or in a way of preventing the identification of the source.

Another significant amendment which might be criticized is about the transfer of personal information abroad. In accordance with the Article 2 of the amending Electronic Communications Data Protection Regulation, personal data cannot be transferred abroad. This article may have certain side effects as to the nature of the development of information technologies. As an example such provision may constitute an obstacle against using the cloud computing services which sometimes require transfer of personal data abroad. Also this provision might affect the free flow of the data of within or in between multinational companies. Although ICTA states that this article is for banning transfer of data abroad for commercial purposes, the wording of relevant article, apparently, does not include such an annotation.

As for EU Data Protection Directive, transfer of personal data from a member state to a third country with an adequate level of protection is authorized. "Adequate level of protection" requirement under this provision is explained as having a separate data protection law. Although there is a data protection draft law of 2008 in Turkey; it has not yet entered into force. Therefore transfer of personal data from an EU member state to Turkey is not authorized under EU Data Protection Directive. Moreover, the recent amendment has also disabled the transfer of personal information abroad. Under these circumstances free flow of personal information in electronic communications sector is more restricted than ever.

Due to Article 4 of the amending Electronic Communications Data Protection Regulation, in case of a violation risk of network security and the personal data, operator is obliged to inform the ICTA. Should ICTA deem necessary, the operator also informs its subscribers or users about this risk in an effective and prompt manner. Even if the general effective date of the Regulation is July 24, 2013; this informing obligation has a specific effective date, which is January 1, 2014. Additionally the Authority has the right to request all the information and documents with respect to the systems in which personal data is kept and the security measures taken by the operators, from the operators and to request changes in the aforementioned security measures. Electronic Communications Data Protection Regulation has not specifically regulated under which circumstances ICTA may find informing the users "necessary". Therefore this provision is criticized for granting broad discretion and power to the ICTA.

The permission given to the operator by the subscriber or user also involves processing of the personal data by the parties which are authorized by the operator. Having said that, the process should be carried out fitting within the purposes of the service provided to the subscriber or user. If a third party is authorized by the operator for processing the personal data of the user or subscriber, the operator is liable for ensuring the personal data's privacy, security and use of data compliance with the purpose of the service, including violation of the Electronic Communications Data Protection Regulation by the third parties.

The traffic data processed and stored shall be deleted or anonymized after the completion of the activity required for the processing and storage in the first place.

4.2.1. *Integrity*

In order to ensure the security of electronic communication, confidentiality and integrity of the information transferred from sender to receiver, authentication of the sender, nonrepudiation of the sender or the processor, continuity of the communication shall be provided. Integrity guarantees that information is not altered coincidently or intentionally.

Integrity is the consistency of the data and occurrence of the stored data. Integrity may also be interpreted as protection against unauthorized modification or destruction of information. The elements of accuracy, relevancy, and completeness are the key factors of integrity. Assume that a person needs hospital treatment that includes taking a daily medication dosage of 10 mg, but by accident the electronic record of the treatment is changed to a dosage of 100 mg which may cause fatal consequences[50]. This everyday life example displays the importance of data integrity and the consequences a failure of ensuring data integrity may lead to.

Signature, barcode and stamp may be thought as examples of measures corresponding to electronic signature to ensure data integrity. Authentication is another key factor for a secure electronic communication system as it confirms the identity of the sender regarding an electronic communication. Notary, identity card and driving license are examples of identity confirmation methods used frequently. Similar to the integrity, extract algorithm, electronic signatures, certificates are used for confirmation of identification.

4.2.2. *Confidentiality*

The term "confidentiality" might be simplified as ensuring nondisclosure of the electronic information. Sealed envelopes may be used in everyday life to provide confidentiality of the information transferred; whereas encryption methods are used for confidentiality of electronic communications data.

Cryptographic methods are commonly used for data security. Cryptographic security aims to provide confidentiality, along with integrity of the electronic communication as well as nonrepudiation and approval of the parties of

[50] Ed Gelbstein, Ph.D, Data Integrity—Information Security's Poor Relation, 2011, ISACA Journal Vol. 6, available at http://www.isaca.org/Journal/Past-Issues/2011/Volume-6/Documents/11v6-Data-Integrity-Information-Securitys-Poor-Relation.pdf.

communication. In cryptography systems, the methods used are simply encryption and decryption. In data encryption systems, original version of the data is transferred into an alpha-digital data by the encryption key. For decryption of this data, decryption key is used to transfer the encrypted data into the original data form.[51]

There is a variety in the application of encryption as a security measure for overcoming the data security threats throughout the world. The UK Code of Practice on electronic directories advises use of encryption and recommends its use for all directories in order to avoid misuse.[52] EU member countries such as Italy and Spain are promoting use of encryption in specific circumstances such as in the processing of sensitive data. In Italy, fines of up to 60,000 Euros are rendered for non-compliance with these requirements for sensitive data, and further use of sensitive data is prohibited.[53]

The Spanish Royal Decree 994/1999 on security measures for automated databases requires any sensitive data to be transmitted as long as it is encrypted.[54] This obligation applies to sensitive data transmitted through a public network. Therefore private networks used within a group and which are not available to the public are exempted from this obligation.

Encrypted electronic communications, including software with encryption capabilities, of entities in Turkey, except for the Turkish Army Forces, Gendarmerie General Command, Coast Guard Command, National Intelligence Organization, General Directorate of Security and Foreign Ministry, are subject to ICTA's permission.[55] ICTA requires prior permission for use of encrypted communications and software even if this software will enable encrypted communication between two computers in different buildings in Turkey, unless it is used via close circuit. Furthermore any changes to form or content of the encrypted communication, after its approval by the ICTA is also subject to ICTA's permission.

Operators shall provide different and alternative communication channels, backup systems, and maintenance in order to ensure continuity of the electronic communications. Just to provide a clear picture of the foregoing sentence, a mobile phone operator may provide continuity of its electronic communications services by providing alternative Internet services through WAP, edge, 2G, 3G or 4G. If there are any failures in one of these telecommunication networks, then the Internet service may be provided through the other networks and this will secure continuity of the electronic communication services.

4.3. *Hardware and software security*

4.3.1. *Hardware security*

The term "hardware" refers to the physical components of a computer system which consists of electronic circuits. Hardware, as a physical component, executes stores and transports the data and should be protected from any harm and/or theft. The threats directed to the hardware may be unauthorized access and intentional or unintentional damaging the hardware by stealing, breaking, destroying or seizure by third parties. In order to restrict access to the hardware, applying locks and keys are practical tools. Securing the physical location of the computers or other devices may also be useful to protect the security of the hardware. Moreover negligence may also constitute a threat directed to the hardware. While the bugs entering into electrical circuits may cause short circuit, mice nibbling the cables threaten the security of hardware. Dust on the hardware is also a problem as it blocks fan vents and may damage the hardware.

The physical security of hardware, such as prevention of harm or theft, is also an essential element of hardware security. In the United States of America ("USA"), stealing laptops in the airport while a passenger puts his/her laptop on the conveyer was very frequent before September 11, 2011. However after the terrorist attack of September 11, 2011, USA tightened its security process and policies at the airports, as well as several other countries, which contributed to the assurance of physical security of hardware.[56]

Another good example for consequences of hardware security breaches is an incident reported to ENISA in 2012, where a fiber optic cable was cut off due to a cable theft attempt. The incident affected 70,000 fixed telephony users and 90,000 fixed Internet users. This incident demonstrates the possible magnitude of hardware security breaches' consequences.[57]

4.3.2. *Software security*

Software includes applications, operating systems and assorted command utilities. Software programs are generally the easiest target of accidental or intentional attacks among the other components of the information security system.[58] In order to ensure software security, threats directed to software should be stonewalled.

Removal of software appears to be the most significant threat directed to software security. On the other hand alteration of the software programs is another significant threat against its security, which requires additional knowledge and effort and which is mostly conducted by viruses, worms and

[51] Dr B. Gladman, Wassenaar Controls, Cyber-Crime and Information Terrorism: A Report by Cyber-Rights & Cyber-Liberties (UK), 1998, available at http://www.cyber-rights.org/crypto/wassenaar.htm.

[52] Jethro Perkins, Encryption Guidelines http://www.lse.ac.uk/intranet/LSEServices/IMT/about/policies/documents/Guidelines-Encryption-Guidelines-v1-1.pdf.

[53] Encryption Laws and Compliance for the European Union, available at http://www.echoworx.com/wp-content/uploads/European-Compliance-Laws-3.pdf.

[54] Spanish Royal Decree 994/1999, available at http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs_ingles/reglamento_ingles_pdf.pdf.

[55] Article 5 of the Regulation on the Procedures and Principles of Coded or Encrypted Communication of Public Entities and Real Persons and Legal Entities in Electronic Communication Service.

[56] Michael E. Whitman, Herbert J. Mattord, Principles of Information Society, 2012, Course Technology, Fourth Edition, p.16.

[57] Dr. M. Dekker, C. Karsberg, M. Lakka, Annual Incident Reports 2012, Analysis of Article 13a annual incident reports, 2013, available at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/article-13a-annual-report-2012.

[58] Michael E. Whitman, Herbert J. Mattord, p.18.

Trojan horses. In order to protect the software from foregoing attacks, all software related to electronic communications such as operating systems, application software and embodied software are required to be licensed and updated regularly.

In Turkey the Regulation does not make any distinction with regards to hardware and software security, and refers to them as a unit. According to the Regulation it is necessary to encode the network, whether wireless or cable, through which the hardware/software and their components communicate, to be solely accessed by the authorized persons. It is also required to control and monitor all hardware/software components to be kept under control and monitored at all times in order to prevent any security threats.

The operators are obliged to examine the hardware/software during their purchase, use, maintenance and repair, in order to identify whether they contain any illegal interception and/or monitoring components. In case of an illegal component, the operator shall cease the use of such hardware/software, record and report it. Then it shall take necessary precautions to prevent any possible threats that may occur due to the illegal component. Another obligation for the operators is to determine the critical hardware/software which are significant for the confidentiality, integrity and continuity of electronic communications and create back-ups for such critical hardware/software.

On April 27, 2012 a leading Turkish electronic communication services operator's Internet services were cut widely due to a malfunction in their critical data infrastructure.[59] This malfunction was caused by a configuration error at a device, which is not a top tier device in the network hierarchy (t3). The Board investigated the case and rendered an administrative fine to the operator, in the amount corresponding to 0.008% of the operator's net sales for the year 2011. The Board based its decision on five grounds and stated that the configuration on the device was (i) made on the live systems, (ii) not planned in advance, (iii) conducted by only one person without any approval mechanisms, (iv) initiated before it was examined, (v) not planned and the modifications to current systems were not documented.[60] The Board concluded that these practices do not meet the international standards and/or the quality standards of ICTA.

4.4. *Human resources security*

Lack of training and education of the employees of a company is one of the most security-threatening components of the information security system. Enhancing awareness of the personnel regarding their roles and responsibilities with respect to information security should not be underestimated. The company's vital information provided to the personnel might also raise security problems after the personnel resigns. A former employee might act with the feeling of revenge and attack the information security. These probabilities should be considered and the companies must take appropriate precautions.

Individuals may be considered the weakest link in a security chain.[61] Unless the personnel security is fully obtained, other security measures regarding technical and physical security become useless. For example restricting access to a system with limited personnel will not provide the intended protection if the employees authorized to have access share the passwords with unauthorized persons.

In Austria employers are obliged to inform their employees of the security requirements under their data protection laws and policies.[62] In the Netherlands only the employees who have right to access certain information may access such information and if there are any de facto exceptions (exceptions other than legally permitted ones) made against this rule, employers are held liable for it.[63]

On the other hand, in the UK, employers are also obliged to take reasonable measures to prevent their employee's unauthorized access to certain information. However, these reasonable measures have a broader range than it is in the other countries. The steps to be taken by the employers may be a minimum supervision up to a diligent verification depending on the circumstances of the case.[64]

To prevent the employees from intentionally or accidentally damaging the information systems, the legislation should regulate the acts of the personnel. Pursuant to the Regulation, employees working in electronic communications should be experienced or trained sufficiently and duties and responsibilities of the personnel should be clearly stated. Having said that training of the employees solely would not be sufficient to maintain data protection and the actions of the employees affecting data protection should be monitored.

Another example is the regulations issued under the United States' Computer Security Act.[65] These regulations require federal agencies to provide mandatory periodic training regarding computer security awareness and accepted computer practice for the employees who deal with the management, use or operation of a federal computer system under the supervision of a federal agency.

The security awareness of the employees is the key factor among all the other components of information security, as it minimizes the risk regarding the use of information systems and networks. Personnel's reliability should also be questioned before recruitment. Pursuant to the Regulation record of previous convictions document should be requested from the employees who wish to be involved with the management, use, access or operation of a computer system.

[59] Available at http://haber.sol.org.tr/bilim-teknoloji/turk-telekoma-internet-kesintisi-icin-590-bin-tl-ceza-haberi-68508.

[60] Information and Communication Technologies Board's decision of 23.01.2013 numbered 2013/DK-SDD/65, available at http://www.tk.gov.tr/mevzuat/kurul_kararlari/dosyalar/2013%20DK_SDD-65.pdf.

[61] Michael E. Whitman, Herbert J. Mattord, p.38.

[62] Available at https://www.rtr.at/en/tk/Betreiberservice.

[63] Hogan & Hartson LLP and Analysys Consulting Ltd, Preparing the next steps in regulation of Electronic communications, available at http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/next_steps/regul_of_ecomm_july2006_final.pdf.

[64] Id.

[65] Available at http://csrc.nist.gov/groups/SMA/ispab/documents/csa_87.txt.

5. Notification obligation of the operators

In 2011 EU members, introduced with the Article 13.a of the Framework Directive (2009/140/EC)[66] the security and integrity of public communication networks. Article 13.a of the directive states that providers of public communications networks should take measures to ensure the security and integrity of their networks and continuity of services provided over these networks.[67] Third paragraph of Article 13.a obliges the operators to report significant security breaches and losses of integrity and that, annually, summary reports about significant incidents should be sent to ENISA.[68]

In 2010, ENISA, EC, Ministries and Telecommunication National Regulatory Authorities convened several times to achieve a harmonized implementation of this article.[69] In these meetings, a working group of experts from NRAs reached a consensus on two non-binding technical documents providing guidance to the NRAs in the member states: Technical guideline for incident reporting and Technical guideline for minimum security measures.[70]

The thresholds for breaches subject to notification to ENISA were based on period of unavailability[71] and the number of affected subscribers. These thresholds are announced to the operators each year. Just to provide an example, in a case reported to ENISA in 2012, mobile network and text message services were interrupted for 650,000 subscribers of one operator for seven hours[72] In another instance, fixed telephone network and fixed Internet access were interrupted for 339,000 subscribers of one operator for over four hours. These examples set forth good examples of how these thresholds should be construed by the national regulatory authorities and the operators.

On the other hand, in Turkey, besides taking the precautions and security measures mentioned above, the Regulation also requires the operators to obtain a risk analysis on their technical and administrative structure, regarding the threats and vulnerabilities, from an independent institution at least once a year, so as the EU countries are obliged to do, and take necessary precautions as per these risk analyses.[73]

Operators are also obliged to prepare an annual report regarding electronic communications security, submit them to ICTA when requested and/or during the ICTA audits, and keep these annual reports at least five (5) years.[74] These annual reports shall include at least the following information:

(i) The threats and vulnerabilities determined by the risk analysis, their categorization (e.g. low, medium, high risks), their probabilities and precautions,
(ii) The actions to be taken in case a threat or vulnerability occurs and the personnel which are in charge of such activities, a diagram of their authorities and responsibilities and emergency plans,
(iii) Installation, use and operation of the hardware/software components, and the problems and disorders reported during their repair and maintenance.

The Electronic Communications Data Protection Regulation also sets out the period of storing personal information. In accordance with the Article 10 of the amending Electronic Communications Data Protection Regulation; personal data, which is subject to investigations, evaluations, inspections or disputes, shall be stored until the relevant process is concluded. In any case, records regarding the access to personal data and relevant systems shall be stored for four years.

6. Conclusion

It appears that the domestic laws of countries stipulate differing provisions for electronic communications security and implement different practices, but commonly imposing obligations to the operators to take necessary measures, both technical and organizational, to ensure security of electronic communications. As the electronic communications network gets wider and the interconnectivity increases, the issue of security becomes supranational. The national standards and legal framework need to be harmonized and unified. Furthermore, as the internationally recognized standards, such as ISO/IEC 27001, are in the revision process, both the regulators and the other actors of electronic communications sector should be alerted for future developments on the electronic communications security requirements they might face.

Therefore the precautions to be taken against these threats should be diversified accordingly. The need for creating new ways to overcome these threats, which had never been attempted before, emerged. The national regulatory authorities and international regulatory organizations shall lead the developments in fighting the security threats and act responsibly for mitigating the consequences of any unexpected breaches. It is important to at least determine to the minimum levels of appropriate measures[75] to ensure security of electronic communications in more detail.

[66] Directive 2009/140/EC, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF.
[67] Id.
[68] Id.
[69] Article 13a Working Group portal, available at https://resilience.enisa.europa.eu/article-13.
[70] Technical Guideline for Minimum Security Measures, available at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/minimum-security-requirements/copy_of_minimum-security-requirements/technical-guideline-on-minimum-security-measures.
[71] Procure Secure, A guide to monitoring of security service levels in cloud contracts http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts/at_download/fullReport.
[72] RTR Communications Report 2012, available at https://www.rtr.at/en/komp/KBericht2012.
[73] Article 11 of the Regulation on Security of Electronic Communications.
[74] Article 12 of the Regulation on Security of Electronic Communications.
[75] Hogan & Hartson LLP and Analysys Consulting Ltd, Preparing the next steps in regulation of Electronic communications.

Finally, even though Turkish laws appear to be in conformity with the recent international standards and regulations regarding electronic communications security, the Turkish legal framework for electronic communications security is not comprehensive enough to embrace future developments in the electronic communications sector. The regulators may consider revising the essential regulations for electronic communications security in a more inclusive manner in order to provide quantitative and qualitative continuity, equal treatment, regularity, transparency and effective use of resources, protection of consumer rights and promotion of service quality.

Certain provisions under Turkish law with respect to data protection for electronic communications sector, such as restricting transfer of electronic communications data abroad may hinder international business relations and foreign investments in electronic communications sector. Hence the legal framework with respect to data protection for electronic communications sector should be revised in a proportionate way to both protect the data and the companies in this sector.