Regulating Information Security: A Matter of Principle?

Andreas Mitrakas · Silvia Portesi

European Network and Information Security Agency (ENISA)
{andreas.mitrakas | silvia.portesi}@enisa.europa.eu

Abstract

The widespread use of information technology in daily transactions has exacerbated the role of information security to protect information assets. Regulating network and information security has taken place through instruments and instantiations used for most of the time for different purposes than those strictly needed by information security itself. If information security is the answer to such requirements as confidentiality, integrity and availability of resources, setting up appropriate regulation is the means to set up binding frameworks. Regulation in this respect takes into account the requirements for a soft law approach that encompasses self regulatory frameworks and standards. A set of regulatory principles addressing the content and form of regulation in network and information security is an additional means to further enhance the impact of legislation and serve stakeholders.

1 Introduction

The widespread use of information technology in daily transactions has exacerbated the role of information security to protect information assets. The potential vulnerabilities that have been typically associated with transactions in the Public Administration and private enterprise challenge users and legislators alike. While information security is the answer to such requirements as confidentiality, integrity and availability of resources, establishing appropriate policies is the means to set up binding bilateral frameworks [Pfle00]. Furthermore a regulatory framework underpins certain high level requirements that need to be addressed at legislative level and complements the bilateral arrangements of individual users. Further up stream, there is, however, a latent need of principles of information security in order to guide the regulatory process. This paper addresses such questions as *is there a real need to regulate network and information security*, *under what conditions can it be taken up by the legislator* and *is law is an appropriate means to address regultary principles in information security?* Input to this paper has been drawn from the working group on regulatory aspects of network and information security that ENISA set up in 2006. The remainder of this paper addresses the following areas: an overview of regulatory principles in the light of legal positivism and their influence in the regulatory process of network and information security; specific regulatory considerations for network and information security; a set of regulatory principles that can be leveraged upon to the benefit of more concrete regulation in network and information security.

2 Working with rules

Positivism has vouched that law is a set of rules used to determine which behaviour will be punished and which will be coerced by the public power. If a specific case is not covered under this assertion, then a specialist, like a judge intervenes to determine the case. A legal right or obligation must directly

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2007), 3-17

fall under a legal rule [Dwor77]. Austin described three types of rules, legal, moral and religious ones. A basic set of legal rules is provided by the sovereign who, subsequently, empowers a judge to make new rules or re-assert known ones [Aust1832]. For H.L.A. Hart there is a system of primary and secondary rules whereby primary rules define what is allowed and what is not [Hart61]. Secondary rules affect the operation of primary rules and address three discreet areas namely, the uncertainty about what law is and whether a rule is valid, the rigidity of rules which addresses rules of change and allows laws to be varied, and how to resolve legal disputes from which rules of adjudication emerge. For Hart a legal system is the union of primary and secondary rules.

According to Dworkin, beyond set rules imposed by a designated authority, in a democracy, rules also include policies and social standards that are promulgated through various channels associated with social functions. A policy sets out a standard to improve a certain feature of the society [Dwor77]. Standards in this sense should not be interpreted as technical standards that will be discussed separately further down in this paper, but rather as social norms that cut across the society. Principles on the other hand set out a social standard that is a requirement of justice, fairness, or morality. As Dworkin argues, positivism is a model of and for a system of rules that forces us to miss the important role of social standards that are not rules. Principles are rules that conflict and interact with each other so that each principle that is relevant to a particular problem and it provides a reason arguing in favour of but without necessarily stipulating a particular solution thereto [Dwor77]. Empowering a judge requires exercising discretion, which can be asserted when someone is charged of making decision as part of social standards set by an authority.

Long before any explicit manufacturer's liability rules came about, a New Jersey (US) Court, in the case *Henningsen v. Bloomýeld Motors Inc.* (32 NJ 358, 1961), was faced with an important question of whether and to what extend a car manufacturer may limit its liability for a defective car. The manufacturer in question has set a contract clause signed to by the buyer which said that the manufacturer's liability for defects was limited to "making good" defective parts while "this warranty was in lieu of all other warranties, obligations and liabilities." Faced with a defective product the plaintiff argued that in his case additional expenses should be covered for by the manufacturer due to the defective product that he made available. At the time there was no statute to point to that would allow the plaintiff to support his argument. The Court in its reasoning took into account limitations in the principle of contractual freedom and it suggested that "in a society like ours where the automobile is a common and necessary adjunct of daily life, and where its use is so fraught with danger to the driver, passenger and the public, the manufacturer is under special obligation in connection with the construction promotion and sale of his car". Subsequently the Court refused to be taken as an instrument of inequity that is there to enforce a "bargain" in which one party takes advantage of the economic necessities of the other.

In *Henningsen,* the guidance of the Court was provided not so much from an established and firm background of rules, but rather from a set of social norms or standards that suggest that a Court cannot be used as an instrument to promote unfairness; except in case of fraud and wilful misconduct contractual freedom can be indeed limited to match social needs of the society. In the absence of a set of rules, exercising discretion provided the appropriate interpretation of a social standard and injected input in case law. Luhmann argues that the essence of positive law is that it is a decision; and to that the concept of positive law can be reduced to. A decision entails that law is not only promulgated through decision, but also is valid by the power of decision which subjects it to change [Luhm95]. In an environment where business needs prevail, adapting law enables it to be a powerful instrument for the wilful promotion and regulation of social and economic goals. Luckily, by virtue of an EU regulatory framework for information society services, we do not have to rely on assumptions such as those posed in *Henningsen* any more.

Setting up meta-rules on how to carry our regulation in those areas related to network and information security that has been deemed necessary, we observe the significant role that technical standardisation, for instance, plays in bringing together legal requirements with specific societal needs. Standardisation has emerged as a key EU policy area that complements the legislative process especially in such areas as products and technology. Standardisation policy in the EU goes back to the *Cassis de Dijon* case in which the European Court of Justice ruled that a product meeting the requirements of one member state should be legally made available in another; allowing the emergence of mutual recognition of technical standards as a matter of significant interest in the EU internal market (ECJ 120/78 of 20/02/79). The EU approach to technical harmonisation has resulted in limiting standards to technical specifications and safety requirements while reserving a prominent place for EU standards organisations such as the European Committee for Standardisation (CEN) and European Telecommunications Standards Institute (ETSI). This role for standards has gradually led to a soft approach that contains covers up for limitations emanating from a strict legislative process that can be seen as too narrow to address business and society needs. Technical standards, thus, provide a layer of "soft law" that deviates from a strict legislative approach [Send05] [Send04]. Often technical standards rely on a framework set out through a directive that is complemented by the appropriate standards. These standards are typically promulgated by the industry. The figure below provides an outlook of frequently used soft law instruments and their association with legislative instruments as they are often encountered in an EU context. A co-regulatory process links the requirements at the legislative level with the outcome of the standardization process that remains in line with the stipulations of the legislative framework.

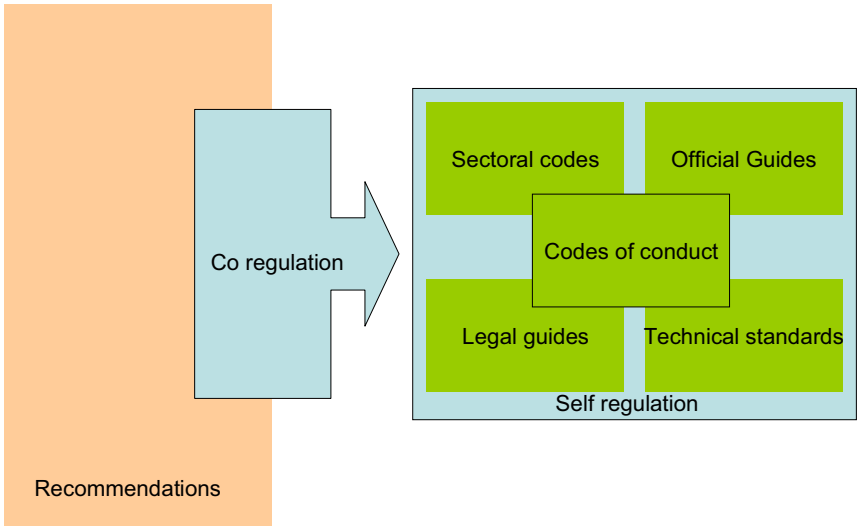

Figure 1: Soft law instruments in a co-regulation approach

In a concrete situation related to network and information security we observe that Directive 1999/93/EC on a Community framework on electronic signatures, standards establishes a presumption of conformity, meaning that the electronic signature products that meet their requirements also comply with the legal requirements [Mitr06]. This approach has been underlined by the Commission Decision of 14 July 2003 on the publication of reference numbers of generally recognized standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council. This Decision has endorsed and given legal effect to certain standards promulgated by the industry-led European Electronic Signatures Standardization Initiative (EESSI). Standards assume legal

significance in cases where the law mandates them in order to give specific effect to a particular regulation within the EU.

With regard to security standards the ISO 27000 family of standards provides recommendations on information security management to those who are designated to initiate, implement or maintain security in an organization. This standard provides a common basis to pursue security management practices and indirectly to provide confidence in transactions. The ISO 27000 family of standards invokes the general requirement for network and information security and more specifically the requirements for confidentiality, integrity and availability. Integrity in this case encompasses the notions of authentication and non repudiation, which have both been subjected to legislation especially through the electronic signatures directive. The ISO 27000 standard is a self regulatory framework that extends to policies and agreements that all aim at setting up the conditions for network security safeguards within an organisation or in specific transaction frameworks [Mitr07]. The instrument of recommendation can be further used at EU level in order to highlight the significance and role of such standards but also of other instruments such as codes of conduct [Send05].

3 Making rules

Starting from mid-1990s, the technological revolution, characterised by the development and spread of information technologies, has reshaped the material basis of the society. “Economies throughout the world have become globally interdependent, introducing a new form of relationship between economy, state and society, in a system of variable geometry” [Cast04]. Adequate regulatory solutions, at national and supranational level, to face these changes, started to be discussed and adopted. In making rules in network and information society, some regulatory principles are followed. Sometimes, however there could be noted a discrepancy between the desired solution and the one made available by the legislator. Inefficient legislation might have further sipped in and influenced bilateral relationships, leading to regulatory solutions that could be a far cry from what was essentially needed in the first place, when regulation was deemed to be an appropriate solution. Especially at the level of regulatory principles a necessary condition to consider regards the efficiency of the offered solution.

The Coarse theorem gives a notion of what efficiency means when making an agreement. Referring to bilateral relationships, Coarse suggests that a contractual solution must take into account three factors: transaction costs, the efficiency of the outcome and the legal framework to lead to a regulatory solution [Poli89]. The efficiency of a regulatory solution, such as a contract for example also depends upon factors such as the social context, the transaction costs and the legal reality of the environment in which the legal solution is applied [Will05]. A regulatory solution should take such variables into account and include for example the cost of obtaining information, the negotiation cost, the gains of breaching a rule as opposed to possible costs like a reliance remedy or a restitution remedy, etc. If, for example, the cost of obtaining information in order to set up a regulatory framework is quite high such solution might not necessarily be a rational choice [Will05]. Determining the cost of obtaining information on the overall solution is yet another facet of the problem that cannot be easily reached.

There is an additional role, reserved to economic rules, which produces outcomes that are in the interest of everyone [Mitn80]. Economic rules aim at correcting market inefficiencies or failures which is an often appearing feature in a society. In a broad sense, regulation in this regard might include technical and consumer related standards, health and environment standards, competition policies, industry regulations etc [Hix99].

Rules provide incentives and set the limits of human interaction and behaviour with regard to an area of interest. Against this background rules that regard services can be seen as comprising of three general discreet categories being moral, social and economic ones. Economic rules, in specific, focus on these very incentives, in order to establish a system of fines that invokes the approach that recklessness is punished or compliance is rewarded. The flip side of these rules with an economic interest encompasses the concept of using a system of credits that it pays to educate and raise awareness in specific areas of interest. This paper suggests that general rules can be used to enhance the current level of security available to the beneficiaries of the information society as a whole in a way that enhances information society services. There is but limited need for specific formal rules as it is addressed further below. Rules can be based on the three main categories that are mentioned above, being moral, social and economic ones, in order to provide a framework for authorities, users and service providers alike in their efforts to make available or rely upon dependable and robust services that appropriately mitigate network and information security risks.

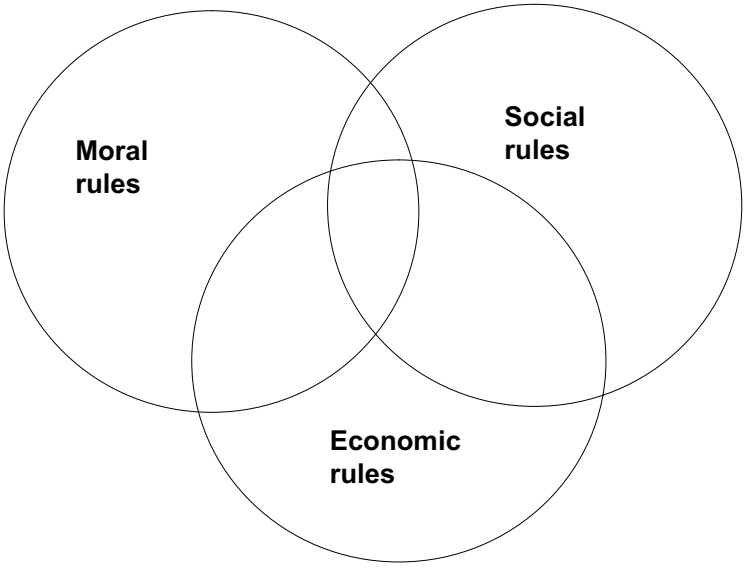

Figure 2: Three types of rules: moral, social and economic

When answering the question "what rules have to do with network and information security?" it is important to highlight the features of the Internet, upon which information society services are largely based in making the most of a secure service and transaction environment. A discreet case that related to information security concerns identity risks in information society that can be epitomised in the motto published along a synonymous cartoon in NY Times on suggesting that "*On the internet nobody knows that you are a dog*", as authored by Peter Steiner who wrote it in his July 1993 cartoon in NY Times. It is questionable whether the age old question regarding social responsibility, which goes: "*could a man resist the temptation of evil if he knew that his acts could not be witnessed*" could be successfully replied in the information age; apparently the reply at least in the real world appears to be 89% of the time [Boas61] [Levitt06]. The shift to avatars made available through the services of Second Life, Second Life is a 3-D virtual world entirely built and owned by its residents demonstrates the significance of this underlying identity drive in information society (http://secondlife.com/). An avatar is an Internet user's own representation in the form of a three-dimensional model used in computer games. Avatars facilitate the need to take up a role, marking or altogether one's real identity and the Internet is a means that predominantly facilitates this need. Avatars can be deemed as an expression of an underlying social desire

to act under an assumed identity that allows the user to authenticate itself in a virtual world. However desirable this approach can barely resemble reality and in a real life context it cannot be morally or socially justified as it would undermine trust. Therefore addressing authentication methods to ensure trust in user access or management for example becomes a priority area for information security.

Readjusting our focus on security, however, the relentless exposure of services, service providers and users to network and information society risks has made it an indispensable feature of information society to rely upon rules in order to ensure the confidentiality, integrity and availability of services. What are these rules that have already become available? Are there any principles that could be leveraged upon in order to ensure that acts and omissions do not necessarily leave services out in the cold?

This paper further examines the role of information security as a component of information society.

4 Information security: to serve and protect?

When examining the role of rules in network and information security it is important to highlight the potential role of rules in addressing the requirements of the information security community. This task becomes more apparent if taking a practical case regarding the protection of personal data and the role of its regulatory framework in Europe. The scope of information security measures in information society can be twofold. On one hand information security aims at protecting the interests of the service provider with regard to access the resources, which are necessary in order to deliver a service [FoBa01]. Security, however, can be used in order to ensure the protection of rights, such as privacy, in a way that the end user benefits. End user in this respect might be a natural person in its capacity as citizen or consumer etc. Additionally, legal persons can benefit in terms of legal safety, compliance with regulations in highly regulated environments such as stock markets and the like. Personal data protection is this emblematic area where all stakeholders are better off if they protect data rather that ignore it. To the data controller personal data is an asset that can be leveraged upon in order to deliver meaningful services; as such the data controller has a duty to protect this asset [Ters06]. To the data subjects, on the other hand personal data represents a means to receive personalised services that requires protection due to its vicinity to the personal sphere of the protection of fundamental rights.

This heightened significance of rules in the area of personal data protection emanates from the strong cultural and legislative drive in the early seventies' Western Europe that led to the gradual adoption of data protection legislation. The European Union considered the global reach of certain aspects of data protection law that has led to the currently available European framework on data protection [Buel06].

When examining the needs in terms of rules of network and information society it is important to envisage the potential objectives that these rules might seek to play. Pursuant to the assumption regarding the protection of personal data it is clear that rules of any sort, in network and information security, serve the dual purpose of protecting fundamental rights and ensuring services rendered. Therefore there is a strong societal drive that powers rule making as well as a strong economic drive that sets out a framework of incentives and fines in case of breach as discussed in the previous section. An underlying strong moral element might remain a little out of sight because it might be embedded in the societal requirement that is manifested through legislation at the Member States level. Such moral element associates, however rather with the moral premise of the right "to be left alone", the core element of privacy, rather with the specific mechanics of how such an arrangement might work out in terms of protecting personal data. As the basic requirement on privacy stated in article 8 of the Council of Europe Convention on Human Rights and Fundamental Freedoms and then in articles 7 and 8 of the Charter of Fundamental

Rights of the European Union, has also been enshrined in legislation such as Directive 95/46/EC etc., the associations among the moral and societal elements become apparent.

5 What's law got to do with it?

An emerging legal framework that derives from the role that information plays in modern day transactions is setting up the pace for developments in business and banking. Organizations that implement appropriate security measures mandated by industry regulations or legislation expect to benefit from the mitigation of potential liability of shareholders, employees, customers, trading partners or other third parties involved in a transaction.

The set up of the European Network and Information Security Agency (ENISA) to address selected network and information security matters has emerged as a new element in supporting the approximation of laws in the Member States in the framework of the First Pillar regarding the EU Internal market. To this effect the decision of the European Court of Justice asserted that the principle of article 95 of the Treaty regarding the EU Internal Market is well served just by setting up a measure such as ENISA along with the array of legislative measures undertaken by the European Union over time.

The ENISA case (C-217/04), UK v. EP & Council presents an example of challenging the legal basis of EU Agency based on article 95 of the Treaty on the EU Internal Market. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (hereinafter, ENISA Regulation) has been challenged before the European Court of Justice (hereinafter, ECJ) with regard to the legal basis of ENISA servicing EU Internal Market purposes on the basis of article 95 of the Treaty (ex art. 100a). While art. 95, maintains the system of majority voting it involves co-decision between Council and parliament under art. 251 of the Treaty. It has been noted that this approach results in greater intermediary powers to the Commission at the Council level since gaining a qualified majority suffices for a vote [Weil91]. In its ruling ECJ affirmed that the ENISA Regulation was yet another measure in a broader EU framework regarding network and information security. Being far from the only measure regarding the approximation of laws, as the plaintiff had claimed, the ENISA Regulation has been part of a broader set of regulatory measures composed by the framework Directive and including specific Directives that address various aspects of the EU Internal Market in the area of electronic communications. The ECJ decision highlighted the potential divergence in Member State laws that could emanate from differences in transposing Directives in this area. The ECJ ruling also removed uncertainty by linking article 3 of the ENISA Regulation (EC) 460/2004 with the objectives of the framework Directive as well as of specific Directives in the area of network and information security.

Additional requirements associated with the area of specific activity that regulation is called in to serve also influence the way that regulation is promulgated. For example the need for the end user to become aware of risks and measures to mitigate them or the need for security measures to facilitate or at least to refrain from hindering interoperability can be seen as measures of specific interest that could typically sip in regulation. The table below makes some associations between areas of network and network security and types of rules, such as the above.

Table 1: *Ad hoc* substance areas and their relation to types of rules

	Ad hoc sample substance				
	Data protection	Privacy	Awareness	Interoperability	Information society Application
Social rules	X	X	X	X	X
Moral rules		X	X		
Economic rules	X	X		X	X

The table above is a plain indication of the associations that certain *ad hoc* sample substance areas might have with the rules of choice that can be used as regulatory instrument in a network and information security framework. Essentially this table demonstrates that not all areas of interest or instruments available in network and information security merit or require being associated with a need to have formal rules with an economic impact. As discussed above these rules with an economic impact are essential formal rules promulgated by the legislator. Inevitably on several occasions a regulation can rest at the level of bilateral arrangements in the framework of self regulation as a reflection of a moral requirement or a social constraint imposed in the transaction. While moral or social constraints address the needs of portions of the society they might not have a universal interest or create a grand impact that merits the attention of the legislator. In this regard self regulation may produce results that are sufficiently efficient and therefore more desirable.

6 A Working Group

The ENISA Working Group on Regulatory Aspects of network information security (hereinafter, WG-RANIS) carried out an overview of EU legislation as it has become available in the area of network and information security (http://www.enisa.europa.eu/pages/ENISA_Working_group_RANIS.htm). The target of this Working Group has been to compile a list of activities in an effort to represent state-of-art in an inventory-centric approach that addresses legal actions on issues relevant to network and information security.

In their report this Working Group came up with a significant number of legislative instruments (over 65 in total) that cover the period as of 1990. In total more that 65 instruments were collected that cover a broad range of EU policy and law making [RANIS06]. The areas of legislative attention with an interest for network and information security cover for example: security and financial services, intellectual property rights, corporate and IT governance, data authentication, data protection and retention, electronic communications, networks and services. This very broad approach that has yet to be systematically addressed had been spared no legislative instruments in order to meet the regulatory requirements of network and information security. In this regard regulations, directives, recommendations, resolutions etc., had all been invariably used in to promulgate the legislative framework of network and information security. The instruments of choice to give effect to this framework can be seen in the radar table below that was compiled by the Working Group itself [RANIS06]:

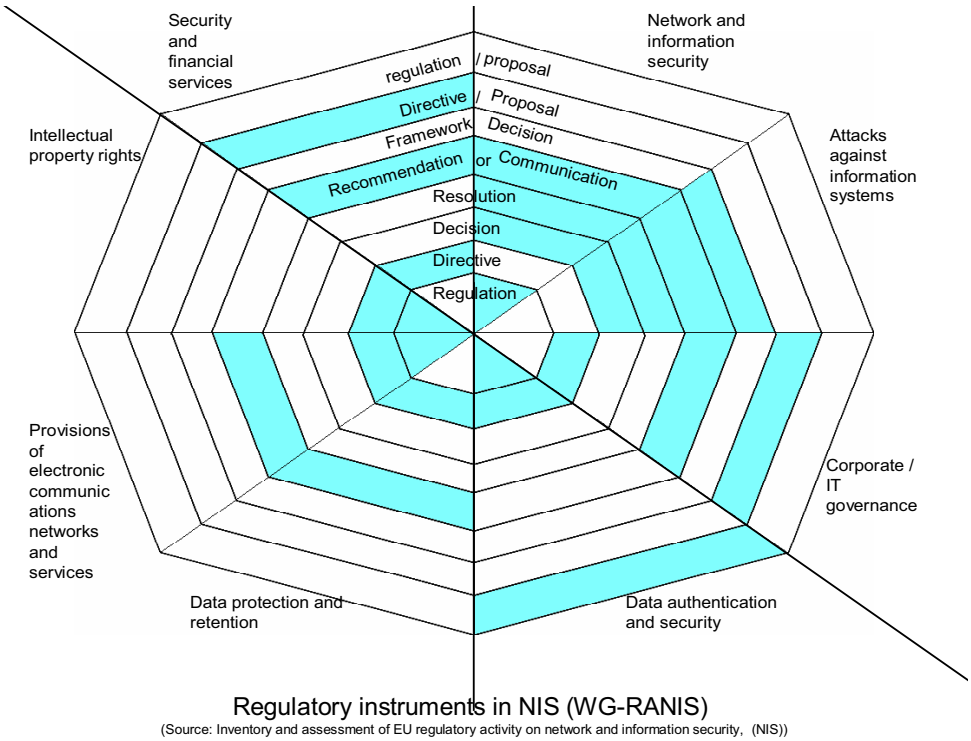

Figure 3: Regulatory instruments in network and information security

7 Regulatory Principles

A set of underlying principles is necessary to guide legislation towards efficient regulation that is commensurate with societal needs. Such legislation should recognise lateral societal needs that are not necessarily represented in legislation itself but which are, nevertheless represented in the form of standards or bilateral arrangements. The principles that WG-RANIS has seen as looming can be found in the report itself. The section below relies on some of these principles, and provides an overview and explanation regarding the regulatory framework at large.

Multi facet legislation

The network and information security regulatory framework is typically multi faceted comprising of several layers, such as privacy, telecommunication, business applications, authentication and identity, intellectual property protection, competition, taxation and electronic communication emerge as interest areas for network and information security. Therefore, as Matsuura points out, there are several substantive categories of law applying to information and network security, such as intellectual property law, privacy law, law of contracts and commercial transactions, consumer protection law, anti-trust law, property law, etc. [Mats02]. Interlacing the underlying legislative principles of various areas can be challenging for the legislator of network and information security who risks voting potentially conflicting rules. Hence, sufficient consideration could be given to legislation of lateral areas in a way that adapts new legislation to the existing framework.