BILETA British & Irish Law, Education and Technology Association
21st BILETA Conference: Globalisation and Harmonisation in Technology Law
April 2006, Malta.

Integrity: using the undefined

M.C. van Stekelenburg
Computer/Law Institute, Faculty of Law, Vrije Universiteit Amsterdam
m.c.vanstekelenburg@rechten.vu.nl

1. Introduction

On the 14th of December 2005 the European Parliament adopted the proposal on the retention of data processed in connection with the provisions of public electronic communication services and amending Directive 2002/58/EC (further to be referred to as the "Data Retention Directive") as an expedient in the fight against terrorism. The Directive has been the subject of much discussion, not only by the Parliament that rejected the former proposals on this Directive, but also by many interest groups (internet providers, privacy- and human rights watchers, consumer groups, etcetera). At the same time, several states of the USA had been adopting laws that have to secure people's personal data. These laws are the result of recent scandals where private data collection companies reported breaches in their computer systems which opened the risk of identity theft for hundred thousands of people.

Both the Directive and the American laws on the protection of privacy use the terms data security and especially data confidentiality and data integrity. What is to be understood by data confidentiality is often not under discussion, because the term confidentiality is clear to most people. Data integrity, on the other hand, is still subject to much discussion. "Still" because the term integrity has been subject of discussion for almost two decades and with still no uniform definition on integrity; neither in the computer security community nor in the legal field.

This paper will look at the various understandings of the term integrity from the time it was introduced by computer scientists. It will research the different definitions and

how these have been adopted by lawyers. One problem that will arise is that no legislator has ever defined the term data integrity. As article 7a, sub b of the Data Retention Directive states that there are consequences to not ensuring the integrity of the communication data, it is important for internet en telecom providers to know the legal meaning of integrity, in order to secure their systems. Further, this paper will examine what legislators have meant by using the word integrity. Finally, it will discuss and provide some legal elements that could or should be part of a definition of integrity.

2. Early discussions about a definition on integrity

The term data integrity was first used during the nineteen seventies in the Glossary For Computer Systems Security (FIPS39), which was published by the National Bureau of Standards.[i] It defined data integrity as

"The state that exists when computerised data is the same in the source documents and has not been exposed to accidental or malicious alteration or destruction."

At that time this definition seemed sufficient to use as security principle. In the nineteen eighties the US Department of Defence published the so called "Orange Book" which describes mechanisms which should be implemented in computer systems to meet its military security policies.[ii] The security mechanisms were derived from the three security principles, availability, confidentiality and integrity, which are still used today for designing security measures for computer systems. As the capabilities of computer systems grew and the systems were used more often for commercial purposes it appeared that the security standards described in the Orange Book did not meet the standards that were needed to secure commercial computer systems.[iii] Also the consensus grew that the FIPS39 definition on integrity was inadequate for security measures in commercial computer systems. It had grown to narrow and the requirements and policies used to implement integrity in computer systems had been subject to a lot of dispute. As a consequence, integrity was more and more used to mean many different things.[iv] To come to a consensus on integrity the National Institute of Standards and Technology of the US Department of Commerce organised the invitational workshop on data integrity in 1989.[v] Despite the

great interest from the computer security field, a consensus on a definition of data integrity was not reached.[vi] In the early nineties Sandhu presented a paper on data integrity at the Workshop on Database Security.[vii] Again it was noticed that there still was no consensus on what was meant by integrity. After the appearance of Sandhu's article it remained silent and it seemed as if the different views on integrity were no longer an issue to the computer security community.

3. Integrity definitions in the technical field

As already mentioned in chapter 2, there are different views on integrity (including data integrity) in the technical field. A few of these have been developed for the NIST Workshop, others can be found in other (most technical) literature. In this chapter we will describe and discuss the definitions that have been used most often in the technical field.

3.1 The Clark and Wilson definition on integrity

The first definition was developed by Clark and Wilson, who defined data integrity as:

"Those qualities which give data and systems both internal consistency and a good correspondence to real world expectations for the systems and data."[viii]

A few things can be said about this definition. Firstly, this definition is applicable to both systems and data and therefore widely applicable. Secondly, to define systems and data as integer they have to meet "real world expectations". In this respect, expectations must be understood as that "systems and data remain predictably constant and that change is only allowed in highly controlled and structured ways".[ix] Thirdly, the question is what can be understood by "good correspondence"? There are many opinions (maybe as many as humans?) about what is good or not. The problem is that good is not objectified and therefore the definition can be interpreted in different ways by different people. Fourthly, it is the question what must be understood by qualities. Clark and Wilson do not provide comments on qualities and it remains unclear what is really meant with qualities.

3.2 The Courtney and Ware definition on integrity

A second definition, has known some of the same problems as the Clark and Wilson definition, is from Courtney and Ware, who made a strawman definition for the NIST Workshop. It defines integrity as:

"The property that data, an information process, computer equipment, and/or software, people, etc. or any collection of these entities, meet an a priori expectation of quality that is satisfactory and adequate in some specific circumstance. The attributes of quality can be general in nature and implied by the context of a discussion; or specific and in terms of some intended usage or application."[x]

This definition leaves us with some issues. In the first place it should be recognised that this definition introduces two variables, namely expectation and (data) quality, which considered in their mutual relation make that data is integer or not. Because of this mutual relation, integrity is considered not to be absolute, but relative. The data can only be considered integer, when the data quality comes up to one's expectations of the data quality. If the quality falls short of the expectations of that quality, the data is considered not to be integer. That leaves us with the question whether data is integer or not when the data quality exceeds the expectation of that quality. The definition states "meet an a priori" and as a conclusion one could say that this excludes exceeding the expectations. However, Courtney and Ware probably intended to cover exceeding expectations by the term "meets an a priori". For now, we will assume that in the case that quality exceeds the expectations, the data can be considered integer. Secondly, the definition is not limited to data, but is also applicable to physical objects and processes (and even behaviour). It is therefore widely applicable. In the third place, it deliberately leaves open the definition of quality, which makes this definition and open ended definition. Fourthly, the "attributes of quality" in this definition, could consist of variables that require proactive steps (like timelines) to maintain this (data) quality.[xi] As a consequence of not taking these proactive steps, it is possible that data integrity can decrease when the data is not altered, because one is sitting still. Fifth and last, we will mention the term expectations. Expectations in this definition differ from the expectations in the Clark and Wilson definition. The Courtney and Ware definition uses the term expectations in a more current way. Expectations must be understood as the thoughts one has about

something (in this case data quality) before knowing it. The problem here is that expectations are highly subjective and therefore may differ for different persons. Expectations may differ for several reasons, such as experience built by people, technical progression, changes in regulation and many other reasons. Whose expectations need to be taken into account? If one has very high expectations, these expectations may never meet the data quality and the data can thus never be considered integer. Do expectations therefore need to be reasonable? That leaves us with the question what expectations one could reasonably have? If person X had higher expectations than person Y, it is possible that data is integer for person Y and not for person X. Data integrity then becomes a matter of one's personal view.

In our opinion, both the Clark and Wilson and the Courtney and Ware definitions are not useful to describe integrity for both the technical and legal field, because they lack objectivity, are not sufficiently absolute and far too open-ended.

3.3 The authorisation definition on integrity

The third definition is the so-called (un)authorised modification definition. This definition relates to the mechanisms due to Biba and is most used in the technical field.[xii] Integrity is defined as:

The state of data when it has not been modified without authorisation.[xiii]

This definition is much less subjective than the previously discussed definitions. What can be described as authorised and unauthorised can be formulated and there are technical mechanisms available that reduce the risk of unauthorised modifications.[xiv] On the other hand, this definition is so narrow that it leaves no space? for specific situations with specific circumstances. For example, person X, though he is not authorised, gets to work on the account of his colleague Y. During this session he changes incorrect data into correct data. In that case, person X was not authorised to modify data, but he modified incorrect data into correct data. On the other hand, if person X works on his own system for which he has been authorised and he changes data from being correct to incorrect, then is it said that the data is not integer. The question needs to be whether the authorised modification definition is the proper definition to describe integrity. In our opinion, this definition can be useful for

designing technical mechanisms which preserve data security, but as will be discussed in the chapters 4 and 5 of this article, it is less useful in the legal field.

3.4 The improper definition on integrity (by Sandhu)

A fourth definition is proposed by Sandhu, who defines integrity:

"as being concerned with the improper modification of information and data".[xv]

This definition leaves us with an open norm namely the term "improper". Sandhu says that he deliberately uses the term improper instead of the term unauthorised, because it acknowledges that security breeches can and do occur without authorisation violations.[xvi] Sandhu also refers to the meaning of improper that has been given by Clarck and Wilson who say that "no user of the system, EVEN IF AUTHORISED, may be permitted to modify data items in such a way that assets or accounting records of the company are lost or corrupted.[xvii] "Malicious mischief by authorised users is therefore also covered by the term improper".[xviii] As we will later discuss in paragraph 5.2, the improper modification can be very attractive in the legal field because of its open norm.

4. Integrity definitions in the legal field

Now, let us move our attention from the technical field to the legal field. During the nineteen seventies and eighties, when technical progression in computation and informatics gave rise to new possibilities (among which criminal or at least undesirable non-criminal possibilities), legislators started to develop new legislation to prevent and criminalize computational crimes. As the technical field had already developed criteria on which mechanisms that guaranteed the security of computer systems should be based, many legislators used these same criteria (availability, integrity and confidentiality) to develop legislation. What legislators did not take into account was the fact that these so called "Orange Book criteria" were no more than security concepts and not security mechanisms. The concepts were all very abstract and were only meant to be used for designing technical mechanisms. Where technicians focused on designing these technical mechanisms, legislators seemed to be afraid (or at least did not dare) to focus on specific legal measures. Instead of

describing specific measures HOW to guarantee integrity, the focus was on prescribing THAT integrity had to be guaranteed.

So let us have a look at how integrity has been used in legislation and what is meant by integrity. Integrity has been used by different legislators and as we will see its meaning has some different nuances. In this paper we will not focus on country specific legislation, but only legislation that has been used by the European legislator. We will look at integrity as described in the Convention on Cybercrime, integrity in the so called Data Retention Directive and integrity as described in Regulation (EG) No 460/2004 that establishes a European agency for network and information security.

4.1 The Convention on Cybercrime

First let us have a look at the Convention on Cybercrime (the Convention) which has been drafted by the Council of Europe. The term integrity is not explicitly mentioned in the Convention itself, but the explanatory report recognises data integrity as a interest that needs legal protection.[xix] The Convention prescribes in article 4, sub 1 that

"each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right".[xx]

It obligates countries to establish as a criminal offence the "damaging, deletion, deterioration, alteration or suppression" of computer data when committed intentionally and without right. The following elements can be subtracted:

1. damaging, deletion, deterioration, alteration, suppression;
2. intentionally;
3. without right.

4.2 The Data Retention Directive

Secondly we will have a look at the so called Data Retention Directive that has been approved last December by the European Parliament.[xxi] In former proposals it was article 6, sub e of the Data Retention Directive which prescribed that member states of the European Union should establish legal remedies (in line with provision of Chapter II of Directive 95/46/EC) for providers that did not ensure the confidentiality and integrity of data. We found it very interesting that the former proposals did not define integrity, especially because of the several technical definitions that were used and because of the legal consequences for providers (such as administrative penalties and civil liability).[xxii] It was not very clear what providers had to guarantee with respect to the integrity of data. In the final draft of the proposal (after amending) the word integrity was deleted from the document and another article (article 7a) was added to it.[xxiii] Article 7a, sub b of the Data Retention Directive requires that

"Each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with the present Directive the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, or accidental loss or alteration, unauthorised or unlawful storage, processing, access or disclosure."

This Directive obligates member states of the EU to make sure that providers shall implement organisational and technical measures that secure data against integrity and confidentiality infringements. These measures have to guarantee protection against "accidental or unlawful destruction or accidental loss or alteration, unauthorised or unlawful storage, processing, access or disclosure". The following elements with respect to integrity have to be taken into account:

1. accidental or unlawful destruction
2. accidental loss or alteration

4.3 EU Regulation No 460/2004

Thirdly, we will mention Regulation (EG) No 460/2004 that establishes a European agency for network and information security.[xxiv] In this document, article 4, sub f of the Regulation defines data integrity as:

"the confirmation that data which has been sent, received, or stored are complete and unchanged."

The following elements can be subtracted:

1. a confirmation
2. data which has been sent, received, or stored
3. complete and unchanged

5. An analysis of three legal integrity definitions

Before analysing the above definitions on integrity, a distinction has to be made clear. This is the distinction between the elements of a definition on integrity itself, the elements of the circumstances in which a breach of integrity exist and the element of the circumstances in which a breach of integrity has legal consequences (for civil or criminal law). In several definitions this distinction is not made clear and as a consequence elements which are only used in definitions which criminalize a breach of integrity are mixed with elements that only affect the definition on integrity. A second remark has to be made about the nature of the integrity definitions. Integrity is a state data is in when some things are not done to the data. Integrity is therefore often described in negative terms (as in NOT touched, UNdamaged, NOT violated). Having recognised the elements of the three above described (somewhat different) definitions, we will now compare each of the elements.

5.1 The modification element

First we will look at the modification element. The Convention on Cybercrime uses the terms damaging, deletion, deterioration, alteration an suppression. The explanatory report says that damaging and deterioration relate to "a negative

alteration" of the integrity of data and programmes, whereas alteration means "the modification of existing data".[xxv] It does not make explicit a definition on alteration. Does alteration only include changes in data or also the complete removal or addition of data? In this particular definition on integrity this question is partially circumvented by explicitly using the term deletion. But does the alteration of data encompass additions to/of data? (if adding data must also be understood by alteration of data). As already said, the definition in the Convention already uses the term deletion for the complete removal of data. Deletion is meant to be "the equivalent of the destruction of a corporeal thing. It destroys them and makes them unrecognisable".[xxvi]

The same remarks can be made with regard to the Data Retention Directive. It uses both "destruction" and "alteration" of data, but not adding data to existing data. Or does the alteration of data also include adding data to existing data? If the answer is yes, then why does the Directive separate the terms destruction and the alteration? Does this mean that the alteration of data does not include the destruction of data? Or was it meant not to include the addition of data at all in this definition?

Thirdly let us look at the EU Regulation. Integrity has to do with "complete and unchanged" data. Though formulated in different words than those of the Convention and the Data Retention Directive, the same remarks are applicable to this definition. The word "complete" could be understood as no (parts of) data missing. It means that no data is deleted, removed, deleted or erased in any way and that the existing data is the same as the original data. The word unchanged could mean that no data has been altered. The question we already asked ourselves with respect to the Convention and the Directive is also applicable to the EU Regulation: does "unchanged" also encompass the addition of data?

5.2 The qualifying element

The elements that are often used in integrity definitions are related to weighting the wrong- or rightness of the modification or excusing some kind of modifications. These elements were not introduced when lawyers started to use the term integrity, but when technicians started to discuss a definition on integrity. In particular the Sandhu definition, which uses the improper modification definition. The main distinction that technicians and lawyers have made is how inappropriateness or some

legal wrong or right has to be constructed in a definition on integrity. First let us have a look at how Sandhu and the proponents of the authorisation definition construct a definition on data integrity. In this kind of definitions, the improper or the authorised element is enclosed in the integrity definition. One can only speak of data integrity when the data has been modified properly or authorized and one can only speak of affected data integrity when the data has been modified improperly or unauthorised. As a consequence, there are modifications that do not affect integrity. These are the proper and the authorised modifications. Contrary to computer scientists, the Convention on Cybercrime and the explanatory report separate the modification element and the "without right" element.[xxvii] In this definition, integrity can be seen as the state data is in when there have been no modifications at all.

The Data Retention Directive on the other hand does something quite different. It splits up the different kinds of modifications (destruction, alteration and loss) and combines these with different elements. If data integrity must be understood as "the accidental or unlawful destruction and the accidental loos or alteration" , the Data Retention Directive gave an entirely different dimension to the term integrity, because it refines the term integrity in a whole new way.

Though it defines integrity the EU Regulation No. 460/2004 uses no terms that refer to any kind of wrong-/rightness. This supports our conclusion that integrity should be understood in a very restrictive way.

5.3 Intentionally or accidentally

Looking at the three definitions given in chapter 5, we think it is noteworthy the Convention uses the word intentionally, that the Data Retention Directive uses the word accidental and that the EU Regulation does not use any of these words. Looking at the purpose of the Convention, the goal is to criminalize integrity infringements. Because we deal with criminal law, it is not strange that the element of intention is used. The question is whether the element of intention is part of a definition on integrity. We do not think it is part of a definition on integrity and feel supported by the fact that legislators use words like intentionally, accidentally or none of these two in different definitions.

Looking at the Data Retention Directive, we do not feel it is remarkable that the element of “accidental” is used. However, we do think it is remarkable that providers need to implement data security principles that protect the accidental and unlawful destruction of data and not the accidental AND UNLAWFUL loss or alteration of data, but only the accidental loss or alteration of data. Can we therefore conclude that providers do not have to protect data against malicious alterations that are intended?

Again, the EU Regulation does not require any form of intention of accident, which is not surprising. As the Regulation only defines integrity and does not define integrity breeches or legal consequences to integrity breeches, we agree that any form of intention or accident is not part of a definition on integrity.

The use of these different elements for different situations in which integrity is an issue only confirms our proposition that the definition on integrity needs to be very restrictive and objective (see chapter 7) and that any form of intention or accident does not include a definition on integrity.

6. Consequences of different definitions on integrity

First we think it should be recognised explicitly that different legal definitions on integrity do not have to be a problem. If the legal scope in the various regulations differ, it is possible there will not be conflicting regulation.

So let us get back to the situation internet and telecom providers find themselves in. Providers are obligated to secure date against integrity infringements by these different regulations. If different regulations with different integrity definitions are applicable, it will not be very clear which security mechanisms should be used. What are the consequences for providers who find themselves confronted with this legislation? Due to the EU legislation and legislation from the Council of Europe, providers are and will be more and more confronted to secure their own data and data of their clients against integrity infringements. And if they do not, it is most likely that they will face legal consequences. The question is what providers should secure by securing data integrity and how they should do that. First, providers need to understand what integrity means. As we hope to have made clear, it is not very clear

what is meant by data integrity. Firstly, it is not clear what is meant by alteration or modification. As deterioration, deletion and destruction are explicitly mentioned, can one reasonably conclude that this means that addition of data to existing date is not included in alteration or modification? Or does it mean the opposite? Does it mean that alteration and modification include the addition of data? If the answer is yes, this could have consequences for the mechanisms that providers use to secure the principle of integrity. Providers than should also protect data against the addition of data into existing data. Secondly, it is not always clear if the modification or deletion (destruction) which has to be prevented or is criminalized, should be accidental, intentional or unlawful. Because of this, providers find themselves in an insecure situation.

7. Some legal elements of integrity

For the future, we think it would be good to think about how integrity, the affection of integrity and the legal consequences of the affection of integrity should be defined. In our opinion, a legal integrity definition should be very restrictive and as little subjective as possible. A very restrictive definition would be “the state data is in when there have been no modifications”, whereas modifications must be understood as any deletion or alteration of existing data and every addition of new data to existing data. By using words as “no modification” and “any deletion, addition or alteration”, the definition on integrity becomes more objective, because integrity is then considered to be binary: the state of data is either integer or it is not.

As a consequence of the definition on integrity, the affection of integrity can be understood as: “every modification to existing data”. Note that these definition do not say anything about authorised, improper, illegal, against the law or purposely. In our opinion these elements should be prohibited for laws that link consequences to affecting integrity.

Acknowledgements:

This article has been written as part of the virtual bridges project in which computer scientists and lawyers work on a framework on agentsystems.
Anja Oskamp, Frances Brazier, Martine Boonk, David de Groot, Maarten van Stekelenburg

---

[i] Glossary For Computer Systems Security, FIPS PUB 39, National Bureau of Standards, June 1974

[ii] Department of Defense, Trusted Computer System Evaluation Criteria, CSC-STD-011-83, Department of Defense Computer Security Center, Fort Meade, MD, August 1983

[iii] D.D. Clarck and D.R. Wilson, "A Comparison of Commercial and Military Computer Security Policies", 1987, <http://www.facweb.iitkgp.ernet.in/~shamik/spring2005/i&ss/papers/a%20comparison%20of%20commercial%20and%20military%20security%20policiesClarkWilson87.pdf>

[iv] Z.G. Ruthberg and W.T. Polk, "Report of the Invitational Workshop on Data Integrity." Procedure of the Invitational Workshop on Data egrity (Ruthberg, Z.G. and Pol, W.T., editors), National Institute of Standards and Technology, Special Publication 500-168, September 1989, page 2-1

[v] Z.G. Ruthberg and W.T. Polk, "Report of the Invitational Workshop on Data Integrity." Procedure of the Invitational Workshop on Data egrity (Ruthberg, Z.G. and Pol, W.T., editors), National Institute of Standards and Technology, Special Publication 500-168, September 1989, pages 1-1 – 1-3

[vi] Z.G. Ruthberg and W.T. Polk, "Report of the Invitational Workshop on Data Integrity." Procedure of the Invitational Workshop on Data egrity (Ruthberg, Z.G. and Pol, W.T., editors), National Institute of Standards and Technology, Special Publication 500-168, September 1989, page 2-6

[vii] R.S. Sandhu, On Five Definitions of Data Integrity, Procedure of the IFIP WG11.3, Lake Guntersville, Alabama, 1993

[viii] D.D. Clarck and D.R. Wilson, "A Comparison of Commercial and Military Computer Security Policies, 1987, <http://www.facweb.iitkgp.ernet.in/~shamik/spring2005/i&ss/papers/a%20comparison%20of%20commercial%20and%20military%20security%20policiesClarkWilson87.pdf>

[ix] D.D. Clarck and D.R. Wilson, "Evolution of a Model for Computer Integrity, Procedure of the Invitational Workshop on Data egrity (Ruthberg, Z.G. and Pol, W.T., editors), National Institute of Standards and Technology, Special Publication 500-168, September 1989, page A.2-2

[x] R.H. Courtney and W. Ware, "Some Informal Comments about Integrity and the Integrity Workshop", Procedure of the Invitational Workshop on Data Integrity (Ruthberg, Z.G. and Pol, W.T., editors), National Institute of Standards and Technology, Special Publication 500-168, September 1989, page A.1-6

[xi] R.S. Sandhu, On Five Definitions of Data Integrity, Procedure of the IFIP WG11.3, Lake Guntersville, Alabama, 1993

[xii] Biba describes integrity as the prevention of information flow from low-integrity objects to high-integrity objects. ITSEC describes integrity as: "prevention of the unauthorised modification of information" See also: C.P. Pfleeger and S.L. Pfleeger, Security in Computing, Third Edition, Prentice Hall PTR, 2002, page 5 and 6.

[xiii] Information Technology Security Evaluation Criteria (ITSEC), ECSC-EEC-EAEC, Brussels, June 1991

[xiv] C.P. Pfleeger, Security in Computing – International Edition, Prentice Hall PTR, 1997

[xv] R.S. Sandhu and S. Jajodia, Integrity Mechanisms in Database Management Systems, page 617,< http://www.acsa-admin.org/secshelf/book001/27.pdf>

[xvi] R.S. Sandhu and S. Jajodia, Integrity Mechanisms in Database Management Systems, page 618< http://www.acsa-admin.org/secshelf/book001/27.pdf>

[xvii] R.S. Sandhu and S. Jajodia, Integrity Mechanisms in Database Management Systems, page 618< http://www.acsa-admin.org/secshelf/book001/27.pdf>; See also: D.D. Clarck and D.R. Wilson, "A

Comparison of Commercial and Military Computer Security Policies, 1987, <http://www.facweb.iitkgp.ernet.in/~shamik/spring2005/i&ss/papers/a%20comparison%20of%20commercial%20and%20military%20security%20policiesClarkWilson87.pdf>

[xviii] Sandhu, R.S., On Five Definitions of data Integrity, Proc. Of the IFIP WG11.3, Lake Guntersville, Alabama, 1993

[xix] "Convention on Cybercrime – Explanatory Report", Council of Europe, ETS No. 185

[xx] "Convention on Cybercrime", Council of Europe

[xxi] The retention of data processed in connection with the provisions of public electronic communication services and amending Directive 2002/58/EC

[xxii] See article 7a of the Data Retention Directive in conjunction with article 23 and 28 95/46/EC.

[xxiii] "Proposal for a Directive of the European Parliament and of the Council of the retention of data processed in connection with the provisions of public electronic communication services and amending Directive 2002/58/EC - Outcome of the European Parliament's first reading (Strasbourg, 12 to 15 December 2005), Council of the European Union, Interinstitutional File 2005/0182 (COD), 19 december 2005

[xxiv] the Regulation (EG) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.

[xxv] "Convention on Cybercrime – Explanatory Report", Council of Europe, ETS No. 185, paragraph 60

[xxvi] "Convention on Cybercrime – Explanatory Report", Council of Europe, ETS No. 185, paragraph 60

[xxvii] Paragraph 62 says: "The above acts are only punishable if committed "without right""