Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

Saggi

Let's Go for New or Emerging Security Technologies!... What About Their Impact on Individuals and the Society? *

di Matteo E. Bonfanti **

1. The Promotion of EU Security through Technological Innovation

Technological innovation is embraced as an unquestionable component of the EU's security policies.[1] From the turn of the century, the EU

* This paper builds on research undertaken within ETCETERA (Evaluation of critical and emerging technologies for the elaboration of a security research agenda - FP7 GA No. 261512), and EVoCS (The evolving concept of security: A critical evaluation across four dimensions; FP7, GA No: 605142). It was presented and discussed at EISA 9th Pan-European Conference on International Relations 23-26 September 2015, Giardini Naxos, Sicily, Italy, Section 38: The Politics of (In)Security: Securitization, Technocratisation or (Re)Politicisation? Panel: The Evidence-base for Security Policy: Addressing the production of knowledge in a contentious policy field. The author would like to thank the anonymous reviewers who provided their useful comments and informed feedback on this paper.

** Senior Researcher at the ETH Center for Security Studies. Contributo sottoposto a doppio referaggio anonimo (*double blind peer review*).

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

has increasingly promoted the development and employment of "new", "advanced", "next generation" or "emerging" technologies for countering its internal and external security threats.[2] These technologies have

[1] Nowadays, technology represents a fundamental element of the articulated approach the EU has adopted to deal with internal (and external) security threats. This approach consists in different initiatives and actions involving many actors that have a stake in the promotion of EU security. For the most part, the aim of the above initiatives is to promote the deployment of available and mature technologies; in some cases, their goal is to encourage the development and adoption of "advanced", "next generation", "new" or "emerging" technological systems. For the purpose this paper, "new" or "emerging" security technologies are meant as technologies that will reach maturity in 5-15 years and that can be relevant for enhancing (European) security.

[2] This is quite evident with regard to the policies and measures that have been adopted to foster the security domain of the EU Area of Freedom, Security and Justice. The pursuit of "new technologies" for security purposes took on new dynamics following the adoption of *The Hague Programme: Strengthening Freedom, Security and Justice in the European Union*, OJ C 53, 3.3.2005, p. 1 ff. In this programmatic document, the European Council supported explicitly the full use of "new technologies" to improve exchange of information among relevant European and national law enforcement and security agencies, as well as stressed the importance of biometrics and information systems in tackling illegal migration, improving border controls and fighting terrorism (*Ibidem*, par. 1.7.2 and 2.1). The Council of the EU has also reiterated the relevance of "technologies and technological developments" in *The European Union Counter-Terrorism Strategy*, Doc. 14469/4/05 REV 4, Brussels, 30.11.2005, par. 16 and 17. However, it is with the adoption of *The Stockholm Programme "An open and secure Europe serving and protecting citizens"*, OJ C 115, 4.05.2010, p. 1 ff, par 4.2 and 4.6, and of *The EU Internal Security Strategy "Towards a European Security Model"*, Doc. 5842/2/10, Brussels, 26.03.2010, p. 2, par VII, that the mobilisation of the "necessary technological tools" has become an integral component of the EU's internal security policy. Both documents supports the adoption of new technologies as well as the promotion of further technological developments (par. VIII). They state that the development of new technologies should not be a fragmented process but follow a common scheme and be informed by the principle of economic efficiency. It should take advantage of a close collaboration between the public and the private sector,

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

been presented as a potential solution not only for one given threat but for many, ranging from natural and man-made disasters to terrorism, organised crime, and, in principle, to any other threats having a direct impact on the lives, safety, and well-being of EU citizens. As emphatically stated in the *The European Agenda on Security*: "Innovative solutions will help to mitigate security risks more effectively by drawing on knowledge, research and technology".[3]

Consistently with the increasing role assigned to technological innovation in countering the menaces to European security, the EU has taken actions in order to acquire the necessary technological tools. It has stimulated the supply of new technologies by: (i) supporting relevant re-

meaning EU public bodies and authorities, academia, research centres and industries. The EU should "drive" such public-private partnership or cooperation and continue to support it through its research and development programmes and funding. To implement the *EU Internal Security Strategy*, the Commission adopted the *Communication on "The EU Internal Security Strategy in Action" Five steps towards a more secure Europe"*, COM(2010) 673 final, Brussels, 22.11.2010. In this Communication, the Commission identified five strategic objectives to be pursued through 41 specific actions. Some of threes actions explicitly recommend the employment of "new" or "emerging" technologies (*Ibidem*, Objective 2, Action 3, p. 8; Objective 4, p. 11). In general, the above-cited policy instruments do not call for the development of specific technologies but refer to technological areas like ICT or satellite imagery. The basis for EU action in this field stems from the Treaty on the Functioning of the European Union, Title V "Area of freedom, security and justice" (AFSJ)". The aim and scope of such action is established by Art. 3 (2) of the Treaty on European Union.

[3] *Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions, Strasbourg*, 28.4.2015 COM(2015) 185 final, p. 11, available at http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

Saggi

search and development (R&D) initiatives at European level; and (ii) sustaining the European security industrial sector.

Significant budgetary resources have been allocated for the purpose of researching new security technologies.[4] One of the main features of the EU financial sponsorship is the involvement of different security stakeholders – *i.e.* the EU and national institutions, law enforcement agencies, research centers, academia, industries and to a certain extent the civil society – in the definition of R&D priorities and in the implementation of R&D plans. The cooperation among the cited stakeholders has been framed by the EU as part of an effort to build a "public-private dialogue" (Bigo & Jeandesboz, 2010).[5] The EU has also promoted the in-

[4] As acknowledged by the Commission in its 2004 *Communication "Towards a Programme to Advance European Security through Research and Technology* COM(2004) 72 final, Brussels, 3.2.2004, p. 4:"In an increasingly technological and knowledge-based world, excellence in Research and Technological Development (RTD) is a prerequisite for the ability to tackle the new security challenges". Support to technological development in the security field has been mainly provided by the European Commission's DG Information Society (INFSO) and DG Enterprise and Industry over the past decade starting with the *Preparatory Action in Security Research* (PASR, 2004-2006) and continued under the *Security Theme of the Seventh Framework Programme* (FP7-ST, 2007-2012). Nowadays, it is up to EU's *Horizon 2020* (2014-2020) programme to foster the development of new technologies in Europe. Parallel to the above research initiatives, DG Home Affairs has run a *Framework Programme on Security and Safeguarding Liberties*. The Schengen area EU countries can also apply for funding to the *External Border Fund. Cf.* http://ec.europa.eu/dgs/home-affairs/financing/fundings/migration-asylum-borders/external-borders-fund/index_en.htm.

[5] Commission, *Communication on Public-Private Dialogue in Security Research and Innovation*, COM(2007)511 Final, 11 September 2007, available at http://ec.europa.eu/enterprise/policies/security/files/study_public_private_dialogue_security_research_and_innovation_en. As far as the "participants" of the promoted dia-

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

volvement of representatives from the military sector in the definition of R&D priorities, in particular the European Defence Agency. This involvement stemmed from the need to synchronise research initiatives carried out, on one side, in the civil and, on the other, military security domain with a view to avoid duplications and to profit from possible synergies.[6]

Both on the supply and the demand side of new technologies for security, the EU has also planned to improve its support for the European security industrial sector, meant as industries offering technological products to end-users in response to their security concerns.[7] Support to

logue are concerned, some criticism has been expressed towards the limited involvement of representatives of the civil society. Other criticism concerned the disproportionate role played by European security and defence industries in defining security R&D priorities; the same industries that have been among the main beneficiaries of EU's funding. This criticism has raised claims for improving oversight and transparency of the dynamics concerning the above "public-private dialogue". It is worth noting that the "public-private dialogue" model/scheme will continue to apply to future EU sponsored research and development initiatives in the field of security. For further references, *see Developing an EU Internal Security Strategy, Fighting Terrorism and Organised Crime*, p. 95.

[6] The EU has already shown commitment to the civilian employment of technologies that are traditionally used in the military sector. Evidence of this commitment is represented by the different initiatives promoted by the EU and aimed at the adoption of Remotely Piloted Aircraft Systems in the civilian sector. The EU is aware of the enormous potential of this technology, also with regard to the possibilities it offers for testing and implementing "new" technologies and procedures for aviation as a whole.

[7] Commission, *Communication Security Industrial Policy Action Plan for an Innovative and Competitive Security Industry*, COM(2012) 417 final, Brussels, 26.7.2012, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0417:FIN:EN:PDF. It should be noted that the Communication accepts that there is no clear definition of the security industry.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

this sector consists of different actions. First, it entails fostering interoperability and compatibility among developed technological systems or equipment across Europe.[8] Interestingly, it also entails the promotion of societal acceptance of new security technologies by enforcing – among other things – the principles of "privacy by design" and "privacy by default". In this context, societal acceptance is seen as an important element to sustain the demand side of new security technologies. This demand comes from end users (*e.g.* International, European, and national law enforcement and security agencies – private operators included) who are interested in purchasing products which fulfill established security requirements and are accepted by society at the same time.[9] According to the EU, the promotion of societal acceptance requires a thorough assessment of the impact new security technologies may have on society and individuals' fundamental rights.[10] This assessment should be

[8] This requires the definition of common standards for security-related equipment as well as the establishment of EU-wide certification schemes for new security technologies. *Ibid*. With regard to the standard, the Commission recently mandated European standardization organisations to produce a "privacy by design" standard. As stated by the Commission «compliance with this standard will ensure that EU security products and services respect individuals' rights and thereby enhance consumer confidence». *Ibidem*, p. 13.

[9] In the cited Communication, the Commission acknowledges that the employment of security technologies may affect individual's fundamental rights. The potential negative impact on such rights should be preventively eliminated or mitigated. For the industrial sector, a negative impact means: «[...] the risk of investing in technologies which are then not accepted by the public, leading to wasted investment. For the demand side it means being forced to purchase a less controversial product which however does not entirely fulfil the security requirements». *Ibidem*, p. 5.

[10] It also requires a wider and more effective engagement of civil society in security research and innovation processes. *Ibidem*.

carried out during the R&D phase, well in advance of a technology employment. It should also be aimed at allowing researcher and developers to enforce fundamental rights compliance by technological design.[11]

2. Societal Acceptance and Respect for Fundamental Rights: It Is Not Only a Matter of Marketing

Respecting individuals' fundamental rights as well as mitigating possible negative ethical and societal consequences that emerging security technologies may generate are not only meant by the EU as requirements for sustaining the demand side of its industrial security sector. In other words, promoting societal acceptance and compliance with ethical values and fundamental rights is not (should not) only intended as a strategy for marketing these technologies.

With regard to fundamental rights, their respect and enforcement is an obligation established by different European (and International) legal instruments. All actions the EU adopts to implement its security strategy have to comply with the fundamental rights provisions contained in the

[11] It will be also necessary to adopt standards enhancing the enforcement of the principle of privacy by technological design. The principle is aimed at the early identification, elimination or mitigation of any potential negative effects technologies may have on privacy. *Ibidem*, p. 11 ff. Privacy and dignity are deserved by particular attention by the EU policy document. Such an emphasis does not mean that other rights are less prominent or deserve minor attention.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

European Convention on Human Rights (ECHR), [12] the *Charter of Fundamental Rights of the European Union (CFREU)*[13], and other relevant instruments, like privacy and data protection regulations. In fact, this obligation is recalled in different policy and legal instruments adopted by the EU and dealing with security. For example, it is stressed by the documents that defines the internal security strategy of the Union – especially *The Stockholm Programme*,[14] *The EU Internal Security Strategy "Towards a European Security Model"*[15], the Commission's *Communication on "The EU*

[12] *Convention for the Protection of Human Rights and Fundamental Freedoms (CETS No. 005)*, 4.11.1950, available at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=005&CL=ENG.

[13] *The Charter of Fundamental Rights of the European Union*, OJ C 83, 30.03.2010, p. 389 ff. The Charter is Europe's primary legal instrument recognising the various personal, civil, political, economic and social rights of EU citizens and residents. The Text of the EU Charter is also available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF

[14] As stated by the *Stockholm Programme*, cit., par. 1.1: «The challenge will be to ensure respect for fundamental rights and freedoms and integrity of the person while guaranteeing security in Europe. It is of paramount importance that law enforcement measures, on the one hand, and measures to safeguard individual rights, the rule of law and international protection rules, on the other, go hand in hand in the same direction and are mutually reinforced». *Cf.* also *Commission Staff Working Paper Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments*, SEC(2011)567 final, Brussels, 6.5.2011, available at http://ec.europa.eu/governance/impact/key_docs/docs/sec_2011_0567_en.pdf. Cf. also par. 2.

[15] According to *"The EU Internal Security Strategy in Action"*, cit., p. 9, the tools and actions to be adopted for implementing the EU Internal Security must be based on: "common values including the rule of law and respect for fundamental rights as laid down in the EU Charter of Fundamental Rights."

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

Internal Security Strategy in Action", and *The European Agenda on Security*.[16]

With regard to the commitment towards the protection of individual rights – especially the right to privacy and to data protection within the information society – the *Stockholm Programme* acknowledges that "technological developments" do not only present new challenges to the protection of such rights, but also offer new possibilities to better protect and enforce them.[17] From this perspective, the *Programme* endorses the principle according to which fundamental rights (privacy and data protection) may be respected and enhanced by the adoption of specific technologies (*Privacy enhancing technologies* or *PETs*) or by technological design (*privacy-by-design* principle).[18] The above approach is endorsed – both implicitly and explicitly – also by other actions adopted by the EU institutions and dealing with new security technologies.

[16] *The European Agenda on Security*, cit., p. 3. «First, we need to ensure full compliance with fundamental rights. Security and respect for fundamental rights are not conflicting aims, but consistent and complementary policy objectives. The Union's approach is based on the common democratic values of our open societies, including the rule of law, and must respect and promote fundamental rights, as set out in the Charter of Fundamental Rights».

[17] *Ibidem*, par. 2.5.

[18] As already pointed out *supra*, the right to privacy and to data protection are explicitly mentioned. This seems the consequence of the fact that technologies to be used for border management or for fighting crime and terrorism as well as some other threats entail most likely the gathering, processing and sharing of personal and sensitive information.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

Saggi

3. Assessing the Impact of Emerging Security Technologies: Not an Easy Task at All

As described above, the same EU policy instruments that support the development and adoption of emerging security technology call also for the assessment of the effects these may have on ethical values, fundamental rights and, in general, the society as a whole. With regard to technologies that are "emerging", such an assessment has to be carried out especially at R&D stage, and should aim at establishing the likely effects these technologies have on the above values, rights, and the society.[19] As such, it is a very wide-ranging and complicated form of investigation.

A general problem is that the ethical, fundamental rights and societal implications of an emerging technology are context/application-dependent. The issues raised by one specific emerging technology employed by one actor in a specific context could well be different from those raised by the same technology but used by another actor in a different context. For example, one may consider the different ethical, fundamental rights, and societal implications stemming from the possible applications of the so called "homomorphic encryption" – an emerging technology that can be applied for security purposes.[20]

[19] The European Commission usually produces impact assessment reports covering economic, social, and environmental consequences of new initiatives.

[20] ETCETERA Project, http://www.etcetera-project.eu/.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

Saggi

Homomorphic Encryption

Current cryptographic algorithms typically do not allow operating on ciphertexts without decrypting them. For example, it is not possible to search data in an encrypted database. Instead, it is first necessary to decrypt the data before it can be processed. Only afterwards the data can be encrypted again. A possible solution is the use of so-called homomorphic (structure-preserving) encryption schemes. Homomorphic encryption schemes allow specific types of computations to be carried out on the ciphertext, so that the result obtained is the encryption of the result of analogous operations performed on the plaintext.

The development and use of homomorphic encryption is likely to generate some ethical and fundamental rights issues as well as to have an impact on a given society. Of course, the kind of issues and impact will change according to the broad context this technology is adopted, its specific application, the entities that control or are empowered by its deployment or, in general, the actors involved. For example, the ethical and fundamental rights implications will be different according as this technology is used by governments or public authorities to cipher diplomatic communications, by private corporations to encrypt sensitive information, by individuals to communicate privately or by criminals to avoid being intercepted or tracked by law enforcement authorities. In some of the above cases, the use of homomorphic encryption will raise a transparency issue while in others it will be a matter of legitimate protection of sensitive information or a question concerning individual's freedom of information. In other words, it is the type, context and purpose of the adoption of homomorphic encryption that matters in order to determine the relevant ethical, fundamental rights and societal impli-

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

cations.

Having said that, homomorphic encryption may be an effective tool to enforce the right to private life and/or correspondence/communication (CFREU, art. 7) and to data protection (CFREU, art., 8). As discussed above, homomorphic encryption enhances information confidentiality to a very great extent. Thus, it can be used to "secure" personal information and/or private communications. As far as data protection is particularly concerned, it should be noted that the "principle of security" requires the adoption of appropriate technical measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing (cf. Directive 95/46/EC, art. 8; General Data Protection Regulation, art 32).[21] Homomorphic encryption can be a useful tool to be adopted for enforcing such principle. In this sense, it becomes a "privacy-enhancing technology". However, in order to be in full compliance with data protection norms and principles, the encrypting process should guarantee the integrity of the personal information provided in the plain text. Indeed, data protection requires personal data to be accurately processed (cf. Di-

[21] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L119, 4.05.2016, p 1 ff; Directive 1995/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281, 23.11. 1995, p 31 ff. The General Data Protection Regulation entered in to force on 24th May 2016 but will apply from 25th May 2018.

rective 95/46/EC, art. 6; General Data Protection Regulation, art 5).

Homomorphic encryption may also represent an effective tool to enforce freedom of expression and information, in particular the right to receive and impart information and ideas without interference by public authority (CFREU, art. 11).

From a broad societal point of view, it should be noted that coding and encrypting information has traditionally been the province of spies and their governments. Today, it is a part of everyday life for many individuals. Nowadays, personal data and other relevant information are processed electronically by governments, health care providers, banks, insurance companies, industries etc for different purposes. Without effective encryption of this information, anyone of these processing operations would be potentially vulnerable to criminal actions. Crimes like identity theft, credit card fraud, and other kinds of "cyber-crime" would jeopardise not only the public security and order, but also the economic growth and social trust of a given community.

The above example shows that each application of a certain technology needs to be considered on its merit. Since it is difficult to foresee the exact context an emerging technology ends up to be employed, targeting all the ethical, societal and fundamental rights issues is not an easy task. In some cases, it could be relatively feasible, especially when emerging technologies are to be used for carry out pre-identified tasks – like surveillance of individuals – in targeted contexts: an airport, a train station, a border checkpoint. However, even in these cases it is difficult to have a comprehensive picture of all the issues that may arise. This does not mean that anticipatory thinking on ethical, fundamental rights and societal implications of emerg-

ing technologies is useless. On the contrary, it may help to identify and mitigate some negative effects as well as fully exploit all the benefits the concerned technologies may generate. In other words, tackling the above issues well in advance – *i.e.* at research and development stage – may help in identifying problems and finding appropriate solutions.

Further to the above-discussed general problem, other issues may affect the feasibility of a sound and comprehensive ethical, fundamental rights, and societal impact assessment of new and emerging technologies. The following paragraphs try to highlight these issues. They also discuss what the assessment of societal impact or the *ex-ante* identification of ethical and fundamental rights issues, of emerging security technologies may entail.

4. Assessing Societal Impact

4.1 General Difficulties Related to the Notion of "Societal Impact"

The idea that there is any single entity, the European society, seems a myth. "Societies" are groups of groups, communities of communities. One may (and probably must in some cases) talk about societies as if they were unified entities; but the reality is far from that: every society is immensely complex. Hence, it follows that predicting, analysing, or mapping the array of potential or actual societal impacts of any mature or emerging technology is an immensely complex task.[22]

[22] *Cf.* PACT (*Public perception of security and privacy: Assessing knowledge, Collecting evidence, Translating research into action*), Societal Impact Report (D1.4), 30 June 2012, p. 9 ff.,

Secondly, societal impact incorporates a wide range of categories ranging across the different aspects of people's lives (Burgess, 2012).[23] It is thus connected with people's health and wellbeing, economic prosperity, cultural integrity, the fundamental rights, fears and aspirations.

Given that societal impact assessment involves assessment of change, it is perhaps natural to think of it in terms of measurement of change. This, however, is a controversial point: for "assessment" and "measurement" are not synonyms. If one looks again at the above-mentioned categories, while some are amenable to some sort of metric – and hence to measurement – some are not. In some cases, impacts are only controversially measurable (*e.g.* aspirations). In other cases, it makes only sense to speak of "more" or "less". In further cases, this would be impossible. Suppose a proposed employment of an emerging technology is predicted to breach a fundamental right, or a legal norm (perhaps it would constitute a violation of human dignity or a breach of some article of data protection legislation). In these cases, to speak of "more" or "less" violation seems inappropriate: a violation is a violation. Presumably, the punishment could be more or less severe depending on the severity of the breach to rights, but the breach itself (as opposed to its punishment or the sense of outrage it provokes) is an all or nothing matter. This sug-

available at http://www.projectpact.eu/deliverables/wp1-root-branch-review/d1.4-social-impact-report/PACT_D14_FINAL.pdf/view.

[23] According to the Author, "Societal Impact Assessment" (SIA) is: «An assessment of the change brought about within a society as a result of a prior change within that society. Thus a SIA might make an assessment of the various changes brought about within a society as a result of the introduction of a new technology».

gests that there are some societal impacts which, depending on how one looks at it, are either not amenable to measurement at all, or are amenable only to a strict binary classification (*e.g.* that a breach of rights either did occur or did not).

The need for careful analysis is nowhere clearer than in the case of societal impact assessment with respect to technologies to be used for security. This is because security always has two sides: there is actual, objective security – *i.e.* how secure a society actually is; and there is perceived, felt security – *i.e.* how secure a society perceives itself to be. Societal impact assessment with respect to security technologies must take into account both actual security and perceived security. Moreover, it must take into account the relationship between the two. This latter task turns out to be extremely difficult. It thus follows that in assessing the societal impact of a security or surveillance technology, one must consider: (i) the issue of whether people are *actually* more or less secure; (ii) the issue of whether people *perceive* themselves to be more or less secure; (iii) the fact that both *being secure* and *feeling secure* involve a wide range of domains (wellbeing, suspicion, economic life, political life, security is *human* security).

4.2 Societal Impact Assessment of Security Technologies

In 2011 the Directorate Enterprise – Security Programme of the European Commission set up Societal Impact Expert Working Group, whose

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

results were published in a Report released in February 2012.[24] In their reports the experts acknowledged that the securitization of society is a complex process and involves a range of impacts and consequences, some real and some matters of perception, all of which need to be addressed properly.

With regard to research initiatives aimed at developing new security technologies that have been so far sponsored by the EU, the experts complained about an insufficient consideration of the societal impact these initiatives generate. Addressing this impact would first require to reflect on the necessity and proportionality of a new security technology in a democratic society. Then, it would entail investigating the effects that both the implementation of a security research programme/project and the future employment of a new technological solution have on society. As stated in the Report: «Societal relevance asks whether research actually leads to enhancing the security of European citizens and how it will affect the lives of citizens in doing so».[25]

The study of such an impact should not be restricted to the EU. It should also consider the potential effects these technological solutions may have outside Europe, *i.e.* in third countries. Indeed, as previously stated, a technology could be used in a very different way then what it was developed for. This means that it could be deliberately employed in a way that contravenes individuals' fundamental rights, or amplifies

[24] *Report of the Societal Impact Expert Working Group EC DG ENTR*, February 2012, available at http://www.bioenv.gu.se/digitalAssets/1363/1363359_report-of-the-societal-impact-expert-working-group-2012.pdf.

[25] *Ibidem*, p. 10.

people's fear or frustrates their aspirations. It is therefore paramount that developers together with EU Commission make sure that adequate regulation, control and licensing is available for a concerned security technology before it is finished and can be sold or exported.

4.3 Societal Impact of "Emerging" Security Technologies

4.3.1 Methodological Considerations

The main difficulties related to the analysis of the societal impact generated by security technologies tends to be exacerbated by the fact that the technologies here at stake are "emerging", *i.e.* yet to be developed and employed. Investigating such an impact implies making statements about events whose actual outcomes have not yet been observed. In other words, it entails thinking about the potential effects these technologies may have on society and forecasting their societal consequences.

There are different methods or techniques to forecast events (Makridakis, 1998; Amstrong, 2001). These methods may be applies in different fields and for diverse purposes. There are methods that may reveal appropriate and useful in order to investigate the likely societal impact of emerging security technologies.

One of the latter, entails asking for, gathering, and examining experts' opinions on the subject matter. These may be social scientists, economists, technologists or other specialists who can provide useful information, ideas and foresights about social consequences stemming from the development and adoption of emerging security technologies.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

Among the most traditional techniques for collecting information from experts, there are "Delphi surveys", "nominal group conferencing" and "structured interviews". The choice of the technique to be employed will influence the selection of experts and vise versa.[26]

Another forecasting method to be potentially employed to investigate the likely societal impact is trend analysis. This method is based on the assumption that the future will be very much like the past for some period of time. Trend analysis assumes that events, trends and development patterns in the past were shaped by various fundamental driving forces and that, as long as these forces do not change significantly, past change will continue into the future (Vanston, 1998). Usually, trend analysis is adopted and works quite well for quantifiable parameters. This makes it not suitable for investigating the societal impact comprehensively. As already pointed out, societal impact incorporates a wide range of categories ranging across the different aspects of people's lives. Therefore, trend analysis can be appropriately used to forecast societal effects that are quantifiable (*e.g.* economic prosperity).

As per the societal effects that are "qualitative" in their nature, another forecasting technique to be employed is historical analogy (Aquilano, 2005). Very basically, this technique entails studying the past for extrapolating what will happen in the future. Applying this methods to investigate the societal impact that is likely to derive from the development and employment of emerging security technologies would roughly en-

[26] It should be noted that there are several other techniques for exploiting the power of groups in forecasting: brainstorming, gaming, synectics, focus groups are commonly refereed techniques.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

tail: (i) to identify technologies or cluster of technologies that are similar – both in their main functions, operating conditions and context of employment – to a concerned emerging security technology; (ii) to examine the societal effects that the adoption of the former technologies generated and consider which effects are the most likely to reoccur when the emerging technology is introduced. For example, in order to forecast the societal consequences deriving from the use of emerging satellites technologies for monitoring public spaces in urban areas to prevent criminal activities, it may be worth studying the effects generated by the adoption of CCTVs or drones in the same areas for the same purpose. It is important to stress that the effects will not be the same. However, can be very similar.

Another useful forecasting technique that can be adopted in order to study the societal impact of emerging security technologies is scenario analysis. It is the process of analyzing possible future events by considering alternative possible outcomes (sometimes called "alternative worlds") (Maack, 2001). In contrast to trend analysis, the scenario analysis is not using extrapolation of the past. It does not rely on historical data and does not expect past observations to be still valid in the future. Instead, it tries to consider possible developments and turning points, which may only be connected to the past. The main strength of this forecasting technique is that it offers the potential to integrate information from diverse sources and of different character into a single forecast (Porter, 1991). It allows to incorporate a wide range of quantitative and qualitative information produced by other forecast techniques (*e.g.* trend extrapolation and expert opinion studies). Scenario analysis represents

also an effective way of communicating forecasts to a wide variety of users.

It goes without saying that the employment of one of the above forecasting methods does not exclude the simultaneous adoption of any of the others. Indeed, they represent a set of tools that can be used in combination.

4.3.2 A Set of Questions

In order to think about and identify the potential societal effects stemming from the development and employment of emerging security technologies the following set of questions is here proposed. Questions are drawn on the EU Commission, *Impact Assessment Guidelines*, issued in 2009.[27] The Commission guidelines are for its staff preparing impact assessments of proposed and implemented policies. They do not deal with the impact generated by technologies. However, they offer a useful framework to carry out social impact assessment that may be employed for identifying and assessing the effects of a new security technology. It has to be noted that a set of questions to investigate the societal impact of EU sponsored security R&D initiatives has been already proposed by the Societal Impact Expert Working Group and adopted by the Commission for Horizon 2020.[28] The questions proposed here may integrate that

[27] *Ibidem*. The Guidelines explain what an impact assessment is, presents the key actors, sets out the procedural rules for preparing, carrying out and presenting an impact, and gives guidance on the analytical steps to follow in the impact assessment work

[28] *Report of the Societal Impact Expert Working Group EC DG ENTR*, cit., p. 17.

framework in order to make the assessment of the societal impact more comprehensive.

Security and Public Order: What documented security need(s) would the development and employment of an emerging security technology address? What threats to society would be addressed *(e.g.* crime, terrorism, pandemic, natural and man-made disasters, etc.)? Would the development and employment of an emerging security technology improve actual or perceived security, or both? What segment(s) of society would benefit from increased security as a result of the development and employment of an emerging security technology?

Fundamental Rights: What fundamental rights are likely to be affected by the development and proposed use of a certain emerging technology with security implications? What could be the impact of such technology on those rights? Would it be beneficial (promotion) or negative (limitation) or even both depending on the right concerned?

Equal Treatment and Non Discrimination: Could the development and employment of a new emerging security technology affect the principle of non-discrimination, equal treatment and equal opportunities for all? Could they have a different impact on women and men? Could they promote equality between women and men? Could they entail any different treatment of groups or individuals directly on grounds of sex, racial or ethnic origin, religion or belief, disability, age, and sexual orientation? Or could they lead to indirect discrimination? Would they be able to change power relations among individuals in a given community?

Social Inclusion: Could the development and employment of a new or emerging security technology lead directly or indirectly to greater equal-

ity or inequality in society? Could they affect specific groups of individuals (for example the most vulnerable or the most at risk of poverty, children, women, elderly, the disabled, unemployed or ethnic, linguistic and religious minorities, asylum seekers), firms or other organisations or localities more than others? Could they significantly affect third country nationals?

Public Health and Safety: Could the development and employment of a new emerging security technology affect the health and safety of individuals/populations? Could they increase or decrease the likelihood of health risks due to substances harmful to the natural environment? Could they affect health due to changes in the amount of noise, air, water or soil quality? Could they affect health due to changes energy use and/or waste disposal? Could there be specific effects on particular risk groups (determined by age, gender, disability, social group, mobility, region, etc.)?

Culture: Could have an impact on cultural diversity? Could they affects individuals' participation in cultural manifestations?

Employment and Labour: Could the development and employment of a new or emerging security technology facilitate new job creation or lead directly or indirectly to a loss of jobs? Could they have specific negative consequences for particular professions or groups of workers? How could they impact on job quality? Could they affect workers' health and safety?

Social Impact in Third Countries: Could the development and employment of a new emerging security technology have a social impact on third countries that would be relevant for overarching EU policies and obligations, especially those concerning respect for human rights?

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

Saggi

5. (*Ex-ante)* Identification of Ethical and Fundamental Rights Implications

Assessing the societal impact of new and emerging technologies for security involves examining the effects they may have on individuals' fundamental rights. This section aims at describing in more details what the identification of these effects entails in terms of anticipatory thinking. It considers also the ethical implications. Actually, the notion of ethics is larger than the concept of fundamental rights, because it includes notions about human agency, duties, personality, habits, virtues, and so. However, this section will cover only the normative dimension of ethics and consequently discuss together ethical and human right implications. With regard to the latter, they are generally discussed by taking in to account the substantive content of the CFREU's provisions as defined by the scholarship and the established case-law (ECtHR and EUCJ). Nevertheless, although important and useful, the analysis of the jurisprudence concerning each Charter's rights is beyond the scope of this study.

5.1 The Preamble of the Charter of Fundamental Rights of the European Union

The first paragraph of the preamble of the Charter of Fundamental Rights of the European Union reads: «The peoples of Europe (…) are resolved to share a peaceful future based on common values». It is then apparent that the EU is first of all a community of values, say, the European identity is based on some shared values. The second paragraph specifies that « (…) the Union is founded on the indivisible, universal values of human dignity, freedom, equality and solidarity; it is based on

the principles of democracy and the rule of law». In other words, the Charter lists of the essential values that ground European identity, i.e.: 1) human dignity, 2) freedom, 3) equality, 4) solidarity, 5) democracy, 6) rule of law. The second paragraph continues by stating that the Union «places the individual at the heart of its activities, by establishing the citizenship of the Union and by creating an area of freedom, security and justice». According to the second part of the second paragraph the focus of the Union is the individual. The establishment of the European citizenship and the creation of an area of freedom, security and justice are instrumental to the promotion of the human being. In other words, this paragraph seems to deny the possibility that an abstract notion of society should ever prevail on the concrete individual existence. This implies, for instance, that the notion of "security" is tenable only to the extent that it protects actual individuals. It is intuitive the deep consequences that these implications may have on the development and the adoption of security technologies in the EU.

The following paragraphs discuss the six basic values in relation with emerging security technologies.

5.2 Human Dignity

The notion of dignity is difficult to define and there is disagreement about its exact content (Lebech, 2016; Donnelly, 2009; Meyer, 2002).[29]

[29] Legal scholars describe dignity as «[an] ethereal concept " which "can mean many things " and therefore suffers from an inherent vagueness at its core». *Cf.* for example, Wright, 2006.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

Although it should always be seen against a specific cultural background, dignity is a universal concept (Marshall, 2009). It is recognized as a fundamental right in many national and international declarations, proclamations, and conventions (Glensy, 2011).[30] Art. 1 of the CFREU states that: «Human dignity is inviolable. It must be respected and protected». However, human dignity is not only a fundamental right in itself; it constitutes the real basis of fundamental rights (Eberle, 1998). These rights or, better, their enforcement, may be interpreted as a particular (and concrete) mechanism for realizing human dignity (Donnely, 2009).

However, what does respect for someone's dignity mean or entails? First, it entails refrain from any action or omission that have the result of dehumanizing an individual, *i.e.* depriving him of his human qualities, or causing him an experiences of shame or humiliation. Furthermore, it entails treating another individual always as an end and never solely as a mean or tool (Schachter, 1983, 848-850).[31] It involves avoiding to subject another individual to torture or other degrading treatments, or holding him in a condition of slavery or servitude. Respecting human dignity

[30] It has to be noted that the European Convention on Human Rights is completely silent about human dignity. There is no formal and explicit acknowledgment for this right of concept. Within the Convention, human dignity does play a role not in the treaty text, but in the practice of the Court's case-law (Buyse, 2016).

[31] See CJEU, *Kingdom of the Netherlands v European parliament and Council of the EU*, Case C-377/98, 9.10.2001, par. 69, 71, 76. In the ruling, the Court did not refer to CFREU, nor did it defined human dignity. However, it can be argued that it implicitly acknowledged the Netherlands' approach that human living matter could not be reduced to a means to a an end. Cf. Dupré, 2014, p. 14.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

requires safeguarding individual's integrity, but also privacy – meant as personal intimacy, identity and honour –, and broadly other fundamental rights which represent inherent components of his dignity (e.g. the right to equal treatment).[32]

With regard to integrity, it refers to the quality of individual's body and mind of being complete or undivided. Integrity is a fundamental right itself – *i.e.* the right to be free from bodily and mental intrusions or interferences – recognised in many international and national legal instruments.[33] In general, physical integrity is threatened by physical pain, injuries, sexual assaults, rape, physical inspections, and the like. Mental integrity is violated any time when emotional and cognitive processes are brutally invaded, abused and/or disrupted. As one may note the above actions impact also on individual's dignity.[34] The latter is undoubtedly violated any time that an undue and unsolicited intrusion or interference with individual's body and mind entails humiliation independently from the type of intrusion (tactile, visual, acoustic, psychological, olfactive), from whether it produces harm or adverse health conditions and whether the individual has given his consent.

Furthermore, respecting dignity requires also protecting privacy, a concept that in its broader meaning involves claims about the moral sta-

[32] *See* for example CJEU, *A, B and C v Staatssecretaris van Veiligheid en Justitie,* Joined Cases C 148/13, C 149/13 and C 150/13 Judgment, 02.12.2014, par. 65. Cf. Dupré, 2014, p. 6.

[33] Art. 3 par. 1 of the Charter, placed in Title I "Dignity". Given the context in which the above provision is framed, it is evident that human dignity relates to personal integrity.

[34] See for example ECtHR (GCh), *Jalloh V. Germany*, Judgment, 11.07.2006, par. 68.

tus of the individual self and its honour (Bloustein, 1964, 1004; Whitman, 2004). In narrow sense, privacy involves personal knowledge and the power to protect or control it. It concerns not only information about an individual but the power of an individual to determine how information about him is used (Mordini, 2012, 18). This power allows its owner to prevent the use of personal information in a way that may jeopardise his identity, image and respectability. The notion of privacy stems from the concept of human dignity. It has its roots in human dignity, and the ultimate aim of protecting privacy is to contribute in protecting dignity. Privacy implies that there is a kind of border that define and protects personal life, personal characteristics, habits, feelings and opinions; a border that preserve personal autonomy, identity and integrity (Bonfanti, 2014). These elements can all be tied to human dignity. It should be noted that the above articulated notion of privacy is enshrined in the national and international provisions stating the individual's fundamental right to privacy (Bonfanti, 2011).

What has been discussed so far shows what respecting human dignity entails in general. But what does it involve when the development and (future) employment of emerging security technologies are at stake – especially those technologies that target individuals or require monitoring individuals' behavior (surveillance technologies)?

It is paramount that any emerging security technology is designed or employed in a way that does not humiliate individuals or treat them as they were not human beings but mere objects. Such kind of humiliation or treatment may derive from technologies the employment of which results in severe interferences with individuals' personal integrity and privacy (as well as discrimination on ground such as sex, race, colour,

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

ethnic or social origin, genetic features and similar). As far as integrity is concerned, one may for example think about an emerging technological device that is designed or used for screening people's body (and mind) in order to detect potential threats to other person's or infrastructures' security. Irrespective of the type of screening at stake, it is important this device does not intrude individuals' bodily or mental integrity in such a way it causes them experiences of shame, moral degradation or that make them feeling subject to public scorn. Similar considerations can be made with regard to the effects the concerned emerging device may have on privacy. In this case it should not jeopardise individual's honour and respectability, severely hinder his capacity to take autonomous decisions, or even expose him to serious forms of harassment (*e.g.* sexual). It should not disclose persons' nakedness and their vulnerabilities. Worries about the risk that the use of some security technologies entails humiliation may be raised for particular vulnerable categories like children, pregnant women, elderly, or for incapacitated persons, or for specific ethnic, religious and cultural groups.[35]

Past experience regarding the impact on human dignity – meant both as personal integrity and privacy – generated by the deployment of technologies for security screening seems to confirm the soundness or, at least, the plausibility of the above concerns. One may think about the huge debate and critics following the adoption of image body scanners for security checks at European (and non-European) airports. As it was argued, the use of these devices entails treating individuals undergoing

[35] *Cf.* also below in the text.

security checks as though they were commodities, and no more human beings. In other words, the body scanners dehumanise individual to the extent they «reduces the traveler's body to the same legal status as a piece of luggage on a conveyor belt» (Murphy, 2001).

In light of the above, it is necessary to adopt adequate strategies aimed at preventing that the development and employment of emerging security technologies may jeopardize human dignity. These strategies require taking actions from the early research and development stage of new and emerging technologies. They require thinking about: possible employments a concerned technology may have; the actors that are potentially involved in its use, in particular, the individuals or category of individuals that may be affected by its use; the effects it may have on their dignity – privacy, integrity – and the associated risks or problems. Once these risks and problems have been identified, it is necessary to think about and adopt measures aimed their elimination or mitigation. These measures may be technological, meaning that they may consist in technical solutions that inhibit the possibility a technology will be employed to jeopardise individuals' dignity by violating their integrity and privacy. Once adopted, the consistency and effectiveness of these measures have then to be validated and monitored.

In sum, the described approach aims at embedding respect for human dignity in the design phase of a new technology. In other words, it has the goal to prevent or limit breaches of individual's dignity, integrity and privacy from the very beginning. Now, one may think it is a too generic and vague approach, which is difficult to enforce in practice. Nevertheless, there are examples where it has been already successfully adopted. Reference is made to the new versions of image body scanners

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

Saggi

that do not show the "naked" body of the passenger undergoing the screening but merely the objects he holds. Such a scanners are designed in a way that the officer viewing the image of the passenger cannot see the scanned person, his anatomic and medical details, but only a silhouette, or just a red light whereas prohibited items are detected.

5.3 Freedom

Broadly, freedom is the value of individuals to have control over their own actions (Nys, 2004; McHugh, 2006). The Charter of Fundamental Rights of the EU acknowledges both negative and positive freedoms. Its Title II, "Freedoms", is "mainly" concerned with negative freedoms or, better, with negative rights.[36] The adverb "mainly" is used here because the above rights generally require that the individual right-holder should not be subjected to *arbitrary or unnecessary*[37] interference carried out by established public authorities – or other persons or groups (Clapham, 1993). In other words, they mainly require inaction. However, more or less explicitly, some of these rights ask for action too. This is for example evident as far as the right to data protection is concerned. According to Art. 8, par. 3 of the Charter «Compliance with these rules [*data protection rules*] shall be subject to control by an independent autho-

[36] Artt. 6-19.

[37] The rights can be limited. Measures taken by public authorities that interfere with these rights can be justified under certain conditions. The interference will only amount to a violation when the justifying conditions cannot be fulfilled. The requirements for a justified limitation are set out in Article 52 of the Charter.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

rity» [emphasis added].[38] Although less explicit, action is also required by the right to education or to engage in work.[39] In general, rights that demands "respect for" or "safeguard for" they also ask for action by established authorities. In other words, they impose on these authorities the duty to adopt measures for realising effective protection. The main example is the right to privacy.[40]

As the past and ongoing huge debate concerning the impact of security policies and practices on civil rights shows, interferences with the above rights may originate from the deployment and use of technologies aimed at preventing and contrast security threats. Examples of these technologies are CCTV, UAVs, imaging scanners, satellites, biometrics technologies, tracking devices, data mining and profiling software, and in general those devices employed for cyber or real, visual, acoustical, olfactive, behavioural surveillance and monitoring. In general, they are used to identify individuals, verify and authenticate their identity, detect and monitor their behaviour in public or semi-public spaces, check and screen their bodies and belongings, locate or track their movements, collect and link information about them and create profiles. Irrespective of considerations about the necessity and proportionality of the interferences the above technologies bring about, they affect the right to liberty and security (Zedner, 2008, 254), right to privacy and to the protection of personal data (Schermer, 2007), freedom of assembly (Gogarty, 2008;

[38] Art. 8.

[39] Artt. 14 and 15.

[40] Art. 7.

Smith, 2013), freedom of expression,[41] and of thought, conscience and religion.[42] Each technology may interfere with more rights at the same time and the combination of more technologies may raise the severity of the interference.

The above concerns may be addressed to security technologies to be developed and deployed in the future. With regard to these technologies, it is necessary to adopt adequate strategies aimed at preventing they may jeopardize individuals freedoms. As already explained above with regard to human dignity, one of these strategies requires thinking about: possible employments a concerned technology may have; the actors that are potentially involved in its use, in particular, the individuals or category of individuals that may be affected by its use; the effects it may have on their freedoms and the associated risks or problems. Once these risks and problems have been identified, it is necessary to think about and adopt measures to eliminate or mitigate them. These measures may be adopted at operational or technological level. With regard to the latter, they may consist in technical solutions that inhibit the possibility a technology will entail an arbitrary, unnecessary or not proportional interference with individuals freedoms. Once adopted, the

[41] Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, F. La Rue, 17 April 2013, available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf, Cf. also *The Era of The Digital Mercenaries*, at http://surveillance.rsf.org/en/.

[42] FRA, *The Use of Body Scanners: 10 Questions and Answers*, July 210, p. 5, available at http://fra.europa.eu/sites/default/files/fra_uploads/959-FRA_Opinions_Bodyscanners.pdf.

consistency and effectiveness of these measures have then to be validated and monitored.

5.4 Equality

The notion of "equality" is difficult to define and there are different interpretations of it. The EU Charter of Fundamental Rights sets out a series of principles and rights aimed at clarifying the notion of equality, the enforcement of which has the objective to realise equality. These principles and rights imply considering all individuals, or specific groups or categories of individuals having the same value and being worth of respect. In some cases, respect has to be pursued by affording to these individuals or group a special protection. In the Charter perspective, equality implies that everyone should be entitled to receive the same treatment before the law and that there should be no discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation; cultural, religious and linguistic diversity are to be respected; right of children, the elderly and persons with disabilities have to be enforced effectively by adopting concrete and specific measures.[43]

Equality may be threatened by emerging security technologies in different ways. First, unequal treatment or discrimination may stem both

[43] Art. 20-26.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

from the technology's operational capabilities and/or from its "governance", *i.e.* the decisions concerning when and how to employ it. In the former sense, unequal or discriminatory treatment against individuals or groups is the direct consequence of the way an emerging technology for security is designed (Hildebrandt, 2008). For example, one may think about technologies that use personal characteristics, information or behavioral patterns to determine whether an individual may represent a security threat (Guzik, 2009). If such a determination is based on individual's race, colour, ethnic or social origin, genetic features, religion or belief etc., and entails *per se* a disadvantageous treatment, one may say that the principle of equality is infringed (Norris, 2003). However, it is also possible that apparently neutral or objective criteria, such as specific movements, are used as classifiers, which in practice would disproportionally affect the specific individuals or groups.

Again, experience regarding the impact on the value of equality, and the right to equal treatment, generated by the deployment of security technologies seems to confirm the plausibility of the above concerns. For example, as it was pointed out with regard to image body scanners, their use, which produces "naked images", may result in direct discrimination. Concerns about respect of the value and right to equal treatment between individuals and groups have also been raised by biometrics as well as data mining technologies (Cantore, 2011; Hildebrand, 2008).

In light of the above, emerging security technologies should be designed in a way that inhibit or limit the possibility to process sensitive data (*data protection by design*), *i.e. data* «revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life»; they

should be designed by taking in to consideration the specific needs of people with particular disabilities and that may be negatively affected.

5.5 Solidarity

"Solidarity" is another fundamental value on which the European Union is funded. According to the Charter of Fundamental Rights of the EU, solidarity may be realised through the enforcement of some specific social rights.[44] Two of these rights are particularly relevant with regard to emerging security technologies. They are the individual's rights to have ensured a high level of human health and environment protection.[45]

As far as the former right is concerned, it entails to protect individuals from possible or established negative effects emerging technologies may have on their health. These effects may originate both from the materials/substances that are employed to build a concerned technology and the effects generated by its use. Developers and manufactures should ensure that their products not only meets but also exceeds established safety standards to account for unexpected factors. The employment of new technologies should be based on a preliminary assessment of possible health risks both for users and for any other individuals that may be affected by these technologies.

[44] Art. 27-38.

[45] Art. 35 and 37.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

It is clear that safety is paramount and a lack of safety measures could have severe consequences also with regard to the "life" of a certain technology. Safety concerns have been already raised with regard to different types of "new" materials and technologies, like nano- and biotechnologies. In addition, technologies that emit radiations may represent a potential threat to individual health. Speaking about security technologies, it is worth reminding the case of X-ray body scanners, which use "backscatter" ionized radiation technology, that were deemed too dangerous for passengers' health. Therefore, the EU decided to ban these type of scanners and preferred millimeter-wave scanners that utilize low-energy radio waves.[46]

Further to the potential or established risks for human health, the development and use of emerging security technologies may have a negative impact on the environment. Manufacturing new and emerging technologies will of course need materials and energy, which in themselves may present a new environment burden or hazard. Furthermore, the components such technologies consist of could be highly polluting or the provision of the raw materials that are necessary in the manufacturing of such components may entail severe intervention on the planet hearth (mining, drilling, and interferences with eco-systems). These aspects should be monitored and assessed.

[46] Cf. http://www.forbes.com/sites/daviddisalvo/2011/11/15/europe-bans-airport-body-scanners-over-health-and-safety-concerns/.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

5.6 Democracy

The EU is funded on the value of democracy that implies individuals' active and equal participation to the decision-making process (Shapiro, 2005, 10, 35). The EU's embodied notion of democracy emphasises the features of civility, mutual respect, and open-mindedness through which debate and critical examination leads to a fuller understanding of issues and a more reflective set of preferences. This aspect of democracy is valuable because it corresponds to a society in which open and uncensored debate leads to the formation of individual and collective preferences and embodies the ideas of democratic equality among citizens (Sen, 1999). In turn, democracy provides the natural environment for the protection and effective realization of fundamental rights. Equality, freedom and the respect for the principle of the rule of law have both been identified as important characteristics of democracy.

As pointed out by the European Court of Human Rights – that is the monitoring body of the European Convention of Human Rights, to which the EU Charter is linked[47] –, a democratic society is based on "pluralism", "tolerance", "broadmindedness", "equality", "liberty", "right to fair trial", "freedom of expression, assembly and religion".[48] The Charter of Fundamental Rights of the EU then specifies that the value of democracy in the EU entails acknowledging and enforcing citizens' rights: to vote and stand as a candidate at elections to the European Par-

[47] Art. 52.

[48] *Cf.*, for example, ECtHR, 13.02.2003, *Refah Partisi (the Welfare Party) v. Turkey*, Judgment, available at http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-60936.

liament and at municipal elections; to good administration; of access to documents; to petition, freedom of movement and residence; to receive diplomatic and consular protection, to consult and receive redress from the European Ombudsman.[49]

Over the past decade, interest in the relationship between democracy and security technologies has grown up among scholars and practitioners. The main object of their debate has been the democratic procedure in making decisions about security technologies (Sclove, 1999). Nevertheless, they have omitted the equally important question of whether security technologies are *substantively* democratic – that is, whether their design and use is compatible with the value of democracy (Sclove, 1995, 26-33). As it was argued: «Technological innovations are similar to legislative acts or political foundings that establish a framework for public order that will endure over many generations. For that reason the same careful attention one would give to the rules, roles, and relationships of politics must also be given to such things as the building of highways» (Winner, 1989).

In theory, an emerging security technology may be deemed democratic if it enables individuals and groups to participate fully in political and social life. It is democratic if it does not contribute in establishing authoritarian relationships between individuals or support illegitimately hierarchical power relations between groups and organizations (Sclove, 1995); if it is not vulnerable to catastrophic sabotage that may represent a risk for democratic institutions and individuals rights; finally, if promo-

[49] Art. 29-36.

tes tolerance and justice. The above said is the theory; what does it imply in practice?

To be democratic, emerging security technologies should *at least* be designed in a way they do not allow for arbitrary, illegal and not proportional interference with freedom of information, freedom of speech, of assembly, and the right to privacy (Petri, 2008). Democracy means respect for individuals' freedom of information, *i.e.* their right to hold and impart information as well as their right to know. Enforcing these rights entails allowing citizens to develop personal political opinions and to adopt political decisions. Nevertheless, democracy also means safeguarding individual's freedom of speech and freedom of assembly, as well as fostering their participation in public life. Finally, democracy means respect individuals privacy, *i.e.* their autonomy and decisional power, as well as to protect their personal data, especially those that are sensitive (*e.g.* political opinions). Indeed, if individuals are aware or feels that such kind of information may be routinely collected for security purpose they may refrain from participating to the social and political life.

In light of the above, it is paramount to make emerging security technologies "democratic" by technological design. For example, by limiting the possibility that surveillance technologies may collect and process information revealing political opinions (Data Protection-by Design).

5.7 Rule of Law

The principle of the rule of law, or the supremacy of the law, requires a system of governance based on non-arbitrary rules. In other words, it requires the government to exercise its power in accordance with well-

established and clearly written rules, regulations, and legal principles. The Charter details the principle of the rule of law in its last Title, "Justice".[50]

On the one hand, laws are used for the regulation of technologies; on the other, they allows the use of technologies to pursue established goals, among which (national) security. However, technologies may change the contents of protected legal interests. They can contribute in modifying the notion of some fundamental rights as it has been the case of the right to privacy, whose content has been transformed by the rise of ICT (Cassano, 2001). In other word, the change in technologies influences the change in the law; and the rules regulating new technologies are shaped by the features characterizing such technologies.

6. Conclusions

The development and adoption of new technological solutions can foster the security of the European Union, its Member States, as well as of European communities and citizens. Security is a fundamental and overarching societal value that should be preserved and pursued. Threats to security are not simply physical threats to individuals, institutions, infrastructures or assets; they are also threats to societal core values of peace and liberty, to the socio-economic well-being of a given community as well as to its traditions, shared experiences, organic, dy-

[50] Art. 47-50.

namic and collective life. Therefore security extends beyond the material aspects of the physical protection and gives attention to the actual resilience and robustness of a community and in general in its confidence, trust, economic stability and growth, and territorial cohesion. Furthermore, it seems obvious that no fundamental rights can be fully enjoyed without a secure environment. In other words, security is a prerequisite for enjoying human rights and civil liberties. It should anyhow not be forgotten that a primary and very core aim of any security policies or practices is to safeguard the human being. Respect for individuals' fundamental rights is thus an essential element of any security policy or practice.

The development and employment of emerging technologies for security promise benefits, but also have the potential for novel risks, not just in the domain of traditional environmental, health, and safety risks, but also broader ethical, fundamental rights and socio-economic risks and impacts.[51] Their development and future adoption tend to destabilize existing norms, institutions and power relationships (Allenby, 2011, 7). Their complexity often exceeds the capacity of governance institutions and, in general, of large part of society, to understand them. The problem is also exacerbated by the rapid pace these technologies develop and the uncertainties surrounding the outcome of their development, as well as their possible utilisation. In a context of great uncertainty, foreseeing and governing the effects of emerging security technologies

[51] Actually, technologies may have impact on technologies too (Twiss, 1992, 56; Bijker, 1997).

on a given legal, political, environmental system, and, in particular, on individuals' fundamental rights and values before they are actually adopted is a very hard task. The issues raised by one specific emerging technology in one context could well be different from those raised by the same technology but used in a different context. Each case needs to be considered on its merits. Since it is difficult to foresee the exact context an emerging technology ends up to be employed, targeting all the ethical, societal and fundamental rights issues maybe very complicated. Furthermore, although it seems clear that carrying out an ethical, societal and fundamental rights impact assessment roughly entail to establish the likely effects a concerned emerging security technology has on individual rights, values and society, a sound methodology(ies) for such a difficult assessment has yet to be established.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

References

Allenby, B.R. (2011), *Governance and Technology Systems: The Challenge of Emerging Technologies*, in Marchant, G.E. (2011), B.R. Allenby and J.R. Herkert (Eds), *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight*, Dordrecht: Springer.

Aquilano, N.J., R.B. Chase and F.R. Jacobs (2005), *Operations Management for Competitive Advantage*, New York: McGraw-Hill-Irvin Series.

Armstrong, J.S. (ed.) (2001), *Principles of Forecasting: a Handbook for Researchers and Practitioners*, Norwell: Springer.

Bigo, D. & J. Jeandesboz (2010), *The EU and the European Security Industry Questioning the "Public-Private Dialogue"*, 5, http://aei.pitt.edu/14989 (consultato il 2 Ottobre 2016).

Bijker, W. E., T.P. Huges, and T. Pinch (Eds) (1997), *The Socio Construction of Technological Systems*, Cambridge: MIT Press.

Bloustein, E.J. (1964), *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, in *New York University Law Review*, 39, pp. 962–1007.

Bonfanti, M.E. (2014), *From Sniffer Dogs to Emerging Sniffer Devices for Airport Security: An Opportunity to Rethink Privacy Implications?*, in *Science and Engineering Ethics –Special Issues on Human Security*, pp. 791-807

Bonfanti, M.E. (2011), *Il diritto alla protezione dei dati personali come riconosciuto dal Patto internazionale sui diritti civili e politici e dall'art. 8 della Convenzione europea dei diritti dell'uomo: similitudini e difformità di contenuti*, in *Diritti Umani e Diritto Internazionale*, 5(3), pp. 437-481.

Burgess, J.P. (2012), *The Societal Impact of Security Research*, in *Prio Policy Brief*, 9, http://file.prio.no/Publication_files/Prio/Burgess-Societal-Impact-Policy-Brief-9-2012.pdf (consultato il 2 Ottobre 2016).

Buyse, A. (2016), *The Role of Human Dignity in ECHR Case-Law*, in *ECHR Blog*, 21 October 2016, at http://echrblog.blogspot.ch/2016/10/the-role-of-human-dignity-in-echr-case.html (consultato il 2 Ottobre 2016)

Cantore, D. (2011), *On Biometrics and Profiling: A Challenge for Privacy and Democracy?*, in *International Journal of Technoethics*, 2(4), pp. 84-93.

Cassano, G. (2001), *Internet e riservatezza*, in G. Cassano, *Internet. Nuovi problemi e questioni controverse*, Milano: Giuffrè, pp. 9-18.

Clapham, A. (1993), *The "Drittwirkung" of the Convention*, in MacDonald R.St.J, F. Matscher, H. Petzold (eds), *The European System for the Protection of Human Rights*, Dordrecht/Boston/London: Martinus Nijhoff, pp. 163-206.

Eberle, E. (1998), *Human Dignity, Privacy, and Personality in German and American Constitutional Law*, in *Utah Law Review*, 4, pp. 964-1056.

Donnelly, J. (2009), *Protecting Dignity: An Agenda for Human Rights, Research Project on Human Dignity: "Human Dignity and Human Rights"*, University of Denver, pp. 14-35, http://www.udhr60.ch/report/donnelly-HumanDignity_0609.pdf (consultato il 2 Ottobre 2016).

Dupré, C. (2014), *Art. 1 – Human Dignity*, in S. Peers, T. Hervey, J. Kenner, A. Ward (Eds.). *The EU Charter of Fundamental Rights. A Commentary* (1st ed.), pp. 3-38, Croydon: Hart Publishing.

Glensy, R.D. (2011), *The Right to Dignity*, Drexel University Earle Mack School of Law Research Paper No. 2011-W-01, http://www3.law.columbia.edu/hrlr/hrlr_journal/43.1/Glensy.pdf (consultato il 2 Ottobre 2016).

Gogarty, B. (2008), *Unmanned Vehicles, Surveillance Saturation and Prisons of the Mind*, in *Journal of Law, Information and Science*. Special Edition: *The Law of Unmanned Vehicles*, 19, pp. 73-145.

Guzik, K. (2009), *Discrimination by Design: Predictive Data Mining as Security Practice in the United States' War on Terrorism'*, in *Surveillance and Society*, 7(1), pp. 1-17.

Hildebrandt, M. (2008), *Profiling and the Rule of Law*, in *Identity in Information Society*, 1, pp. 55-70.

Lebech, M. (n.d.), *What is Human Dignity?* http://eprints.nuim.ie/392/1/Human_Dignity.pdf (consultato il 2 Ottobre 2016).

Maack, J.N. (2001), *Scenario Analysis: a Tool for Task Managers*, http://siteresources.worldbank.org/EXTSOCIALDEV/Resources/3177394-1167940794463/ScenarioAnalysisMaack.pdf (consultato il 2 Ottobre 2016).

Makridakis, S.G. S.C. Wheelwright, R.J. Hyndman (1998), *Forecasting: Methods and Applications*, III Ed., New York: Wiley.

Marshall, J. (2009), *Personal Freedom through Human Rights Law? Autonomy, Identity and Integrity*, Leiden: Martinus Nijhoff.

McHugh, P.J. (2006), *Negative and Positive Freedom – An Introduction*, http://www.tere.org/assets/downloads/secondary/pdf_downloads/ALevel/NegativePositiveFreedom.pdf (consultato il 2 Ottobre 2016).

Meyer, M.J. (2002), *Dignity as a (Modern) Virtue*, in Kretzmer D. and E. Klein (ed.), *The Concept of Human Dignity in Human Rights Discourse*, The Hague: Kluwert Law International.

Mordini, E. (2012), *New Security Technologies and Privacy, in Ethical and Regulatory Challenges to Science and Research Policy at the Global Level*, pp. 14-30, Luxembourg: EC DG Research and Innovation.

Murphy, M.C. and M.R. Wilds (2001), *X-Rated X-Ray Invades Privacy Rights*, in *Criminal Justice Policy Review*, 12(4), p. 333–343.

Norris, C. (2003), *CCTV, the Panopticon, and the Technological Mediation of Suspicion and Social Control*, in Lyon D. (Ed.), *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*, London: Routledge, pp. 249-281.

Nys, T. (2004), *Re-Sourcing The Self? Isaiah Berlin and Charles Taylor and the Tension Between Freedom and Autonomy*, 14(4), pp. 215-227.

Petri, T. (2008), *The User Perspective – Democracy and the Citizen: Criteria for Security Technologies*, 4 http://www.prise.oeaw.ac.at/docs/Democracy_and_the_Citizen_-_Criteria_for_Security_Technologies_-_Thomas_Petri.pdf (consultato il 2 Ottobre 2016).

Porter, A.L., A.L. Roper, T.W. Manson, F.A. Rossini, J. Banks, B.J. Wiederholt (1991), *Forecasting and Management of Technology*, New York: Wiley.

Schachter, O. (1983), *Human Dignity as a Normative Concept*, in *American Journal of International Law*, 77, pp. 848-854.

Shapiro, I. (2005), *The State of Democratic Theory*, Princeton: Princeton University Press.

Schermer, B.W. (2007), *Software agents, surveillance, and the right to privacy: a legislative framework for agent-enabled surveillance*, Leiden: Leiden University Press.

Sen, A. (1999), *Democracy as a Universal Value*, in *Journal of Democracy*, 10(3), pp. 3-17.

Sclove, R.E. (1995), *Democracy and Technology*, New York and London: The Guilford Press.

Sclove, R.E. (1999), *Democratic Politics of Technology: The Missing Half. Using Democratic Criteria in Participatory Technology Decisions*, at http://www.loka.org/idt/intro.htm (consultato il 2 Ottobre 2016).

Smith, M. (2013), *Resist the Surveillance Drones, a threat to Freedom of association!*, http://solanopfp.blogspot.it/2013/04/resist-surveillance-drones-threat-to.html (consultato il 2 Ottobre 2016).

Twiss, B.C. (1992), *Forecasting for Technologists and Engineer: A Practical Guide for Better Decisions*, London: Peregrinus.

Vanston, J.H. (1998), *Technology Forecasting: An Aid to Effective Technology Management*, Austin: Technology Future Inc.

Whitman, J.Q. (2004), *The Two Western Cultures of Privacy: Dignity Versus Liberty*, in *Yale Law Journal*, 113, pp. 1151-1221.

Winner, L. (1989), *The Whale and the Reactor: A Search for Limits in an Age of High Technology*, Chicago: University of Chicago Press.

Wright, R.G. (2006), *Dignity and Conflicts of Constitutional Values: The Case of Free Speech and Equal Protection*, in *San Diego Law Review*, 43, pp. 527-576.

Zedner, L. (2008), *Epilogues: the Inscapabable Insecurity of Security Technologies*, in Aas, K.F., H.O. Gundhus, H.M. Lomell, *Technologies of Insecurity: The Surveillance of Everyday Life*, 2008, pp. 219-237.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno VII, n. 2, 2017
data di pubblicazione: 15 settembre 2017

Saggi

Abstract

Let's Go for New or Emerging Security Technologies!… What About Their Impact on Individuals and the Society?

Technological innovation is embraced as an unquestionable component of the EU's security policies which promote the development and employment of "new", "advanced", "next generation" or "emerging" technologies for countering security threats. The same policies call also for the assessment of the impact emerging technological tools may have on individuals' values, their fundamental rights, and the society as a whole. With regard to technologies that are "emerging", this assessment should occour at R&D stage, and aim at establishing the likely effects the technologies may have on the above values, rights, and the society. It should estimate to what extent their potential employment comply with the principles of a democratic society and the rule of law. As such, it is a very wide-ranging and complex form of investigation. The proposed paper examines the benefits stemming from an ex-ante impact assessment of emerging technologies for security. It argues that anticipatory thinking on ethical, fundamental rights and societal implications of emerging technologies is paramount to identify and mitigate possible negative effects as well as fully exploit all the benefits the concerned technologies may generate. It then discusses a methodology for investigating the ethical, fundamental rights and societal implications generated by the adoption of emerging technological solutions.

Keywords: Security; Technology; Fundamental Rights; EU; Impact Assessment.