European Commission

JRC TECHNICAL REPORTS

# Governance of ICT Security: A Perspective from the JRC

*Technical document annexed to the presentation given to BEPA-EGE hearing of 19/03/2013*

*Angela Guimarães Pereira*
*and Mariachiara Tallacchini*

2014

Report EUR 26631 EN

Joint
Research
Centre

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen
Contact information
Mariachiara Tallacchini
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 361, 21027 Ispra (VA), Italy
E-mail: mariachiara.tallacchini@jrc.ec.europa.eu
Tel.: +39 0332 78 9746

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

This publication is a Technical Report by the Joint Research Centre of the European Commission.

Legal Notice
This publication is a Technical Report by the Joint Research Centre, the European Commission’s in-house science service.
It aims to provide evidence-based scientific support to the European policy-making process. The scientific output expressed does not imply a policy position of the European Commission.Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication.

JRC90033
EUR 26631 EN

ISBN 978-92-79-37967-3
ISSN 1831-9424

doi:10.2788/72624

Luxembourg: Publications Office of the European Union, 2014

Printed in Italy

# Table of contents

# 1 ICT ethics: from Opinion 26 to Opinion 28

Information and communication technologies (ICT) are enabling unforeseen capabilities in all aspect of our lives. They are reframing how we think, learn, work, play, and interact at personal, social, and political level. While these technologies are essential for society and for today's information economy, several aspects of their applications remain un-reflected and open to surprises.

For the first time in Opinion 26 (2012) the EGE has extended its analysis to ICT, identifying and addressing some key-problems in ICT ethics, as well as looking at the ethical implications of different ICT applications, new fields of research, and future developments. Opinion 28 will specifically deal with security and surveillance technologies, a domain where the ICT normative issues are even more problematic, due to the ethical, legal, and political ambiguities affecting these concepts and their histories.

The reflections proposed here below touch on some general normative issues concerning ICT implications, and discuss a few key elements in the construction of a framework for their governance, especially in the fields of security and surveillance.

## 1.1 Technological and normative co-produced complexities in ICT governance: a loop of powers-and-limits, rights-and-constraints

In the past decades, several fields of ethics have been described as radical paradigm shifts instead of new sectors of applied ethics. This has been the case for bioethics, environmental ethics, and also ICT ethics. Without entering into a discussion on the (widely unexplored) relations and legacies between life sciences and ICT ethics – it cannot be denied that ICT display some special features. [1]

As “enabling technologies” which apply to, and interact with, all other technological fields, not only do ICT introduce, or deepen certain ethical concerns (e.g. privacy issues already existing may be amplified through ICT); they are also radically reframing numerous techno-scientific fields (e.g. Internet of Things (IoT) transforming the energy or transport sectors, communication systems acting in place of banking activities, online consent and patient enrollment modifying research ethics, genetic research becoming genetic social networks, etc…). Moreover, ICT oblige us to re-think the relationships between individual and collective lives: while creating unprecedented forms of empowerment for users, they introduce new limitations and obligations. Their deployment generates, both factually and normatively, a loop of powers-and-limits, rights-and-constraints.

Scholarly work, especially in Science & Technology Studies (STS), [2] has shown that science and technology cannot be separated from the normative context where they are imagined,

[1] Curvelo, Guimarães Pereira, Tallacchini, Rizza, Ghezzi, Vesnic-Alujevic, Breitteger, Boucher 2014.
[2] See Hackett, Amsterdamska, Lynch, Wajcman 2007.

constructed, and developed. This inextricably interdependency between techno-scientific and regulatory dimensions has been referred to as “co-production.”[3]

These intertwined “loops” are relevant to ICT governance. In Opinion 26 the EGE has primarily focused on individual rights and their protection (e.g. privacy and identity), and has consequently strengthened individuals’ ethical and legal centrality. In addressing the ethical aspects of security and surveillance – where public authorities are the main actors and where surveillance measures directly impact on fundamental rights— the EGE will presumably have to provide guidance on how and when some constraints and controls for those same rights are legitimate.

Even though these seemingly opposing dimensions may be harmonized and become complementary, a delicate balance between rights and constraints/ obligations, at the individual as well as at the collective level is needed.

When limiting rights in the name of security – in democratic, under the rule of the law, societies – specific information and warrants should be provided: which authorities are entitled to proceed, the alleged reasons for these limitations, the modalities of their implementation. This commitment towards a whole series of rights of access, right to know, and transparent action is even more relevant when normative decisions are physically embodied (and black-boxed) in technology designs (e.g. programs and devices).

## 1.2 Legitimizing security and surveillance: the European vision

Security and surveillance have been traditionally connected to discourses of politics and power, and to the need for sovereign States to legitimize their decisions – and their unique privilege to invoke “states of exception”[4] –, even when these are suspending or limiting citizens’ rights in the name of security.

This is why security and surveillance pose delicate ethical issues – and, according to some scholarly work, the very existence of an “ethics of security” may be questioned.[5] Even in the more delimited ICT domain similar controversial issues exist about the ethical foundation of security.

Contemporary critical studies in security and surveillance (CSS), especially in the European area,[6] have deeply scrutinized the rhetoric of invoking security to limit rights, and the potential for abuses in times of renewed terrorism threats (e.g. after 9/11). In fact, since the construction of the metaphor of social contract to build modern societies and national States, security has been proposed as a fundamental element of the social contract itself, and in some cases the main reason for being part of it. Tacitly assumed as a necessity, security has

[3] The concept of co-production comes from the field of Science and Technology Studies (STS). Though introduced by Bruno Latour in 1993, the term is associated with Sheila Jasanoff ‘s wide investigation of the links between science, law, and politics, and the ways they reciprocally influence and shape their knowledge, languages, values (see Jasanoff 2012).

[4] Agamben 2006.

[5] Burke 2007.

[6] Leading to the emergence of distinctive European research agenda(s) in the traditionally US-dominated field of ‘security studies.’ For a comprehensive analysis of the developments of the security field see CASE 2006.

become a “metaphysical discourse,” a word rhetorically evoked as self-legitimizing, especially in periods of terroristic attack fears.[7]

CSS propose a vision primarily centered on human beings as individuals, by reconsidering the idea of sovereignty, the state of exception, and in general by separating what should be kept and what should be rejected about the security discourse. CSS make explicit the largely statist and military-oriented assumptions of traditional security studies in order to open the field to greater theoretical scrutiny and debate; and suggest to replace this state-centered understanding of security with a project that would have human emancipation as its central concern. From this perspective the connection “security–power–normality is replaced by security–emancipation–normativity, with emancipation disentangling security from power and achieving a fuller and more inclusive realization of security.” [8]

This “humanistic turn” of the assumptions lying behind security and surveillance has been endorsed by international organizations. After the UN launched in 1994 [9] and re-proposed in 2012 [10] the concept of “human security,” namely that security should focus on making human beings, and not sovereign States, more secure, security issues have been increasingly centered on individuals’ and communities’ well-being as criteria for legitimization.

The centrality of human beings and their rights is strongly informing the overall European ethical and legal vision, and is declaredly at the core of the European policies in the field of cyber- and ICT-security. [11] In the EU vision, security, including cyber- and ICT security, [12] is grounded, to be legitimate, in the European fundamental rights and values. This means, as recently stated by the EC vice-President Neelie Kroes, that the same European values should be promoted when you're walking down the street, and when you're online. [13]

However, in the cyber domain, the word security has been interpreted in two different ways: the technical definition of cyber-security that is used within the scientific and technical community; and the national security definition belonging to the political environment. According to the former meaning of security, referred to ICT systems, security is primarily focused on individual systems and networks, and has its roots in computer science and engineering communities; according to the latter, security focuses on collective and institutional systems, reflecting the influence of political and national security actors. [14]

[7] Burke 2007.

[8] CASE Collective 2006.

[9] UNDP 1994.

[10] UN General Assembly, Follow-up to Paragraph 143 on human security of the 2005 World Summit Outcome, 25 October 2012.

[11] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, Brussels, 7.2.2013.

[12] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union Proposal for a Directive on Cybersecurity, COM(2013) 48 final 2013/0027 (COD), Brussels, 7.2.2013.

[13] Kroes 2013.

[14] Porcedda 2012.

What is relevant here is that these two different meanings make reference to heterogeneous sets of values, but are also connected to different policy and technology outcomes, namely prevention or punishment. The technical community interprets security as integrity, confidentiality, authenticity, non-repudiation, and availability of the service,[15] and assumes that, by ensuring both at individual and Internet Service Provider's (ISP) level the necessary measures to protect privacy, security is highly ensured as well. As a consequence, rights protection and security always proceed hand in hand. In general, there is a wide agreement that security of communication is part of human security, and is necessary for freedom, for human dignity, and for consent of the governed. Moreover, according to some authors, ICT security should be designed with the principle of securing "the blessings of freedom for posterity" in mind. [16]

The national security community, instead, focuses on collective existential harms that need to be securitized, and proposes punishment and extended surveillance. Here, "(p)rivacy and data protection cannot be seen as a complement to security, but simply as an obstacle to achieving control." [17]

The EU security strategy – encompassing cybercrime, terrorism, public transport protection, and natural disasters – is based "based on common values including the rule of law and respect for fundamental rights as laid down in the EU Charter of Fundamental Rights. Solidarity must characterise our approach to crisis management. Our counter terrorism policies should be proportionate to the scale of the challenges and focus on preventing future attacks." All these action should be taken while respecting "the privacy of individuals and their fundamental right to protection of personal data." [18] Similar provisions are established in the field of cybersecurity, that "can only be sound and effective if it is based on fundamental rights and freedoms (…) and EU core values;" and "(r)eciprocally, individuals' rights cannot be secured without safe networks and systems". Access for all, democratic and efficient multi-stakeholder governance, and shared responsibility to ensure security are further elements of this normative landscape.[19]

[15] These qualities are considered as security primitives. Authenticity provides the ability for receiver of a message to ascertain the origin of the message. Confidentiality implies the ability for a message to be exchanged without eavesdropping. Integrity is the ability for receiver of a message to verify that the message has not been modified in transit. Non-repudiation ensures that a sender cannot falsely deny later that he sent a message. Availability is the ability to deliver the service.

[16] Landau 2010.

[17] Ibidem, 45.

[18] Communication from the Commission to the European Parliament and the Council, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, COM(2010) 673 final, Brussels, 22.11.2010.

[19] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final, 2013/0027 (COD), Brussels, 7.2.2013. Article 3 defines security as Art.3: "the ability of a network and information system to resist, at a given level of confidence, accident or malicious action that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data or the related services offered by or accessible via that network and information system…"

Studies in the field have shown that the two separate meanings (and ends) are increasingly blurred, namely that there is a trend towards a "securitisation of cybersecurity." [20] Even though a balance between rights and obligations is always needed, in weighing security and rights, there is a tendency "to restrict rights for the sake of security, instead of reconciling the two." [21]

In fact, as systems are made more secure at some level (e.g. use of ICT in passports), the threshold of security shifts to a deeper level (e.g. the documents needed in order to obtain a passport). As a weaker level can be always identified, security is never enough and becomes a totalizing issue. "How much security is secure enough?" is an ethical question with no easy answer.

This trend seems to apply also to the EU rights-centered vision, where the boundaries between the security of civil life and needs – usually identified in critical infrastructures such as those related to energy, transport, banking, financial market infrastructures, and the health sector – that should be prioritized over the military, appear sometime blurred (for instance, when dealing with border security, migration, etc.).

It has to be recognized, however, that these ambiguities are also an outcome of the inextricable loops connecting previously distinct topics and areas. [22] Not only "a concept of internal security cannot exist without an external dimension, since internal security increasingly depends to a large extent on external security;" [23] but ICT systems are critical infrastructures connected to all other infrastructures, with interdependent cyber and physical networks. [24]

Surveillance, even more than security, is traditionally linked to the images of power and control. In fact surveillance has never represented just a mean for security, but it has been framed as an end in itself. Bentham and Foucault's image of the Panopticon colonised the

[20] In the US, the integrated cyber-security policy refers to a "strategy, policy and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure" (The White House, President's Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, 2009, p.12).

[21] Porcedda 2012.

[22] This can be seen, for instance, in the field of cybercrime. This is described as "a term of hype and not a legal definition" (Brenner and Koops 2006) as it encompasses domains formerly distinguished, and now with blurred boundaries. A distinction is made between two broad categories: a) the security of ICT systems, including: personal security, computer security, network security, national security, digital identification and authorisation, tracking network traffic across borders and jurisdictions, data protection, intellectual property right protection on digital media; from b) safety to people, including: the protection of children using the internet and mobile cell-phones; family/school/ community/responsibilities; paedophilia; cyber-bulling; digital dossier recording details of an individual's life; addiction to online games; suicide and self-harm websites" (Porcedda 2012).

[23] European Council. Draft Internal Security Strategy for the European Union: Towards a European Security Model. 5842/2/10, Brussels, 23 February 2010, p.16.

[24] Communication from the Commission. Green Paper on a European Program for Critical Infrastructure Protection. COM (2005) 576 final, 17 November 2005, p.20.

modern imaginary for surveillance: subjects are reduced to objects as they are forced to internalize the gaze of the power and to self-discipline their conducts. [25]

The ubiquitous presence of electronic eyes in contemporary societies has ambiguously changed this gaze. While the Panopticon's "big single gaze" has faded away, a kaleidoscope of massive, distributed, and inexpensive technological "eyes," from sensors to mobiles to drones, [26] has colonized sparse, interconnected fragments of personal and social lives. Public and private spaces cannot be sharply separated any more, but have become engrained as part of a continuum. [27]

Moreover, surveillance is no longer just visual. The metaphor for "eyes" applies in reality to a variety of devices to store all kind of information; again, in a continuum from the external environment to the internal genetic make-up.

Finally, the privatization of surveillance that can be individually and reciprocally performed in increasingly unnoticeable ways is radically transforming the issue of the legitimate uses of these technologies. Together with sovereign States, corporations, groups, and individuals can now intrude in all aspects of life. All these unleashed powers need to rethought on order to assess and balance them, to harmonize them with fundamental rights, and to ground them in more robust forms of democratic legitimacy.

# 2 A few reflections on ICT ethics and governance

These preliminary considerations about the loops generated by mixing the technological and normative

ICT dimensions are necessary to introduce some specific reflections on ICT governance, and on security and surveillance ICT.

A first remark concerns the specific roles for ethics in the ICT domain, dominated, at least in Europe, by legal instruments. In most field of emerged and emerging technologies (e.g. biotechnology, nanotechnology, and synthetic biology), ethics has played a strong normative role, by normalizing new techno-scientific applications, allowing the legislative process not to be rushed, and by representing citizens' values. Ethics has become an influential form of "soft law" – though having being officially framed as policy advice – complementing legally binding tools. [28]

In the ICT field, however, for a long time normative issues have been primarily identified with privacy and data protection; and legislation has quite promptly and widely taken care of these concerns by building a comprehensive legal framework (though composed of both hard and soft laws). Only more recently other relevant normative issues have become apparent,

[25] Foucault 1975.

[26] See, for instance, Do-It-Yourself Drones, http://diydrones.com/ , and http://www.meetup.com/DC-Area-Drone-User-Group/, defined as "a group for amateur and professional drone users committed to promoting the use of flying robots for recreational, humanitarian, and artistic purposes" (Accessed 13 May 2013).

[27] See, for instance, the European Court of Human Rights case *Peck V. United Kingdom* (2003) 36 E.H.R.R. 41.

[28] Tallacchini 2009.

and specific roles for ethics, especially in rapidly developing sectors (such as IoT), can be envisaged.

These roles deal with the need for a commitment towards human agency and for integration between the technical and human dimensions. This integration is briefly exemplified in the following paragraphs through the issues of securing trust, ethics-by-design, ethics-in-design, and participatory surveillance.

Also, the importance of well-established ethical principles in the field of research, especially security research, has to be outlined.

Notwithstanding the essential role that dedicated institutional bodies on ethics (such as the EGE) should play, ICT dynamic developments may require that other ethical spaces are opened up as well. As a matter of fact, the very concept of “in garage” scientific and social practices, namely DIY (Do-It-Yourself) communities engaging in science, technology, and ethics in non-institutional contexts, though recently associated to synthetic biology, was started and has a long standing tradition in IT.

Due to how the ICT contexts are constantly expanding and changing, “research communities” and “communities of citizen scientists”, as places for research, may be relevant in perceiving and conveying new ethical challenges and emerging values. This means, for instance, that there is the need to collect groups and communities experiences and continued reflexive work in the field in order to establish shared conducts, practices, values. These bottom-up forms of normativity should be connected both with a broad public dialogue, and reflections coming from institutions.

Forms of invited and self-organized public engagement should be supported as ways to overcome the limits of a just “defensive” vision of privacy. While citizens become more skilled about technoscience and knowledge production, the formation, development, and application of crowd-sourced, collectively generated, knowledge is changing the ways we think about knowing and learning.[29]

People are increasingly eager to reinterpret what counts as their privacy in order to participate in jointly created “augmented intelligence” for the benefit of society (as several experiences in the field of genetic research show); [30] and they are becoming ready to create new forms of trusted relationships with institutions and corporations with shared benefits and powers.

All these topics illustrate the rise of new needs and claims for potential rights and new obligation, their meanings and limits as well as their weighing. Building new digital relationships with institutions and corporations, for instance, require also new principles about knowledge and powers. For instance, the “right to be forgotten,” [31] that has been

[29] Nielsen 2012.

[30] Tallacchini 2013.

[31] Article 17 of the proposed Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (25.1.2012 provides the data subject's right to be forgotten and to erasure. It further elaborates on Article 12(b) of Directive

established for individuals, cannot be applied to institutions and corporations. Instead, according to the principles of "institutional ethics,"[32] a "duty to be remembered" should be introduced for these entities to be accountable and trusted: they should remain always traceable as to their past activities (including past websites), histories, controversies.

## 2.1 Ethics in governance: a commitment towards cultivating human agency and moral skills

As said, not only through ICT are our private lives and identities reframed, but most human skills – our ways of thinking, speaking, writing, and acting – are increasingly reshaped and informed by technologies and their architectures as well.

This implies that, together with privacy and identity, another concept should be considered: human agency. ICT governance seems to require an ethical commitment towards human agency – *Vita activa*, according to Hannah Arendt's tradition.[33] This means to raise awareness about the potential tendency towards passive acceptance of mechanical acting, and not to reduce all normative issues to technical fixes. In other words, there is a need to prevent human agents from behaving just as "actants" (term that may apply to mechanical entities, such as robots' acts), namely as causal forces instead of intentional, responsible subjects.

Human agency – as the capacity for human beings to act as subjects instead of deterministic mechanisms — should become part of an active commitment in ICT governance: the commitment towards a full concept of humanness and towards moral development as an essential (and endangered) human skill.

This challenge of the potential mechanization of human actions (and moral acts) and a related "duty to preserve human acting" represent ethical features almost unique to ICT governance.

In fact, the daily substitution of human-mediated relations with ICT-mediated forms of life to, as well as the transfer of most life aspects and decisions to ICT devices, can give rise to a situation where these automatic, invisible mechanisms hinder and impair the specific skills for moral experience, perception, and learning. Similarly to how the predominant and pervasive use of hand-typing is leading to a loss of handwriting ability,[34] scholarly research is increasingly revealing that the deprivation of real life experiences and the prolonged exposure to virtual life are gradually de-sensitizing people to moral aspects of human relations (doing harm, non-respect, insensitivity to vulnerability) and making them unable to connect and integrate their virtual and non-virtual lives.[35] Several examples of this diminished awareness exist: situations where individuals intervene in emergency situations not by helping the human beings involved, but by taking pictures of the scene; the risks that war attacks performed with drones can be perceived just as virtual games; the diminished

95/46/EC and provides the conditions of the right to be forgotten. As known, in 2008 the European Court of Human Rights applied this rights in *S. and Marper v. the United Kingdom* - 30562/04, Judgment 4.12.2008.

[32] See, for instance, Ariansen 2003.

[33] Arendt 1998 (1958).

[34] See http://www.cbsnews.com/2100-201_162-626663.html (Accessed 10 May 2013).

[35] Pagallo 2012; Hildebrandt and Rouvroy 2011.

protection for research subjects enrolled on the web; cyber-bulling as a lack of perception of (and respect for) vulnerability in online life.

In the IoT domain, the challenges to human acting become even more extreme. IoT opens towards futures of seamless hybridized interactions between human beings, their extended ICT-mediated capabilities, and smart and dynamic objects displaying emerging unplanned behaviors. Agents and actants' acts join towards unintended, unforeseen and unexpected outcomes.

In Opinion 26, EGE already noticed that "(t)echnical solutions should not violate an older person's dignity and it is critical that ICT serves to augment, rather than replace, human interaction" (p.41). However, not only the relevance of maintaining human relationships alive, but more in general the need and the duty to nurture human agency have to become part of ICT governance.

## 2.2 Integrating the human and the technical dimensions

Human agency is relevant also in framing and balancing different regulatory instruments for ICT governance. In framing the tools to implement security and rights protection, there is the need to integrate, complement, and balance technical approaches with human action, awareness, and understanding. In fact, an increasing number of ICT solutions to (ICT-related) ethical and legal problems have become available.

However, the need to warrant a space for agency within increasingly mechanistic and deterministic contexts is not just an ethical requirement. This need also depends on the stronger effectiveness of integration – as opposed to substitution – and interaction between the human and technological dimensions.

An example is the idea of relying completely on ICT security systems, and thus of "securing trust." "Securing trust" is a paradoxical idea: securing trust implies "replacing trust with security." [36] But the complete mechanization of deeply rooted cognitive and emotional skills, besides being difficult, was also shown as a weaker solution than that of combining technology and human action. What can be done, alternatively, is "nourishing trust," namely to cultivate "digital trust," by integrating *ad hoc* security devices and algorithms with traditional forms of human trust. Merging technical solutions (such as by-design measures, certifications and self-certifications, institutional and corporate digital memories) with trust-generating human behaviors (direct repeated experiences, consistent institutional and/or corporate behavior, prolonged relationships and reliability, available information and reputation, etc...) can lead to "more robustly" trusted digital relationships – together with more education and the development of new psychological skills specific to the digital world.

In analyzing ICT approaches (such as privacy-by-design) to fostering data protection, the European Data Protection Supervisor (EDPS) suggested that these mechanisms would be implemented in the legal framework on privacy together with two non-ICT measures (i.e.

[36] Nissenbaum 2004.

accountability and notification of data breach) in order to make them more effective. [37] Both measures have been included in the privacy legal framework. Accountability requires data controllers to demonstrate that they have put in place the mechanisms necessary to comply with applicable data protection legislation; data breach notification, namely any breach leading to the destruction, loss, disclosure, etc… of personal data, provides a strong feedback about the reliability of a given service.

Both measures help making the ICT security mechanism more reliable by providing information about the actors involved and their duty to report the potential negative outcomes of the implementation. What is relevant here is that both measures require more traditional forms of human trust (though digitally revisited). Automatic forms of protection can still be strengthened by human-related forms of trust (e.g. privacy seals).

This case aims to show that ICT governance should encompass a mixture of technological and normative approaches, by integrating and complementing human(ness) skills, specific ICT education and learning (digital human behavior), and technological fixes. An integration of human and technological dimensions in the governance of ICT is not only more legitimate (ethically and democratically), but it may also prove more effective.

## 2.3 "By-design" ethics and rights: wired-in normativity

"Technologies," as Lawrence Lessig has pointed out, "can undermine norms and laws; they can also support them." [38] A variety of technological measures have been proposed and/or already implemented to automatically – which would imply more effectively – protect individual rights and security (such as privacy-by-design). Broadly speaking, these techno-legal approaches are defined as "ethics-by-design," "rights-by design," [39] "ambient law." [40] By-design normativity consists of mechanisms "embedded within the entire life cycle of the technology, from the very early design stage, right through to their ultimate deployment, use and ultimate disposal." [41] The idea is to integrate normativity into information and communication systems and solutions. Privacy-by-Design (PbD), for instance, can be implemented through elimination or reduction of personal data, or prevention of unnecessary and/or undesired processing. It may consist in offering tools to enhance individuals' control over their personal data; and it can be incorporated in the architecture of information and communication systems.

The European Data Protection Supervisor (EDPS) has strongly supported the by-design approach [42] and the reasons for this endorsement depend on the enhanced power that by-design tools seem possess in implementing the law. If traditional legal instruments "are

[37] EDPS 2010, 19-20.

[38] Lessig 2006 (1999), 124.

[39] Porcedda 2012.

[40] Hildebrandt and Rouvroy 2011.

[41] EDPS 2010, 2.

[42] See also Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee, Security Industrial Policy Action Plan for an innovative and competitive Security Industry, COM(2012) 417 final, Brussels, 26.7.2012.

helpful towards the *promotion* of privacy by design, in practice they have not been sufficient in *ensuring* that privacy is embedded in ICT." [43]

EDPS has referred to PbD both in normative and technical terms. PbD has been defined as a "general, binding principle" that has to be included into the data protection legal framework; and also as a technical architecture and design incorporated "in particular ICT areas."

Therefore, ethics and law by-design can be understood not just as technical solutions, but as specific normative orientations and "regulatory principles" in themselves: namely, the principle of providing default protection to internet users/citizens – it may be recalled that the right to privacy, in Europe, is a human right, while in the US it represents a consumer right.

In a similar way, the Article 29 Working Party asked for PbD to be made compulsory in the area of freedom, security and justice, "where public authorities are the main actors and where measures increasing surveillance directly impact on the fundamental rights to privacy and data protection." [44]

By-design forms of protection are effective tools for reducing individual users' burden in dealing with ICT and as an institutional commitment to limiting public power through built-in trust. However, the perspective of complete replacement of norms and rules with technology should be cautiously considered in the governance of ICT both for ethical and pragmatic reasons.

On the one hand, enhancing awareness is part of keeping human agency alive. There is a need to increase knowledge and attention about how technology and normativity co-generate each other, and to open up co-produced loops to transform them into sites for transparent deliberations. Also, as privacy is a complex concept dealing not only with different aspects of human personality, but also with a variety of individual, collective, and cultural sensibilities, mechanisms for PbD are (and will become) more numerous and diverse.

On the other hand, the proper functioning of by-design tools cannot be separated from establishing and implementing certain related rights, and enabling people to use them.

Technological neutrality, namely the idea that regulation "neither imposes nor discriminates in favour of the use of a particular type of technology," [45] represents a European (and widely internationally shared) commitment. As a consequence, network providers have chosen to inform users and enable them to consent or not (e.g. to receiving cookies) through browser settings and privacy policies. However, even though privacy policies explain how to opt-out from certain procedures, only a minority of users is informed and knows how opt-out mechanisms actually work. In this respect, EDPS has recommended that, if by-design

[43] Ibidem, 7.

[44] Art.29 WP 2009.

[45] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), Whereas (18): "The requirement for Member States to ensure that national regulatory authorities take the utmost account of the desirability of making regulation technologically neutral, that is to say that it neither imposes nor discriminates in favour of the use of a particular type of technology."

mechanisms will be increasingly in place, the EU institutions and national authorities should invest in educating citizens about the threats posed by social networking websites.

Rights to adequate, complete, and simple information – as it happens for informed consent in other fields – are waiting to be implemented.

Technological neutrality cannot amount to ethical and legal neutrality. This means, for instance, that by-default protection systems should be preferred to opt-out systems; proper accounts should be provided of the reasons for users to accept invasive procedures; by-design tools should be accompanied with adequate descriptions of the specific aspects of privacy that are granted. Track-Me-Not (TMN), [46] for instance, generates random search to create noise around the actual search performed by users, but does not hide their IP addresses; also, TMN can have undesirable side effects, as its random searches can include sexual matters (which already has been the cause for several complaints).[47]

## 2.4 "In-design" ethics and rights: architecture matters

In listing the essentials for an "Internet compact," in 2011 Commissioner Kroes recalled that "architecture matters," referring to how the Internet structures do not only have ethical and policy impacts, but are based on certain values and choices. Therefore, she added, in discussing the "future Internet" there is the need "to have a broad, structured and coherent debate, with the Internet policy and research communities, on the impact of architectural change." [48]

However, the need for open and thorough discussion goes even further – representing a matter of democratic legitimacy involving citizens' rights – if normative decisions are pervading the design of all ICT.

We tend to think of ethical and legal norms as intentional decisions we make about how to act. However, ICT involve also a different kind of ruling as they embody rules and decisions in their own designs and structures.

The widespread modern "prejudice" about the separation between facts and values has been, amongst other things, a major intellectual obstacle to timely recognition and intervention on the values embedded in ICT. The idea that machines and programs can embody values is not new. Already in 1980, in "Do Artifacts have Politics?," Langdon Winner noticed that all machines, structures and technical systems should not only be analyzed from the perspective of their efficiency and productivity, but also "for the ways in which they can embody specific forms of power and authority." [49]

[46] In 2011 the US Senate passed the "Do-Not-Track Online Act", http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=85b45cce-63b3-4241-99f1-0bc57c5c1cff (Accessed 14 May 2013).

[47] Nissenbaum 2011.

[48] Kroes 2011.

[49] Winner 1980.

These early observations (that have led to a number of developments in ICT, e.g. to make them more "human-centered"), [50] have raised awareness about the choices implicitly black-boxed (and hidden) in programs and devices. As Winner has pointed out, "a great latitude of choice exists when a particular instrument, system, or technique is introduced. Because choices tend to become strongly fixed in material equipment...the same careful attention one would give to the rules, roles, and relationships of politics must also be given to such things…" [51]

Now, these normative decisions should be made explicit, transparent, discussed, and controllable, from designers and engineers, to institutions, and citizens.

"(A)rchitectural regulation operates surreptitiously and may not even be perceived as governmental action. Architectural regulation thus allows government to shape our actions without our perceiving that our experience has been deliberately shaped, engendering a loss of moral agency." [52]

Ethics "in-design" has to be distinguished from ethics-by-design, even though they complement each other. If "by-design" approaches explicitly aim to create built-in algorithms for law enforcement, "ethics in design" raises awareness about the processes through which values and norms become embedded in technological architectures. While ethics-by-design looks at how to technically transform values and rights into algorithms, ethics-in-design looks at the normativity of structural choices to make it apparent and transparent.

Ethics-in-design is relevant in several domains, especially when institutions and citizens interact, ranging from how information is delivered to how laws are implemented. It has been noticed, for instance, that if governments want to embrace a politics of transparency through the Internet, they should reduce their active role in presenting and selecting information. "Today, government bodies consider their own Web sites to be a higher priority than technical infrastructures that open up their data for others to use." However, it "would be preferable for government to understand providing reusable data, rather than providing Web sites, as the core of their online publishing responsibility." [53]

Also, the details of legal implementation can be crucial when encrypted in programs or artifacts, and this is particularly delicate in relation to security and surveillance. The "supposedly technical" decision to trace either a document or a person in a security or surveillance program should be disclosed to citizens, who have a right to be informed about the implementation procedures. For instance, while the Schengen written regulation established that information should be stored "exclusively on stolen, misappropriated, lost

[50] In the mid-1990s the movement for Human Centered Computing (HCC) was started to design machines with a focus on humans, their capabilities, their preferences their environment.

[51] Winner 1980, 29. Landau (2010) has pointed out that in-design choices, once made, tend to last beyond their reason to exist. For instance, keyboards were built so that the most commonly used letters in English the metal keys do not hit each other; but they have survived in computer keyboards.
keyboards were built so that the most commonly used letters in English the metal keys do not hit each other.

[52] Tien 2005, 2.

[53] Robinson, Yu, Zeller, and Felten 2009, 159.

and invalidated documents,” [54] the software actual implementation does not “exclusively” trace stolen documents, but also the person who was victim of the theft.

Architectural regulation can be covert or not noticed, and thus can affect the exercise of certain rights more deeply. [55]

This situation calls for a variety of normative and educational measures to be adopted.

Engineers and informatics should work together with ethicists and lawyers in order to build collective transdisciplinary knowledge of the relationships between technology and normativity. [56]

Moreover, both normativity “by-design” and in-design” require establishing new forms of protection. Normativity consciously and unconsciously inscribed in, and embodied by, artifacts should be made explicit and transparent before and during the design phase, when normative decisions are taken and transformed into programs and functions. Moreover, it should reflect/protect the same values and rights written in constitutions and informing legal systems. A new “generation of rights” for (the whole population brought to the level of) skilled “ICTzens” is waiting to be framed.

## 2.5 Ethics of security research

Security and ethics are strongly connected in the field of research. In the past few years research ethics has been challenged with issues of security, dealing with the publication and dissemination of results as well as the right itself to perform certain research (e.g. in the case of the engineering of avian flu viruses). Moreover, issues of dual use, and related potential export ban, of technologies, including ICT, have represented a constant concern.

In the ICT domain, the ethics of security research has been recognised as an extremely relevant and complex issue, an emerging field requiring dedicated analysis, and an important element in ICT governance. [57]

An increasing number of studies have started reflecting on the “ethics of ICT security research,” [58] arguing that the field is not well established, that most principles are simply

[54] Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code), Art. 7.2: “All persons shall undergo a minimum check in order to establish their identities on the basis of the production or presentation of their travel documents. Such a minimum check shall consist of a rapid and straightforward verification, where appropriate by using technical devices and by consulting, in the relevant databases, information exclusively on stolen, misappropriated, lost and invalidated documents, of the validity of the document
authorising the legitimate holder to cross the border and of the presence of signs of falsification or counterfeiting.”

[55] Porcedda 2012, 47.

[56] Nissenbaum 2000; Detweiler, Pommeranz, van den Hoven, Nissenbaum 2011.

[57] See Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee, Security Industrial Policy Action Plan for an innovative and competitive Security Industry, cit.

[58] As the coming Dialogue on Cybersecurity Research Ethics (June 2013) shows: http://www.caida.org/workshops/creds/1305/

borrowed from medical research ethics, but that more specific reflection is needed. [59] ICT research lacks an equivalent of the Declaration of Helsinki and well defined structures (e.g. ethics committees) for research or publication approval.

Security research poses difficult ethical issues as, in order to assess the reliability of products and procedures, research subjects are exposed to damages (e.g. safety and security *in vivo* demonstrations against dangerous behaviors, substances, terrorist attacks). [60] If undergoing potential risk is true by definition in research, ICT research appears to be "obliged" to adopt questionable behaviors for "good ends," such as harming programs users actively, watching bad things without intervening, undercover research. For instance, in order to understand and develop effective defenses to significant Internet threats, researchers infiltrate malicious botnets; or, in order to understand Internet fraud (phishing) studies require that users are unaware they are being observed. [61]

## 2.6 Ethics of surveillance? Surveillance as a legitimate participatory tool in democratic societies

If the effects of individual surveillance technologies are problematic, these are also at the origin of interesting trends, partially modifying the main *Gestalt* for surveillance.

The recent tragic events in Boston – with the precedents, in this respect, of phenomena such as the Arab Spring and the riots in Vancouver— have shown the potential for citizens to be actively involved in collaborating in public security endeavors through their personal means of surveillance. In recognizing the gaps in the security system, the Boston police asked participants in and observers of the Marathon to help by sending the images taken with their cameras and cell phones.

However, if citizens' collaboration with the power has only re-novated the means of surveillance, these practices are not modifying the balance of powers, nor the purposes (or potential secondary uses) that remain largely unverified by citizens/participants.

A radical paradigms shift in surveillance, with the potential for rehabilitating the current imaginary requires re-balancing the powers at stake, recognizing and implementing rights, and acting for legitimate goals. The concept (and practice) of "participatory surveillance" is moving towards experimenting (and establishing limits) in this direction; and participatory exercises of this kind are increasingly organized around the world in private or public forms.

These experiences include a variety of structures, platforms, technical tools, and goals.

In some cases the empowerment gained through surveillance methods consists in exerting pressure on third parties. For instance, populations living in highly polluted sites started self-monitoring their environment and health conditions in order to have industry behavior under

[59] van den Hoven J., Weckert 2008.

[60] See, for instance, the FP7 SECURED project, where a specific informed consent for in vivo demonstrations in transport threats has been prepared, http://www.secur-ed.eu/

[61] Schrittwieser 2013.

surveillance; in Corporate Social Responsibility citizen surveillance of industry behaviors may be an indirect form of control of good practice implementation.

In other experiences individuals and communities become empowered for themselves and/or for the benefit of others. Examples are: communities concerned about the spreading of infectious diseases in potentially affected areas perform early detection of cases and symptoms; [62] communities living in areas susceptible to natural disasters use surveillance methods for preparedness and to limit damages; communities of diabetic people monitoring each other's hypoglycemia events. [63]

In all these cases, the general framework for surveillance is oriented towards more democratically-shared and controllable goals; it is conceived for, and legitimized by, the benefit of communities; and represents a strategy to empower citizens.[64]

Moreover, this paradigm shift is coherent with the concept of security endorsed by critical studies as it is moving towards an emancipated normativity, with security and surveillance disentangled from power.

# 3 ICT Governance as a flexible balancing act

The few elements offered in the previous pages can be summarized as the balancing of different elements: balancing technology and humanity, balancing normative and technical instruments as well as legally binding and soft law tools, and balancing powers.

As the balance of technology and humanity is concerned, some reasons for the need to nurture human agency and to integrate human and technical actions were provided.

As to the balancing of normative instruments, legal instruments have been primarily and widely used in the ICT field in the EU context, while soft law and ethics have played a much more limited role (as the EGE quite recent involvement in the ICT field also shows). In several ICT regulatory domains, the idea that only law enforcement can achieve effective results is widely shared; [65] and this idea has become even stronger with normativity by-design.

As said, though all these instruments can be usefully applied, and the meaning of, for instance, privacy-by-design as a normative principle is actually strengthening the value of normativity, by-design protection cannot be separated – as the EDPS outlined— from other instruments that can be implemented through human-based behaviors.

Both by-design tools and values -in-design require the framing of new rights in order to make these black-boxed normative choices accessible, disclosed and discussed by citizens.

[62] http://healthmap.org/en/ (Accessed 14 May 2013).

[63] See the recently published Weitzman, Kelemen, Quinn, Eggleston, Mandl 2013.

[64] See the journal Surveillance & Society 2011, http://www.surveillance-and-society.org/ (Accessed 14 May 2013).

[65] Against the use of soft law and self-regulation see, for instance, http://www.edri.org/edrigram/number11.8/commission-opinion-self-regulation (Accessed 14 May 2013).

Still, ethics may play a relevant role in the ICT dynamic and complex context. Together with the importance of institutional ethical guidance (e.g. EGE opinions), ICT dynamics may require that other spaces for ethical reflection be opened up.

The loops generated in ICT at the interface between technology and normativity can become part of a virtuous governance circle.

# References

Agamben G. (2005), State of Exception, Chicago IL, Chicago University Press (2003).

Arendt A (1998), The Human Condition, Chicago IL, University Of Chicago Press (1958).

Ariansen P. (2003), Institutional Ethics, Encyclopedia of Life Support Systems, vol.I, http://www.eolss.net/Sample-Chapters/C14/E1-37-02-03.pdf (Accessed 14 May 2013).

Art.29 WP (Article 29 Working Party) (2009), Opinion 168 on The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data.

Brenner S. and Koops B-J. (eds) (2006), Cybercrime and Jurisdiction. A Global Survey, The Hague, TMC Asser Press.

Burke A. (2007), What security makes possible: some thoughts on critical security studies, Working Paper 2007/1, Australian National University, Canberra, http://ips.cap.anu.edu.au/ir/pubs/work_papers/07-1.pdf (Accessed 14 May 2013).

C.A.S.E. Collective (2006), Critical Approaches to Security in Europe: A Networked Manifesto, in Security Dialogue 37, 443-487.

CEC (2012), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, The Digital Agenda for Europe - Driving European growth digitally, COM(2012) 784 final, Brussels, 18.12.2012.

Curvelo P., Guimarães Pereira A., Tallacchini M, Rizza C., Ghezzi A., Vesnic-Alujevic L., Breitteger M., Boucher P. (2014). The constitution of the Hybrid World, JRC87274 (Scientific and Policy Reports).

Detweiler C., Pommeranz A., van den Hoven J., Nissenbaum H. (2011). Proceedings of the 1st International Workshop on Values in Design – Building Bridges between RE, HCI and Ethics, 6th of September, 2011, Lisbon, Portugal, http://mmi.tudelft.nl/ValuesInDesign11/proceedings.pdf (Accessed 14 May 2013).

EDPS (European Data Protection Supervisor) (2010). Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy (Opinion on Privacy By Design). OJ C 280, 16.10.2010, p. 1–15.

Foucault M. (1975). Discipline and Punish: the Birth of the Prison, New York, Random House.

Hackett E.J., Amsterdamska O., Lynch M.E., Wajcman J.( 2007), Handbook of Science and Technology Studies, 3rd ed. Cambridge, MA, MIT Press.

Hildebrandt M. and Rouvroy A. (eds) (2011), The Philosophy of Law Meets the Philosophy of Technology. Autonomic Computing and Transformations of Human Agency. London, Routledge.

Jaimes A., Sebe N., Gatica-Perez D. (2006). "Human-Centered Computing: A Multimedia Perspective". Proceedings of the 14th annual ACM international conference on Multimedia. Santa Barbara, CA, ACM Press, 855–864.

Jasanoff  S. (2012), Science and Public Reason, Oxon, Routledge.

Kling R. and Star S.L. (1997). "Human centered systems in the perspective of organizational and social informatics." Human Center Systems. National Science Foundation, http://www.ifp.illinois.edu/nsfhcs/bog_reports/bog4.html (Accessed 14 May 2013).

Kroes N. (2011), Internet essentials, OECD High Level Meeting on the Internet Economy, Paris, 28 June.

Kroes N. (2013), Using cybersecurity to promote European values. Launching the EU's Cybersecurity Strategy press conference /Brussels, SPEECH/13/104, 7 February.

Landau S. (2010), Surveillance or Security? The risk Posed by New Wiretapping Technologies, Cambridge, MIT Press.

Lessig, L. (2006), Code, Version 2.0, Basic Books, New York (1st ed. 1999).

Nielsen M. (2012), Reinventing Discovery: The New Era of Networked Science, Princeton NJ, Princeton University Press.

Nissenbaum H. (2001), How Computer Systems Embody Values, Computer, http://www.efiko.org/material/How%20Computer%20Systems%20Embody%20Values%20by%20Helen%20Nissenbaum.pdf (Accessed 14 May 2013).

Nissenbaum H. (2004), Will Security Enhance Trust Online, or Supplant it?, in Kramer R.M. and Cook K.S. (eds), Trust and Distrust in Organizations: Dilemma and Approaches, New York, Russell Sage Foundation, 155-188.

Nissenbaum H. (2011), From Preemption to Circumvention: If Technology Regulates, Why Do We Need Regulation (and Vice-versa)? Berkeley Technology Law Journal, 26, 3, 1367-1386.

Pagallo U. (2012), Good Onlife Governance: On Law, Spontaneous Orders, and Design, Onlife Project, https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Contribution_Pagallo.pdf (Accessed 14 May 2013).

Porcedda M.G. (2012), Data Protection and the Prevention of Cybercrime: The EU as an area of security? EUI Working Papers, LAW 2012/25, European University Institute, Florence.

Robinson D., Yu H., Zeller W.P., and Felten E.W. (2009), Government Data and the Invisible Hand, Yale Journal of Law and Technology, 11, Article 4, http://digitalcommons.law.yale.edu/yjolt/vol11/iss1/4 (Accessed 14 May 2013).

Schrittwieser S. (2013), Ethics in security research, January 7, 2013 http://www.youtube.com/watch?v=rtkDHVTSPSc (Accessed 14 May 2013).

Tallacchini M. (2009), Governing by Values. EU Ethics: Soft Tools, Hard Effects, Minerva, 47, 281–306.

Tallacchini M. (2013), Human Tissues in the “Public Space:” Beyond the Property/Privacy Dichotomy, in Pascuzzi G., Izzo U., Macilotti M. (eds), Comparative Issues in the Governance of Research Biobanks, Heidelberg-New York, Springer, 87-103.

Tien L. (2005), Architectural Regulation and the Evolution of Social Norms, Yale Journal of Law & Technology, 7, Article 1, http://digitalcommons.law.yale.edu/yjolt/vol7/iss1/1 (Accessed 14 May 2013).

UNDP (1994), Human Development Report 1994, Oxford, Oxford University Press.

van den Hoven J., Weckert J. (2008), Information Technology and Moral Philosophy, Cambridge, Cambridge University Press 2008.

Weitzman E.R., Kelemen S., Quinn M., Eggleston E.M., Mandl K.D. (2013), Participatory Surveillance of Hypoglycemia and Harms in an Online Social Network, JAMA Internal Medicine 173, 5, March 11, 345-351.

European Commission
EUR 26631 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen

Title: Governance of ICT Security: A Perspective from the JRC

Author(s): Angela Guimarães Pereira and Mariachiara Tallacchini

Luxembourg: Publications Office of the European Union

2014 – pp. 23 – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424
ISBN 978-92-79-37967-3

doi: 10.2788/72624

Abstract

Information and communication technologies (ICT) are enabling unforeseen capabilities in all aspect of our lives. They are reframing how we think, learn, work, play, and interact at personal, social, and political level. While these technologies are essential for society and for today's information economy, several aspects of their applications remain un-reflected and open to surprises.

For the first time in Opinion 26 (2012) the EGE has extended its analysis to ICT, identifying and addressing some key-problems in ICT ethics, as well as looking at the ethical implications of different ICT applications, new fields of research, and future developments. Opinion 28 will specifically deal with security and surveillance technologies, a domain where the ICT normative issues are even more problematic, due to the ethical, legal, and political ambiguities affecting these concepts and their histories.

The reflections proposed here below touch on some general normative issues concerning ICT implications, and discuss a few key elements in the construction of a framework for their governance, especially in the fields of security and surveillance.

LB-NA-26631-EN-N

## JRC Mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

*Serving society*
*Stimulating innovation*
*Supporting legislation*

Publications Office

ISBN 978-92-79-37967-3