



European Group on  
Ethics in Science and  
New Technologies  
to the European Commission

# Ethics of Security and Surveillance Technologies

Brussels, 20 May 2014

Jim Dratwa  
*Chief Editor*  
*Head of the EGE Secretariat*

# 28

Opinion N°





# OPINION OF THE EUROPEAN GROUP ON ETHICS IN SCIENCE AND NEW TECHNOLOGIES TO THE EUROPEAN COMMISSION

---

## **Ethics of Security and Surveillance Technologies**

No 28

20/05/2014

*Reference: Request from President Barroso*

*Rapporteurs: Inez de Beaufort, Linda Nielsen, Siobhán O'Sullivan*

---

THE EUROPEAN GROUP ON ETHICS IN SCIENCE AND NEW TECHNOLOGIES (EGE),  
Having regard to the Treaty on European Union, and in particular Article 6 of the common  
provisions concerning respect for fundamental rights,

Having regard to the Treaty on the functioning of the European Union, and in particular  
Article 16 concerning the right to the protection of personal data,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular  
Article 1 (Human dignity), Article 3 (Right to the integrity of the person), Article 6 (Right to  
liberty and security), Article 7 (Respect for private and family life), Article 8 (Protection of  
personal data), Article 10 (Freedom of thought, conscience and religion) Article 11 (Freedom  
of expression and information), Article 20 (Equality before the law), Article 21 (Non-  
discrimination), Article 42 (Right of access to documents), Article 47 (Right to an effective  
remedy and to a fair trial), Article 48 (Presumption of innocence and right of defence) and 52  
(Scope of guaranteed rights) thereof<sup>1</sup>,

Having regard to the Universal Declaration of Human Rights, in particular Articles 7,8,10, 11,  
12 and 14<sup>2</sup>,

Having regard to the European Convention of Human Rights (ECHR), in particular Article 5  
'Right to liberty and security' and Article 8 'Right to respect for private and family life'<sup>3</sup>,

Having regard to the International Covenant on Civil and Political Rights, in particular Articles  
14, 17, 18 and 19<sup>4</sup>,

Having regard to Article 6 of the Seventh Framework Programme of the European Union for  
research, technological development and demonstration activities (2007-2013), which states  
that 'All the research activities carried out under the Seventh Framework Programme shall be  
carried out in compliance with fundamental ethical principles',

---

<sup>1</sup> Official Journal C 364 of November 2000, pp. 1- 22

<sup>2</sup> <http://www.worldservice.org/udhr.html#12>

<sup>3</sup> [http://www.echr.coe.int/Documents/Convention\\_ENG.pdf](http://www.echr.coe.int/Documents/Convention_ENG.pdf)

<sup>4</sup> <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>

Having regard to the Council of Europe Convention on Human Rights and Biomedicine, signed on 4 April 1997 in Oviedo<sup>5</sup>,

Having regard to the Council of Europe Convention on Cybercrime signed on 23 November 2001 which provides for modern and flexible means of international co-operation,<sup>6</sup>

Having regard to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, signed on 28 January 2003<sup>7</sup>,

Having regard to 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<sup>8</sup> (Framework Directive),

Having regard to Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities<sup>9</sup> (Access Directive),

Having regard to Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services<sup>10</sup> (Authorisation Directive),

Having regard to Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services<sup>11</sup> (Universal Service Directive),

Having regard to the Convention for the Protection of Human Rights and Fundamental Freedoms, 213 U.N.T.S. 222, entered into force Sept. 3, 1953, as amended by Protocols Nos 3,5,8 and 11 which entered into force on 21 September 1970, 20 December 1971, 1 January 1990 and 1 November 1998 respectively, especially Article 8- Right to respect for private and family life<sup>12</sup>,

Having regard to Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector,

---

<sup>5</sup> <http://conventions.coe.int/Treaty/en/Treaties/Html/164.htm>

<sup>6</sup> <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

<sup>7</sup> <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>

<sup>8</sup> OJ L 108, 24.4.2002.

<sup>9</sup> OJ L 108, 24.04.2002.

<sup>10</sup> OJ L 108, 24.04.2002

<sup>11</sup> OJ L 108, 24.04.2002.

<sup>12</sup> <http://www1.umn.edu/humanrts/instreet/z17euroco.html>

Having regard to the Council Regulation (EC) 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States<sup>13</sup>,

Having regard to the Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas COM (2004) 835 final,

Having regard to Directive 2006/24/EC of the European Parliament and of the Council of March 15, 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of communications networks and amending Directive 2002/58/ECV,

Having regard to the 'Communication from the Commission to the European Parliament and the Council- An area of freedom, security and justice serving the citizens' (Stockholm programme) COM (2009) 262/4,

Having regard to the European Council (March 2010) *Internal security strategy for the EU. Towards a European security model*<sup>14</sup>,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,

Having regard to the Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441<sup>15</sup>,

Having regard to the Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data<sup>16</sup>,

---

<sup>13</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0001:0006:EN:PDF>

<sup>14</sup> [http://www.consilium.europa.eu/uedocs/cms\\_data/librairie/PDF/QC3010313ENC.pdf](http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ENC.pdf)

<sup>15</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML>

<sup>16</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF>

Having regard to the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters<sup>17</sup>,

Having regard to the Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM (2013) 847, 27.11.2013<sup>18</sup>,

Having regard to the Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA<sup>19</sup>,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data,

Having regard to the Proposal for a regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country national crossing the external borders of the Member States of the European Union COM (2013) 95<sup>20</sup>,

Having regard to the Proposal COM(2013) 107 final 2013/2014 (COD) for a Decision of the European Parliament and of the Council establishing a space surveillance and tracking support programme<sup>21</sup>,

Having regard to Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation for all citizens<sup>22</sup>,

Having regard to the European Parliament Resolution (2010/2154(INI)) of 6 July 2011 on aviation security, with a special focus on security scanners<sup>23</sup>,

Having regard to the Council Resolution of 17 January 1995 on the lawful interception of telecommunications (96/C329/01)<sup>24</sup>,

---

<sup>17</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:01:EN:HTML>

<sup>18</sup> [http://ec.europa.eu/justice/data-protection/files/com\\_2013\\_847\\_en.pdf](http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf)

<sup>19</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF>

<sup>20</sup> [http://ec.europa.eu/dgs/home-affairs/doc\\_centre/borders/docs/1\\_en\\_act\\_part1\\_v12.pdf](http://ec.europa.eu/dgs/home-affairs/doc_centre/borders/docs/1_en_act_part1_v12.pdf)

<sup>21</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0107:FIN:EN:PDF>

<sup>22</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:en:PDF>

<sup>23</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:033E:0125:0134:EN:PDF>

<sup>24</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996G1104:EN:HTML>

Having regard to the European Parliament Resolution of 23 October 2008 on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection (2010/C 15 E/14)<sup>25</sup>,

Having regard to the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (EUROSUR) COM(2011) 873 final,<sup>26</sup>

Having regard to the Communication COM(2011) 670 final from the Commission to the Council and the European Parliament setting up an Aviation Safety Management System for Europe<sup>27</sup>,

Having regard to the Commission Regulation (EU) No 573/2010 of 30 June 2010 amending Regulation (EU) No 185/2010 laying down detailed measures for the implementation of the common basic standards on aviation security<sup>28</sup>,

Having regard to the Commission Regulation (EU) No 358/2010 of 23 April 2010 amending Regulation (EU) No 185/2010 of 4 March 2010 laying down detailed measures of the implementation of the common basic standards on aviation security<sup>29</sup>,

Having regard to the Commission Regulation (EU) No 72/2010 of 26 January 2010 laying down procedures for conducting Commission inspections in the field of aviation security<sup>30</sup>,

Having regard to Commission Regulation (EC) No 915/2007 of 21 July 2007 amending Regulation (EC) No 622/2003 laying down measures for the implementation of the common basic standards on aviation security<sup>31</sup>,

Having regard to the Commission Regulation (EU) No 297/2010 of 9 April 2010 amending Regulation (EC) No 272/2009 supplementing the common basic standards on civil aviation security<sup>32</sup>,

Having regard to the Commission Regulation (EU) No 1254/2009 of 18 December 2009 setting criteria to allow Member States to derogate from the common basic standards on civil aviation security and to adopt alternative security measures<sup>33</sup>,

---

<sup>25</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:015E:0071:0072:EN:PDF>

<sup>26</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0873:FIN:EN:PDF>

<sup>27</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0670:FIN:EN:PDF>

<sup>28</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:166:0001:0005:EN:PDF>

<sup>29</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:105:0012:0014:EN:PDF>

<sup>30</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:023:0001:0005:EN:PDF>

<sup>31</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:200:0003:0004:EN:PDF>

<sup>32</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:090:0001:0003:EN:PDF>

<sup>33</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:338:0017:0017:EN:PDF>

Having regard to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Schengen governance—strengthening the area without internal border control<sup>34</sup>,

Having regard to the Communication COM(2009)262/4 from the Commission to the European Parliament and the Council. An area of freedom, security and justice serving the citizen<sup>35</sup>,

Having regard to the EU 'Smart Borders' initiative to replace the manual stamping of passports of third country nationals with an automated electronic registry to monitor the stay of these visitors<sup>36</sup>,

Having regard to the Communication COM(2010) 673 final from the Commission to the European Parliament and the Council: The EU Internal Security Strategy in Action: Five steps towards a more secure Europe<sup>37</sup>,

Having regard to the Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System (June 2013)<sup>38</sup>,

Having regard to the Commission Staff Working Document *Towards a European Strategy for the Development of Civil Applications of Remotely Piloted Aircraft Systems (RPAS) September 2012*<sup>39</sup>,

Having regard to the Communication from the Commission to the European Parliament and the Council Rebuilding Trust in the EU-US Data Flows, COM (2013) 846 final,

Having regard to the Special Eurobarometer 359- 'Attitudes on Data Protection and Electronic Identity on the European Union from June 2011'<sup>40</sup>,

Having regard to the Special Eurobarometer 390- 'Cyber Security' from July 2012<sup>41</sup>,

Having regard to the US *Review Group on Intelligence and Communications Technologies 2013*,

Having regard to the *Ernst & Young Fighting to close the gap. Global Information Security Survey 2012*<sup>42</sup>,

---

<sup>34</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0561:FIN:EN:PDF>

<sup>35</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0262:FIN:en:PDF>

<sup>36</sup> [http://europa.eu/rapid/press-release\\_IP-11-1234\\_en.htm](http://europa.eu/rapid/press-release_IP-11-1234_en.htm)

<sup>37</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF#page=2>

<sup>38</sup> [http://ec.europa.eu/enterprise/sectors/aerospace/files/rpas-roadmap\\_en.pdf](http://ec.europa.eu/enterprise/sectors/aerospace/files/rpas-roadmap_en.pdf)

<sup>39</sup> <http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INI&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>

<sup>40</sup> [http://ec.europa.eu/public\\_opinion/archives/ebs/ebs\\_359\\_en.pdf](http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf)

<sup>41</sup> [http://ec.europa.eu/public\\_opinion/archives/ebs/ebs\\_390\\_en.pdf](http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf)



Having regard to the Opinion No. 26 Ethics of Information and Communication Technologies of the European Group on Ethics in Science and New Technologies (22 February 2012),<sup>43</sup>

Having regard to 'Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices'<sup>44</sup>,

Having regard to the Report of the Committee on Civil Liberties, Justice and Home Affairs (LIBE) on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs,

Having regard to the Open Round Table organised on the topic of the Ethics of Security and Surveillance Technologies on 18 September 2013 in Brussels,

Having regard to the contributions from the EGE open consultations on ethics of security and surveillance,

Having heard the EGE Rapporteurs, Inez de Beaufort, Linda Nielsen, Siobhan O'Sullivan,

HEREBY ADOPTS THE FOLLOWING OPINION:

---

<sup>42</sup>[http://www.ey.com/Publication/vwLUAssets/Fighting\\_to\\_close\\_the\\_gap:\\_2012\\_Global\\_Information\\_Security\\_Survey/\\$FILE/2012\\_Global\\_Information\\_Security\\_Survey\\_\\_\\_Fighting\\_to\\_close\\_the\\_gap.pdf](http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf)

<sup>43</sup> [http://ec.europa.eu/bepa/european-group-ethics/docs/publications/ict\\_final\\_22\\_february-adopted.pdf](http://ec.europa.eu/bepa/european-group-ethics/docs/publications/ict_final_22_february-adopted.pdf)

<sup>44</sup> <http://www.privacybydesign.ca/content/uploads/2013/01/operationalizing-pbd-guide.pdf>



## Table of Contents

Introduction .....	17
I.1. Scope of the Opinion.....	17
I.2. What is meant by Security? .....	19
I.3. What is meant by Surveillance? .....	19
I.4. EU Political Actions and the Stockholm Programme .....	20
Chapter 1 Security and Surveillance Technology Applications.....	25
<b>1.1. Telecommunications</b> .....	26
<b>1.2. Information and Communication Technology</b> .....	28
<b>1.3. Location and Tracking Technologies</b> .....	35
<b>1.4. Technology Characteristics</b> .....	38
1.4.1. Miniaturisation.....	38
1.4.2. Ubiquity .....	41
1.4.3. Automation .....	42
<b>1.5. Convergence of technologies</b> .....	43
<b>1.6. Drivers of Technology</b> .....	43
1.6.1. Social Drivers .....	44
1.6.2. Political Drivers .....	44
1.6.3 Economic Drivers .....	44
<b>1.7. Limits of technology</b> .....	45
<b>1.8. Technology Lock-in</b> .....	46
<b>1.9. Privacy Enhancing Technologies</b> .....	47
<b>1.10. Challenges</b> .....	48
Chapter 2 Governance – overview, challenges, possibilities .....	49
<b>2.1. The regulatory landscape in the area of security and surveillance</b> .....	49

<b>2.2. Human Rights</b> .....	50
2.2.1. Human Rights and Privacy .....	51
2.2.2. Security as justification to limit privacy.....	54
2.2.3. Security as a self-standing human right.....	55
<b>2.3 Surveillance regulation</b> .....	58
2.3.1. Jurisprudence .....	58
2.3.2. Surveillance cameras – CCTVs .....	59
2.3.3. Telecommunications surveillance.....	65
<b>2.4. Specific Regulatory Areas</b> .....	67
2.4.1. Data protection .....	67
2.4.2. Aviation security, border control, cybercrime .....	70
2.4.3. Whistle-blowing.....	74
2.4.4. Drones.....	76
<b>2.5. Regulatory concerns, challenges and possibilities?</b> .....	82
2.5.1. How are the ethical principles balanced in the regulatory landscape? .....	82
2.5.2. Is more regulation needed? .....	83
2.5.3. How should the global challenges be dealt with? .....	85
2.5.4. Which governance possibilities should be considered – the “tool-box”? .....	86
<b>Chapter 3 Ethical analysis</b> .....	89
<b>3.1. Historical and socio-political perspectives</b> .....	89
3.1.1. The evolution of the concept of security.....	89
3.1.2. The tensions structuring/pervading the notion of Security .....	97
<b>3.2. Ethical Concerns, Considerations and Concepts</b> .....	99
3.2.1. Security, surveillance, fear and control .....	99
3.2.2 Control, security, protection .....	102
3.2.3. Public and private .....	104
<b>3.3. Ethical principles</b> .....	105

Chapter 4 On the Notion of Trade-Off .....	115
<b>4.1. Balancing rights</b> .....	116
<b>4.2. The trade-off between security and freedom</b> .....	118
<b>4.3. The trade-off between growth and freedom</b> .....	118
<b>4.4. Alternative to the trade-offs?</b>	
<b>'Positive-sum' or 'win-win' paradigms</b> .....	121
<b>4.5. Alternative to the trade-offs?</b>	
<b>Lessons from privacy based upon notice and consent</b> .....	122
<b>4.6. Going beyond the trade-off: <i>Any person – and any society – that would sacrifice freedom for security deserves neither</i></b> .....	125
<b>Recommendations</b> .....	<b>131</b>





European Group on  
Ethics in Science and  
New Technologies  
to the European Commission

OPINION OF THE EUROPEAN GROUP ON ETHICS IN SCIENCE  
AND NEW TECHNOLOGIES TO THE EUROPEAN COMMISSION

# Ethics of Security and Surveillance Technologies

*Reference:* Request from **President Barroso**  
*Rapporteurs:* **Inez de Beaufort, Linda Nielsen,**  
**Siobhán O'Sullivan**

**Jim Dratwa**  
*Chief Editor*  
*Head of the EGE Secretariat*

# 28

Opinion N°





# Introduction

## I.1. Scope of the Opinion

On 21 March 2011 President José Manuel Barroso requested the EGE to draft an Opinion on the ethical implications of information and communication technologies and to produce, subsequently and separately, an Opinion on the ethical implications of security technologies, with due attention given to the development of security technologies and to surveillance technologies. The EGE has provided the Commission with its Opinion on *Ethics of Information and Communication Technologies* on 22 February 2012. It also drafted an Opinion on Research, Production and Use of Energy that was published on the 16th January 2013, in response to an intervening request from the President of the Commission. The present Opinion addresses the issues of security and surveillance technologies from an ethical perspective. As the group prepared the report, the revelations of Edward Snowden emphasised how important a reorganisation and reinterpretation of our approach to security and surveillance is. Indeed the predicament of data flows and surveillance activities thrown into sharp relief by these revelations form part of the evolving backdrop against which this Opinion is set<sup>45</sup>.

*National security* is the responsibility of the Member States, but the Lisbon Treaty, and particularly the Charter of Fundamental Rights embedded in it provides for action by the Union where necessary to protect the rights of individual citizens. In addition, the EU shares competence with member states as regards the internal security of the Union and has established an Internal Security Strategy to identify and coordinate action against common threats. In this opinion we address the manner in which surveillance has been enhanced due to the availability of new technologies and the means to record and analyse and retain vast amounts of data provided by advances in information and communication technologies.

While *national security* or *state security* paradigms pertain to a state's ability to defend itself against external threats, the notion of *human security* holds that the referent for security is the individual rather than the state. This is to be considered against the backdrop of the forms of security expected from the Westphalian nation-state<sup>46</sup> (with the social contract on which it is premised calling upon the state to ensure the security of its citizens) and against

---

<sup>45</sup> <http://www.theguardian.com/world/the-nsa-files>

<sup>46</sup> Peace of Westphalia, 1648

the backdrop of an increasing technologically mediated attention to border control as well as to the 'enemy within'.

Security procedures lie within the compass of the State that in addition may procure services from national or international companies to provide the facilities for collection and management of information that the security services require. Information gathered about individuals or organisations may then be held either by the State, where democratic accountability ought to exist, or by private entities where the conditions for handling sensitive material may not be in the public domain and may possibly be retained or may not be only used for the purposes of a particular State. **The Opinion addresses the principles by which these forms of surveillance should be governed.**

In addition, surveillance of the public by companies or by other individuals should be subject to conditions, and again, **the opinion addresses the principles that govern these forms of 'commercial' or individual surveillance**, and the manner in which the data so gathered may be used as part of a data mining or profiling system by private entities or the state.

The digital revolution and subsequent advances in mobile, wireless and networked devices have significantly contributed to the development of security and surveillance technologies. New technologies offer the possibility of recording the everyday activities of billions of individuals across the globe. Our mobile phones can identify and pinpoint our location at any given moment, loyalty cards allow commercial entities to analyse our spending and track our personal preferences, keystroke software monitors our performance and productivity in the workplace and our electronic communications can be screened for key words or phrases by intelligence services. Moreover, personal data concerning our health, employment, travel and electronic communications are stored in databases, and data mining techniques allow for large amounts of personal data from these disparate sources to be organised and analysed, thereby facilitating the discovery of previously unknown relationships within these data. Security technologies are no longer discrete; the trend is toward convergence, creating more powerful networked systems. Thus, our everyday lives are scrutinised by many actors as never before, all made possible by developments in technology together with political choices or lack thereof.

## **I.2. What is meant by Security?**

From a definitional perspective 'security' is a peculiar notion, at one and the same time the object of an easy, familiar and immediate understanding and also a paragon of Gallie's<sup>47</sup> "essentially contested concept". Indeed, labouring within this seeming familiarity is a set of important tensions and oppositions, historically and socio-politically entrenched, which illuminate the ethical stakes pertaining to security and which are further discussed in Chapter 3.

As a heuristic initial shortcut, and for the purpose of this introduction, security can be defined as "protecting people and the values of freedom and democracy, so that everyone can enjoy their daily lives without fear"<sup>48</sup>.

## **I.3. What is meant by Surveillance?**

As is the case for security, the notion of surveillance comes to us with a rich and textured layering of meaning. Its common definition is that of close observation, especially the act of carefully watching a suspected spy or criminal or a place where an incident may occur.

It comes from the French verb *surveiller* "oversee, watch" (16<sup>th</sup> century), from *sur-* "over" and *veiller* "to watch", from Latin *vigilare*, from *vigil* "watchful". Interestingly, "surveiller" carried with it from the start a tension between meanings of watching over, of taking care of, and of suspicion and control. It also comprised from the start the complementary notion of watching over oneself and one's own behaviour.

"Surveillance" is first attested in 1768, in an article (in the economic journal *Ephémérides du citoyen*) pertaining to the role of the police on marketplaces, drawing together individuals and the state, public and private interests, law and law enforcement. It is also worthy of note that the word surveillance came to English from the Terror in France: during the French Revolution "surveillance committees" were formed in every French municipality by order of the Convention – pursuant to a law of 21 March 1793 – to monitor the actions and movements of all foreigners, dissidents and suspect persons, and to deliver certificates of citizenship.

---

<sup>47</sup> W.B. Gallie, 'Essentially Contested Concepts', Proceedings of the Aristotelian Society (1956) 167-198 - Paper delivered to the Aristotelian Society on 12 March 1956,

While not all security technologies involve surveillance in a direct way and not all surveillance technologies have security as their stated goal, and while the very terms 'security technologies' and 'surveillance technologies' are attached to dynamics of relabeling which escape stable typologies and definitions, the classic configuration sees surveillance presented as a means with security as an end.

These considerations are further analysed and refined in Chapter 1.

#### **I.4. EU Political Actions and the Stockholm Programme**

With the Lisbon Treaty in force, and building on the Stockholm Programme and its Action Plan<sup>49</sup>, the Commission's 2010 Communication (COM(2010)673)<sup>50</sup> fleshing out the EU's Internal Security Strategy identified what it understands to be the most urgent challenges to EU security in the years to come and thus proposed five strategic objectives and specific actions for 2011-2014 which, alongside ongoing efforts and initiatives, aim to help make the EU more secure:

1. Disrupting international crime networks threatening our society
2. Preventing terrorism and addressing radicalisation and recruitment
3. Raising levels of security for citizens and businesses in cyberspace
4. Strengthening security through border management
5. Increasing Europe's resilience towards crises and disasters

The rationale set out in the Communication is the following:

'Serious and organised crime takes a variety of forms: trafficking in human beings, drugs and firearms trafficking, money laundering and the illegal shipment and dumping of waste inside and outside Europe. Even seemingly petty crimes such as burglary and car theft, sale of counterfeit and dangerous goods and the actions of itinerant gangs are often local manifestations of global criminal networks. These crimes require concerted European action. Likewise with terrorism: our

---

<sup>48</sup> European Council, 2010, Internal security strategy for the EU. Towards a European security model, 12

<sup>49</sup> After Tampere and The Hague, the Stockholm Programme is the EU's third multi-annual programme for justice and home affairs, covering the period 2010-14. *The Stockholm Programme: An Open and Secure Europe Serving and Protecting the Citizens* (Council Document 17024/09). *Delivering an area of freedom, security and justice: Action plan implementing the Stockholm Programme* (Commission Communication COM(2010) 171).

societies remain vulnerable to the sorts of attacks suffered with the bombings of public transport in Madrid in 2004 and in London in 2005. We must work harder and more closely to prevent new attacks recurring. A growing threat is cybercrime. Europe is a key target for cybercrime because of its advanced Internet infrastructure, the high number of users, and its internet-mediated economies and payment systems. Citizens, businesses, governments and critical infrastructure must be better protected from criminals who take advantage of modern technologies. Border security also requires more coherent action. With common external borders, smuggling and other cross-border illegal activity must be targeted at European level. Efficient control of the EU's external borders is thus crucial for the area of free movement. Furthermore, in recent years we have seen an increase in the frequency and scale of natural and man-made disasters in Europe and in its immediate neighbourhood. This has demonstrated the need for a stronger, more coherent and better integrated European crisis and disaster response capacity as well as for the implementation of existing disaster prevention policies and legislation.'

Taken together, these five issue areas form the EU's current political outline and understanding of its 'internal security' predicament: an increasing and converging set of threats which require more security under the umbrella of a coordinated EU framework. The Internal Security Strategy provides a number of guidelines for action that include an intelligence-driven approach based on dynamic information exchange between law enforcement authorities through the use of EU databases and strengthened cooperation between EU agencies in the Justice and Home Affairs policy field.

To understand the broader picture and the overall framework, it is necessary to refer to the political priorities set out in the Stockholm Programme as adopted in 2009. It is also important to underscore two further elements of context. Firstly, the institutionally entrenched enthusiasm that prevailed in the run-up to and following the entry into force of the Lisbon Treaty. Secondly, the fact that the set-up of the EU institutions (besides the Treaty, notably through Council formations and Commission DG architecture) brought closely together, at the time, "freedom, security and justice".

---

<sup>50</sup> *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe* (Commission Communication COM(2010) 673): <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF>

Therefore, at the very start of the Stockholm Programme, the European Council 'reaffirms the priority it attaches to the development of an area of freedom, security and justice, responding to a central concern of the peoples of the States brought together in the Union' and subsequently 'welcomes the increased role that the European Parliament and National Parliaments will play following the entry into force of the Lisbon Treaty. Citizens and representative associations will have greater opportunity to make known and publicly exchange their views in all areas of Union action in accordance with Article 11 TEU. This will reinforce the open and democratic character of the Union for the benefit of its people.'

As regards the Stockholm Programme's political priorities, this multi-annual programme marked a point of departure with its predecessor (the Hague Programme). No longer does it call for a balance or trade-off to be struck between liberty and security. Rather, the Stockholm Programme put citizens rights front and centre, presenting these two concepts as potentially mutually reinforcing, as follows (emphasis added): 'The European Council considers that the priority for the coming years will be to focus on the interests and needs of citizens. 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*.'

The political priorities set out in the Stockholm Programme are:

1. Promoting citizenship and fundamental rights (giving primacy to the protection of fundamental rights and freedoms. 'Respect for the human person and human dignity and for the other rights set out in the Charter of Fundamental Rights of the European Union and the European Convention for the protection of Human Rights and fundamental freedoms are core values. For example, the exercise of these rights and freedoms, in particular citizens' privacy, must be preserved beyond national borders, especially by protecting personal data. Allowance must be made for the special needs of vulnerable people.')
2. A Europe of law and justice
3. A Europe that protects (calling upon the development of an internal security strategy as discussed above)
4. Access to Europe in a globalised world

5. A Europe of responsibility, solidarity and partnership in migration and asylum matters
6. The role of Europe in a globalised world - the external dimension (highlighting the importance of the external dimension of the Union's policy in the area of freedom, security and justice with due attention to the need for increased integration of these policies into the general policies of the Union and with all other aspects of the Union's foreign policy)

The European Union is currently preparing to set broad policy outlines for justice and home affairs in the coming years – and indeed to set the 'strategic guidelines' foreseen by the Lisbon Treaty – to replace the Stockholm programme, which elapses at the end of 2014.

This Opinion is also particularly timely in that context.

**Further to its Preamble and to these introductory considerations, the present Opinion consists of four chapters and concludes with its Recommendations. The first chapter provides an overview and scrutiny of security and surveillance technology applications; the second chapter delves into the legal and regulatory dimension and presents the governance situation and challenges; the third chapter offers the ethical analysis, encompassing the historical and socio-political perspectives as well as the discussion of the ethical concerns, considerations and concepts; and the fourth chapter scrutinizes and defuses a set of overarching predicaments with regard to the ethics of security and surveillance technologies, leading to the Recommendations.**





## **Chapter 1                      Security and Surveillance Technology Applications**

The digital revolution and subsequent advances in mobile, wireless and networked devices and the programming that drives and links them have significantly contributed to the development of security and surveillance technologies. Radio Frequency Identification tags (RFID), nanotechnology and information technology offer us the possibility of recording the everyday activities of millions of European citizens. Our mobile phones can identify and pinpoint our location at any given moment, loyalty cards allow commercial entities to analyse our spending and track our personal preferences, keystroke software monitors our performance and productivity in the workplace and our electronic communications can be screened for key words or phrases by the intelligence services. Moreover, personal data concerning our health, employment, travel and electronic communications are stored in databases, and data mining techniques allow for large amounts of personal data from these disparate sources to be organised and analysed, thereby facilitating the discovery of previously unknown relationships among the data. Security technologies are no longer discrete; the trend is toward convergence, creating more powerful networked systems. Thus, our everyday lives are scrutinised by many actors as never before, all made possible by developments in technology.

Security and surveillance technologies is something of a misnomer as the technologies elaborated in the following discussion have either been designed specifically for security reasons, or more commonly have been developed for other purposes and laterally found a security and/or surveillance application. Thus, arriving at a specific definition of security technologies is problematic and is inextricably linked to the concept of security which is being evoked. For the purposes of this discussion security technologies are those employed in an effort to provide or enhance the security of people, property and information.

The development and proliferation of security and more specifically, surveillance technologies have been facilitated by advances in a number of scientific domains, most notably in the areas of telecommunications, information and computing as well as location tracking.

## 1.1. Telecommunications

In the last three decades there have been a number of technological changes in the area of telecommunications, not least of which includes a transition to the use of digital signals, fibre optic cables and computer based switching. These changes have led to the introduction of a number of diverse technologies, which have greatly expanded the degree to which the occurrence and content of telecommunications can be monitored. Radio frequency devices have enabled mobile telephony and with it voice, text and video messaging, while fibre optic cables have facilitated high speed Internet connection. The combination of both these technologies allows for wireless computing. One can now connect to the Internet from handheld devices and mobile phones and voice calls can be made from desktop computers using voice over Internet protocols (VoIP) software (such as Skype).

### *Interception of telecommunications*

All of these technologies require the transmission of data which can be captured stored and analysed and linked to other data for security purposes. It has been argued that targeted surveillance and interception of an individual's communications play a vital role in preserving national security, investigating serious criminal activities and even combating terrorism. Manual methods of "wiretapping" telephones such as pen registers (records numbers dialled out) and trap and trace interceptions (records numbers from which incoming calls are dialled) have been replaced by central office switch wiretapping technology operated by remote command, which allows for mass collection of communication data which can be filtered and analysed. Internet communications, whether sending an email, surfing the web or making a phone call using VoIP use Internet Protocol (IP). In IP, the information you transmit is arranged in packets, which be tracked through what are called "packet sniffers." A packet sniffer is similar to a wiretap in that it eavesdrops on telecommunication and can filter information based on source or destination as well as the content of the communication.

These technologies have facilitated States to routinely and on an automated basis, scan all telecommunications of its citizens to identify key words or phrases and to determine when particular online resources are being accessed. Since 2006, the European Data Retention Directive 2006/24/EC, requires telecommunication providers to store communications for a period of 6 months to two years, for the purpose of criminal investigation. In 2012, Microsoft and Skype received a total of 75,378 law enforcement requests for information<sup>51</sup>. Those

---

<sup>51</sup> 2012 Law Enforcement Requests Report, <http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/>

requests potentially impacted 137,424 accounts. Approximately 80% of requests to Microsoft resulted in disclosure of non-content information, while in the case of a small number of requests (2.2%), customer content was also disclosed.

### *Snowden Case*

Transnational State surveillance hit the global headlines in June 2013 with the revelations of former National Security Agency (NSA) contractor, Edward Snowden. A series of leaked documents described the operation of the PRISM programme which allows the systematic interception, storage and analysis of at least 11 different types of electronic communications of non-US citizens from telephone and global Internet companies such as Google, Apple, Microsoft and Facebook by the NSA<sup>52, 53</sup>. It was claimed that the programme facilitated extensive surveillance on stored and real-time communications such as emails, file transfers and web chats, via direct access to companies' servers. Claims of spying by the NSA on world leaders, heads of international aid organizations, directors of the United Nations, foreign energy firms, and the head of the European Union's antitrust division have all been made in documents leaked by Mr. Snowden. Documents also revealed the existence of the TEMPORA programme run by the UK Government Communications Headquarters (GCHQ). It was reported that the UK equivalent of the NSA, has since 2011, had the ability to tap into and store huge volumes of data captured from undersea fibre-optic cables. The documents revealed that interceptors had been placed by GCHQ on 200 fibre optic cables carrying internet traffic between the US and Europe, potentially giving GCHQ access to 10 gigabits of data per second, principally in the form of metadata (connections rather than content). The Guardian newspaper pointed out, that is "equivalent to sending all the information in all the books in the British Library 192 times every 24 hours"<sup>54</sup>. It has been argued that the distinction between content and metadata is not always clear. While metadata generally does not contain personal or content specific details but rather transactional information about the user, it can still reveal sensitive personal information e.g. calls to support hotline for domestic abuse.

---

<sup>52</sup> G. Greenwald, 'NSA collecting phone records of millions of Verizon customers daily' *The Guardian*, 6 June 2013:

<http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order>

<sup>53</sup> B. Gellman and L. Poitras, 'U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program' *Washington Post*, 6 June 2013:

[http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497\\_print.html](http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_print.html)

<sup>54</sup> E. MacAskill et al 'GCHQ taps fibre-optic cables for secret access to world's communications' *The Guardian*, 21 June 2013:

<http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>

## 1.2. Information and Communication Technology

The dramatic growth of powerful computing and communication technologies (ICT) enables the collection, storage and utilisation of vast amounts of personal information, more easily and effectively than ever before. A fundamental enabler of this growth has been the increased availability of cheap and efficient data storage. While storage capacity has increased, the cost of storage has significantly decreased. The volume of personal information being stored in databases has significantly expanded during the last thirty years, due primarily to the explosion of social media data and machine-generated data, such as information from sensors, point-of-sale systems, mobile phone network, Web server logs and the like. According to the Ernst & Young Global Information Security Survey 2012 of 1,850 participants across all industry sectors in 64 countries, the number of organisations using cloud technology has doubled since 2010<sup>55</sup>. This massive adoption of cloud services such as online file repositories, picture sharing and social networks generates enormous volumes of citizen data and metadata data. Multiple data can now be accumulated, tabulated and cross-referenced in large databases for commercial, administrative, medical and judicial purposes. Roger Clarke coined the term *dataveillance* to describe the situation where we are monitored through the data we leave as traces when we use digital media<sup>56</sup>.

### *Data Mining and Data Matching*

Data sets can be matched against each other in order to identify common features or trends in the data. Matching techniques include geo-demographic profiling, where geographic data e.g. post code, internet domain names are connected to demographic data about individuals. There is increasing use of data matching by both public and private organisations in an attempt to reduce fraudulent activity. In an effort to minimise fraudulent social welfare claims Government agencies compare data held across a number of different databases in order to detect similarities or differences between data collected for different purposes, e.g. someone paying income tax and claiming social security at the same time, or a dead person claiming benefits. Financial institutions can match data on accounts, bank cards, credit limits, and average balances in order to assess credit worthiness, thereby reducing their financial risk.

Data Mining enables large amounts of personal data from disparate sources to be organised and analysed, facilitating the discovery of previously unknown relationships amongst the

---

<sup>55</sup>Ernst & Young's 2012 Global Information Security Survey  
[http://www.ey.com/Publication/vwLUAssets/Fighting\\_to\\_close\\_the\\_gap:\\_2012\\_Global\\_Information\\_Security\\_Survey/\\$FILE/2012\\_Global\\_Information\\_Security\\_Survey\\_Fighting\\_to\\_close\\_the\\_gap.pdf](http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey_Fighting_to_close_the_gap.pdf) accessed 24<sup>th</sup> Oct 2013

data. Knowledge Discovery in Databases (KDD) is a heuristic process of data mining which has evolved from the convergence of machine learning, database systems, statistics and artificial Intelligence. KDD is a multi-step process that facilitates the conversion of large data to valid, novel, potentially useful, and ultimately understandable information. Data mining has been used to identify novel adverse drug events in the post approval period and through a drugs life on the market in an effort to improve patient safety<sup>57</sup>. The EU-ADR project is a European Commission funded project which mines clinical data from biomedical databases and electronic healthcare records (EHRs) of over 30 million patients from several European countries for the purposes of the early detection of adverse drug reactions, which should lead to improved drug safety monitoring<sup>58</sup>. It has also been suggested that mining electronic health records has the potential to further medical research as well as clinical care e.g. monitoring treatment adherence<sup>59</sup>. Linking genetic data with electronic health records allows for mapping of genotype-phenotype correlations. One such study identified genetic variants associated with an increased risk of thromboembolism in patients with breast cancer treated with Tamoxifen<sup>60</sup>. Recently data mining has also been employed for epidemic surveillance<sup>61</sup>. Researchers have shown, for example, that “mining” of Twitter postings can be used to track and predict outbreaks of influenza with approximately 90% accuracy.<sup>62</sup>

Increasingly commercial entities are developing business models centred on data mining. There is a move towards understanding the customer at the individual level and leveraging that understanding to provide tailored products and/or services to customers, thereby increasing profitability and customer loyalty. Data mining is used to analyse sales trends and predict the effectiveness of promotions. Market basket analysis employed by the retail industry can find out which products are bought together so that they can be arranged on shelves accordingly. Retail firms and marketing analysts can utilise data mining techniques to better understand customer profiles and behaviour. Data mining can segment customer databases according to demographics, buying patterns, geography, attitudes, and other variables. This builds profiles of the shoppers based on their preferences and allows for more specific marketing to a more select group of consumers. The online retailer Amazon uses multiple sources of data to predict the likely preference of the shopper and “recommends” items to the consumer. The American retailer Target has used predictive analytics to assist in

---

<sup>56</sup> Clarke R 'Communication technology and dataveillance' *Communications of the ACM* 1988;31(5):498-512

<sup>57</sup> Harpaz R *et al* *Clin Pharmacol Ther* 2012;91(6):1010-1021

<sup>58</sup> Coloma PM *et al* *Pharmacoepidemiol Drug Saf* 2011; 20(1):1-11

<sup>59</sup> Jensen PB *et al*. *Nature Rev Gen* 2012;13:395-405

<sup>60</sup> Onitilo A *et al* *Breast Cancer Res Treat* 2009;115:643-650

<sup>61</sup> Kofod-Petersen A. *Med J Aust*. 2012 Mar 19;196(5):301.

effective marketing to pregnant customers. By examining historical purchasing patterns of women who had signed up to baby registries, it was possible to identify approximately 25 products such as vitamin supplements and unscented lotions, which taken together could generate a pregnancy prediction score. Based on the score, women were sent coupons for baby products. This anticipatory direct marketing backfired in the case of one young woman who received such vouchers in the post to her home. Her father contacted the company to express his indignation at the company sending his teenage daughter advertisements for baby paraphernalia. The company made an immediate apology but the man contacted the company a week later to proffer his own apology as his daughter had confided that she was in fact pregnant<sup>63</sup>.

### **Predictive analytics**

Predictive analytics is a subset of data mining which can model complex interactions or relationships from existing information, thereby enabling the identification and characterisation of new relationships and/or to make predictions of future events. The business community has used predictive analytics for many years to anticipate market conditions or trends and to direct sales strategies. More recently, predictive analytics and data mining technologies and techniques are being used by the intelligence, counterterrorism, national security and law enforcement communities.

Time Magazine heralded, “predictive policing” as one of the top 50 best inventions of 2011. Combining and analysing large data sets from disparate sources may allow police forces to anticipate, prevent and respond more effectively to crime. It is argued that allocation of resources and deployment of policing personnel on the basis of such data analysis is a cost effective measure which increases public safety. The term predictive policing brings to mind the short story “The Minority Report” published in 1956 that imagined a future in which individuals would be intercepted and punished before they committed any crime. Predictive policing methods do not identify individuals, rather it enables the identification of trends and patterns; geographically and over time. In complex models of predictive policing, historical information on crimes including location, time of day, weather patterns, proximity to ATMs etc. is combined with real time information and sociological information about criminal behaviour e.g. repeat victimisation and the fact that offenders tend to commit crimes in their own immediate environment. Mathematical modelling can then provide information on the likelihood of a particular crime e.g. a burglary happening in a particular place, a so called “hotspot”. It can also discover new relationships as in the case of stranger rape, where a past criminal history was a reliable predictor but interestingly, predictive analytics uncovered the surprisingly finding that a prior property crime was a better predictor of a stranger rape than a past sexual offence<sup>64</sup>.

Predictive policing has been trialled in the United States of America and more recently in the UK and The Netherlands. When Santa Cruz in California implemented predictive policing in 2011, there was a 27% reduction in burglaries compared to the preceding year. Within four months of introducing predictive policing in the foothill area of Los Angeles in late 2011, crimes were down 13% compared in a 0.4% increase in surrounding areas where the system has not been rolled out<sup>65</sup>. It is difficult to know just how effective predictive analytics are in policing, as the causes of crime are multifactorial and complex and the effect of predictive analytics needs to be separated out from other factors which lower crime, e.g. aging populations. The information generated by predictive analytics is only as good

---

<sup>62</sup> Lampos V et al Proceedings of the 2<sup>nd</sup> IAPR workshop on cognitive information processing IEEE Press 2010:411-416

<sup>63</sup> <http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/>

<sup>64</sup> Coleen McQue Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis 2006 Elsevier / Butterworth-Heinemann

<sup>65</sup> <http://www.predpol.com/results/> accessed 27th August 2013

as the data inputted into the analysis; the more complete the data, the better the predictive power. We know that some crimes such as car theft are more consistently reported than drug related activities and some social groups are more likely to report crimes than others. Concerns have also been raised that this type of analysis could introduce bias into the criminal justice system by perpetuating a self-fulfilling cycle of more arrests in areas identified as hotspots. Judges and jurors might also be more likely to convict suspects active in these high crime areas.

Even more problematic is when prediction moves from places to people. Predictive analytics technology is being used by prison services in the UK in order to identify which offenders are more likely to reoffend once they have been released<sup>66</sup>. Analyses of millions of prisoner files have been used to predict whether offenders with specific problems e.g. drug addiction are more likely to be recidivists than other prisoners. Targeted programmes are then designed to address offender behaviour during their stay in prison with the intention of reducing the probability that they will commit further crimes upon their release. Algorithms have also been developed which estimate the probability that someone on parole or probation will kill within a two year period of being released<sup>67</sup>. Richard Berk, Professor of Criminology and Statistics at the University of Pennsylvania analysed data of over 60,000 cases of those offenders who had already been sentenced or had been released on parole. The algorithm predicted that 1-2% of those on probation or parole would be charged with murder or attempted murder within two years. *"Of the people who will shoot, the algorithm correctly forecasts those outcomes about 75 out of 100 times"*, according Prof. Berk<sup>68</sup>. Assessing the level of "future dangerousness" through software applications is used in sentencing and parole hearings to determine who can be released and subject to what conditions/supervision.

Predictive analytics have also been deployed in the pursuit of border security. Mathematical forecasting has been used to predict which containers entering a port could contain dangerous material or which passengers at an airport should be detained and searched and to identify suspect vehicles at border crossings. Information on vehicle type, ownership and history of crossing borders, as well as geographical and weather conditions are used to construct models which can flag certain vehicles for inspection. Border police can even be provided with information on the most likely risk they will face upon inspection e.g. drugs, weapons<sup>69</sup>. The Department of Homeland Security in the USA has been testing software designed to scan crowds at airport queues to detect nervous or suspicious behaviour such as fidgeting, perspiration and shallow breathing. Predictive analytics, the basis of the future attribute screening technology (FAST) programme is currently running at 78% in detecting mal-intent and 80% on deception<sup>70</sup>. The European Commission is also funding research concerning the detection of abnormal or threatening behaviour under the FP7 Security Programme. The project INDECT is developing advanced and innovative algorithms for human decision support in combating terrorism and other criminal activities, such as human trafficking, child pornography, detection of dangerous situations (e.g. robberies) and the use of dangerous objects (e.g. knives or guns) in public spaces<sup>71</sup>. Similarly, the aim of the ADABTS project is to develop models for abnormal and threat behaviour and algorithms for automatic detection of such behaviour in crowded spaces<sup>72</sup>.

Efforts to statistically forecast terrorism are being pursued, but are complicated by the fact that most predictive models rely on large sets of data<sup>73</sup>. Unlike consumers' shopping habits and financial fraud, terrorism does not occur with enough frequency to enable the creation of valid predictive models. One

<sup>66</sup> [http://www.01.ibm.com/software/success/cssdb.nsf/CS/GREE8F8M82?OpenDocument&Site=default&cty=en\\_us](http://www.01.ibm.com/software/success/cssdb.nsf/CS/GREE8F8M82?OpenDocument&Site=default&cty=en_us) accessed 27th August 2013

<sup>67</sup> Berk R et al. J.R. Statist Soc A 2009;172(1):191-211

<sup>68</sup> <http://www.smartplanet.com/blog/science-scope/in-philadelphia-prediction-and-probability-in-crime-patterns/3598> , accessed 27th August 2013

<sup>69</sup> <http://public.dhe.ibm.com/common/ssi/ecm/en/ytw03024gben/YTW03024GBEN.PDF> accessed 27th August 2013

<sup>70</sup> [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_pia\\_st\\_fast-a.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast-a.pdf) accessed 27th August 2013

<sup>71</sup> <http://www.indect-project.eu/> accessed 27th August 2013

<sup>72</sup> [ftp://ftp.cordis.europa.eu/pub/fp7/security/docs/adabts\\_en.pdf](ftp://ftp.cordis.europa.eu/pub/fp7/security/docs/adabts_en.pdf) accessed 27th August 2013

<sup>73</sup> Jonas J and Harper T. Effective Counterterrorism and the Limited Role of Predictive Data Mining Cato Institute Policy Paper No.584 2006 <http://object.cato.org/sites/cato.org/files/pubs/pdf/pa584.pdf> accessed 27th August 2013



area of counter-terrorism where predictive analytics has the potential to play an important role is in uncovering money laundering activities<sup>74</sup>. Terrorists, their networks and their support structures require funding in some form to exist and operate. Predictive models are capable of detecting unusual or suspicious financial transactions and as the old adage goes, "follow the money" and it can uncover terrorist financing.

Undoubtedly, big data analytics are revolutionising our approach to security and surveillance and offer many potential benefits in an era where the virtual tsunami of information available on almost every aspect of our lives requires new methodologies to make sense of it all. A note of caution however should be sounded. The authors, Cukier and Mayer-Schönberger in their book "Big Data" offer some sage advice against overreliance on data by calling to mind how enamoured Icarus was with his technical power of flight, that he used it improperly and fell into the sea<sup>75</sup>.

### *Biometrics*

Technological innovations in the ICT domain have opened up new possibilities for creating, managing and using identity systems. This includes biometrics which can be defined as any measurable, physical or physiological feature or behavioural trait that can be used to identify an individual or to verify the claimed identity of an individual. Examples of physiological biometrics include fingerprints, hand geometry, the face and the iris of the eye. Behavioural biometrics include voice, keystroke dynamics and gait. The use of DNA as a biometric is attractive from the perspective that it is a unique identifier (except in the case of identical twins) and the structure of a person's DNA is stable over a lifetime<sup>76</sup>. A DNA profile involves the analysis of short tandem repeating sequences (STRs) of non-coding DNA. DNA based identification is mostly used for paternity testing, criminal investigations and forensics. Currently, the use of DNA as a biometric is limited by the fact that automatic, real time recognition is not currently possible. The latest technology allows for the generation of a DNA profile within 90 minutes<sup>77</sup>. The US Department of Defence, along with the U.S. Department of Justice and U.S. Department of Homeland Security under their "Accelerated Nuclear DNA Equipment" programme are funding research to develop technologies that enable automated rapid DNA profiling, for field biometric applications<sup>78</sup>.

### *DNA Profiling*

---

<sup>74</sup> Le Khac NA et al. 2009 International Conference on Computer Engineering and Applications IPCSIT 2011;2:504-509

<sup>75</sup> Mayer-Schonberger V and Kenneth Cukier. Big Data: A Revolution That Will Transform How We Live, Work, and Think (Eamon Dolan/Houghton Mifflin Harcourt, 2013)

<sup>76</sup> Hashiyada Masaki Tohoky Journal of Exp Med 2004;204(2):109-117

<sup>77</sup> <http://integenx.com/integenx-raises-40-million>

<sup>78</sup> <http://biometrics.org/bc2010/presentations/RapidDNA/miles-DHS-Rapid-and-Low-cost-DNA-Biometrics.pdf>



DNA profiling is an important tool in crime detection and can aid in the conviction of those who have committed crimes or conversely can exonerate those who are innocent. A growing number of countries (approx. 60 countries) worldwide operate national DNA databases and databases are being expanded or newly established in at least 34 additional countries<sup>79</sup>. DNA databases differ both in the categories of individuals included in the databases and in the uses permitted of the databases themselves. The National DNA Index (NDIS) in the US contains over 10,581,700 offender profiles, 1,641,400 arrestee profiles and 514,700 forensic profiles as of September 2013<sup>80</sup>. DNA profiles are based on short tandem repeats and do not represent the whole genome sequence. In contrast, DNA samples and the associated whole genome sequence are increasingly being stored in biobanks. Biobanks are recognised as a crucial infrastructure for research and this has led to a significant expansion in the number of population and disease specific biobanks in Europe and globally<sup>81</sup>. The UK biobank which opened its doors to researchers in 2012, currently stores samples and data from 500,000 people<sup>82</sup>.

DNA is different from fingerprint and other biometrics in that it can provide information on ethnicity, predispositions to disease and importantly, can be used to identify other family members. The storage of DNA collected from individuals and the inclusion of computerized DNA profiles on computer databases raises the possibility that as technology advances, far more intrusive tracking and analytical capabilities may be possible. In January 2013, researchers reported that they had identified individuals, and their families, from anonymous DNA data in a research project using information in publically accessible genealogy databases<sup>83</sup>. Thus, DNA is *de facto* identifying and this poses questions in relation to the traditional means of protecting privacy such as coding and anonymisation of data in the field of clinical research.

Everywhere we go, we unwittingly leave behind traces of our DNA in hair, skin cells, saliva and these can potentially be used to determine where you've been, who you've been with, and what you look like; a form of biosurveillance.

Biometrics can be used for *Verification*, where the biometric system authenticates an individual's claimed identity by comparing the sample biometric data with the corresponding enrolled template. This is what is known as a one-to-one comparison. Biometrics can also be

---

<sup>79</sup> Forensic Genetics Policy Initiative <http://dnapolicyinitiative.org/>

<sup>80</sup> FBI CODIS—NDIS Statistics <http://www.fbi.gov/about-us/lab/biometric-analysis/codis/ndis-statistics>

<sup>81</sup> [http://www.eurosfair.prd.fr/7pc/doc/1280153287\\_biobanks\\_eu\\_jrc57831.pdf](http://www.eurosfair.prd.fr/7pc/doc/1280153287_biobanks_eu_jrc57831.pdf)

<sup>82</sup> <http://www.ukbiobank.ac.uk/about-biobank-uk/>

<sup>83</sup> M. Gymrek *et al.* *Science* 2013;339, 321–324

used for the purposes of identification; ascertaining *who* an individual is by comparing the sample biometric with all the templates in a given database, *i.e.* a one-to-many comparison. Biometric data e.g. a fingerprint is collected using a sensor to produce a digital representation of the data, which is linked to the user's identity and stored in the form of numeric data (template) in a database. This template can be compared to the live biometric being presented using a mathematical algorithm, which estimates the degree of similarity between the two templates being compared. Biometric systems, whether used for verification or identification, can be employed in numerous different contexts, for example, security, surveillance and law enforcement, e-commerce, e-government and physical and logical access e.g. children accessing schools.

### *Biometrics and Identification*

More and more governments seek to adopt new technologies like biometrics in order to securitize identities and means of identification e.g. passports and to monitor the movements of people across borders. In 2004, the EU introduced a regulation adopting the inclusion of biometric data into passports for citizens of the EU (except the UK and Ireland) and visas for third country nationals<sup>84</sup>. The regulation required Member States to ensure that all passports issued contain a chip with the holder's facial image and fingerprints by 2006 and 2009 respectively in order to improve document security and prevent falsification of documents. Biometric passports (e-passports) contain a small integrated chip (a radio frequency identification [RFID] chip), embedded in the photo page, which contains a digitised image of the photograph on the passport, fingerprint template, as well as all the additional biographical information visible on the passport.

Within the EU, the Schengen Information System (II), the Eurodac database and the Visa Information System (VIS) are large databases, including biometric data, aimed at controlling migration flows and identifying and sorting legal and irregular migrants. The Eurodac system, which has been operational since 2003, was implemented as a means of comparing the fingerprints of asylum seekers and irregular immigrants throughout the EU (European Union) to determine which Member State is responsible for examining an asylum application. VIS is at the core of the visa application process to the Schengen area and enables Schengen States to store and exchange data relating to visa applications of third-country citizens. In all, 10 fingerprints and a digital photograph are collected from persons over the age of 12

---

<sup>84</sup> Council Regulation (EC) 2252/2004 on standards for security features and biometrics in passports and travel documents <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2004R2252:20090626:EN:PDF>  
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2004R2252:20090626:EN:PDF>

applying for a visa within the EU. This biometric data, along with data provided in the visa application form, is recorded in a secure central database<sup>85</sup>. On 9 April 2013, the Schengen Information System II entered into operation. The SIS II contains data on irregular migrants, lost and false travel documents and wanted or missing persons and stores digital images and biometric data<sup>86</sup>.

Traditionally identity has been confirmed on the basis of an individual's name and, subsequently through the use of identifying documents such as birth certificates, passports and national identity cards. In a globalised world, interconnected through advances in transportation, communication and ICT, there is a greater need for individuals to prove their identity<sup>87</sup>. According to a UNICEF analysis, in 2007 nearly two out of three children in sub-Saharan Africa and South Asia did not have their births registered<sup>88</sup>. The inability to authenticate oneself is important, as it is often a pre-requisite to accessing services e.g. financial services, or exerting rights e.g. voting. There are a number of programs operating in developing countries which aim to "leapfrog" traditional paper-based identity systems by using biometric identification technology<sup>89</sup>. The largest biometric technology project in the world is the nationwide Unique Identification (UID) number system in India<sup>90</sup>. India's Universal ID program seeks to provide a unique identity to all 1.2 billion residents. As of March 31, 2013, the Unique Identification Authority of India (UIDAI) has used the biometrics (10 fingerprints and iris scans of both eyes) to generate a total of 311.9 million unique identifiers, also known also as Aadhaar numbers<sup>91</sup>. By providing a unique number to citizens, the Government hopes to streamline the distribution of welfare and social services.

### 1.3. Location and Tracking Technologies

Emerging Geographical Information Systems (GIS) technologies, such as Radio Frequency Identification (RFID) and the Global Positioning System (GPS) allow us to pinpoint and track the location of people and commodities. There are a vast array of navigation and tracking

---

<sup>85</sup> Proposal for a regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas. Com (2004)835

<sup>86</sup> [http://europa.eu/rapid/press-release\\_MEMO-13-309\\_en.htm](http://europa.eu/rapid/press-release_MEMO-13-309_en.htm) ; [http://europa.eu/rapid/press-release\\_MEMO-13-309\\_en.htm](http://europa.eu/rapid/press-release_MEMO-13-309_en.htm)

<sup>87</sup> Mordini E and Massari S. Bioethics 2008;22(9):488-498

<sup>88</sup> [http://www.unicef.org/protection/files/Progress\\_for\\_Children-No.8\\_EN\\_081309%281%29.pdf](http://www.unicef.org/protection/files/Progress_for_Children-No.8_EN_081309%281%29.pdf)

<sup>89</sup> Alan Gelb and Julia Clark. Center for Global Development. Working Paper 315 Jan 2013.

[http://international.cgdev.org/sites/default/files/1426862\\_file\\_Biometric\\_ID\\_for\\_Development.pdf](http://international.cgdev.org/sites/default/files/1426862_file_Biometric_ID_for_Development.pdf)

<sup>90</sup> Jacobsen EKV. *Security Dialogue* 2012; 43(5): 457-474

<sup>91</sup> <http://pib.nic.in/newsite/erelease.aspx?relid=94946>

systems available but principally they rely on the techniques of triangulation, proximity sensing and scene analysis<sup>92</sup>.

### *Global Positioning System*

Global Positioning System (GPS) is a worldwide radio-navigation system formed from the constellation of 31 satellites and their ground stations. It was developed by the Department of Defence in the US during the 1970's and was fully operational by the mid-1990s. GPS technologies facilitate the collection of location information by enabling devices (mobile phones, vehicles, electronic mapping devices, etc.) to be pinpointed accurately using reference data taken from various sources, most notably GPS location referencing radio signals received from satellites orbiting the Earth. This is done through triangulation, matching three or more separate signals from a selection of the tracking satellites. The GPS receiver uses the signal from a fourth satellite to determine altitude, allowing a determination of position in three dimensions. Data is continuously transmitted by the GPS satellites to the GPS receiver which collects and stores this data. Increasingly, "active" devices are equipped with a communication module e.g. GSM which continuously communicate their present location to a third party allowing for real-time tracking of the GPS device from another location.

Most mobile phones can be set to be active location tracking devices. GPS devices come standard on most new mobile phones, to allow for the phones to be tracked in emergency situations. Using GPS data from a child's mobile phone, parents can not only pinpoint the location of their child at any given moment but they can also be alerted when their child strays out of a given area pre-defined by the parent<sup>93</sup>. Bracelets fitted with GPS and mobile phone technology are being distributed to aid workers working in conflict areas where there is a risk of kidnap. The bracelet can be triggered manually when an aid worker comes under threat, or if the bracelet is forcefully removed. The bracelets issue the wearer's real-time GPS location so rescue teams can identify the location and time of the attack<sup>94</sup>.

As well as monitoring the location the people, GPS technology allows for tracking of objects and commercial goods. A number of car manufacturers including Ford, Volvo and BMW have developed emergency assistance systems based on GPS technology. The system can alert emergency services when an airbag deploys in the car, thereby allowing the emergency

---

<sup>92</sup> Hightower J and Borriello G. Computer 2001;34(8):57-66

<sup>93</sup> <http://news.verizonwireless.com/news/2006/06/pr2006-06-12.html>

<sup>94</sup> "Smart bracelet protects aid workers." BBC News. <http://www.bbc.co.uk/news/technology-22038012>

services to quickly locate the vehicle and provide any medical assistance necessary<sup>95</sup>. GPS can also notify the car owner by phone or e-mail when the car alarm is triggered, and indicate the location of the car<sup>96</sup>.

### *Radio Frequency Identification*

Radio Frequency Identification (RFID) technology involves reading and transmitting wireless radio waves with transponders (tags) and readers (transceivers). RFID tags are either passive or active: passive tags do not have their own power supply and derive their energy from the radio waves transmitted by the reader; active tags contain their own battery and can generate their own radio waves. Information stored on an RFID tag can be read remotely in a contactless system. The maximum operating distance (i.e. the range) between the FID reader and the tag varies from a few centimetres to tens of metres<sup>97</sup>. This range depends on a number of factors such as the frequency being used, the power of the reader, sources of radio interference and objects in the environment that might reflect or absorb radio waves.

The original aim of these small low cost devices was to enable companies to keep track of stock. Retailers such as Tesco, the world's third largest grocery retailer uses RFID tags to help improve stock control systems and track stock through the supply chain. Since 2003, Metro Group in Germany has been running an RF ID-enabled "Future Store," where RFID technology is used for various applications throughout the supply chain<sup>98</sup>.

Animals, including pets and livestock have been implanted with RFIDs in order to track information on ownership and immunisation records and to provide the traceability of livestock needed to ensure food safety. Pets (currently restricted to cats, dogs and ferrets) travelling within Member States in EU are required to have "pet passports" and the pet is connected to the passport by an implanted RFID tag. The purpose of the passport is to protect citizens from the threat of rabies and certain other animal borne diseases<sup>99</sup>.

Recent developments in the area of RFID have seen the technology expand from its role in industrial and animal tagging applications, to being implantable in humans. This has led to fears of "*Ubervveillance*", a term coined in 2006 referring to an omnipresent electronic surveillance facilitated by technology that makes it possible to embed surveillance devices in

---

<sup>95</sup> [http://www.euroncap.com/rewards/ford\\_sync\\_emergency\\_assistance.aspx](http://www.euroncap.com/rewards/ford_sync_emergency_assistance.aspx)

<sup>96</sup> <http://www.techlila.com/trace-stolen-car-using-mobile-phone-technologies/>

<sup>97</sup> Hodges S and McFarlane D (2005). Radio frequency identification: technology, applications and impact. Auto-ID Labs White Paper Series, Edition 1. <http://www.autoidlabs.org/uploads/media/AUTOIDLABS-WP-HARDWARE-016.pdf><http://www.autoidlabs.org/uploads/media/AUTOIDLABS-WP-HARDWARE-016.pdf>

<sup>98</sup> Wamba SF AND Boeck H. Journal of Theoretical and Applied Electronic Commerce Research 2008;3(1):92-105

the human body<sup>100</sup>. In 2004, the U.S. Food and Drug Administration (FDA) approved an RFID tag for implantation into the humans arm called VeriChip, which would allow healthcare professionals to access a person's medical history in the event the person couldn't communicate. The highest profile example of its application came in 2004 when the Mexican Attorney General and 18 of his staff had chips implanted; not for healthcare purposes but and rather to access high security areas in their place of work<sup>101</sup>. In October 2011 PositiveID, announced that it received an order for its VeriChip microchip to be used for disaster preparedness and emergency management by the Israeli Military<sup>102</sup>. Research is currently ongoing to assess if ingestible RFIDs can be used to monitor a patient's drug dosage and compliance<sup>103</sup>, while recent studies have investigated the use of RFID technology as an aid in forensic dental identification, by placing a small transponder in teeth<sup>104</sup>. The technology is not without its critics, and yet it has been suggested that implantable RFIDs devices should be inserted into "vulnerable" citizens such as children, those suffering from dementia and mental illness in an effort to protect them from external dangers, while at the same time there have been calls for migrant workers and criminals with a special emphasis on paedophiles, to be tagged in order to protect 'us' from 'them'<sup>105</sup>.

#### 1.4. Technology Characteristics

Irrespective from which domain security and surveillance technologies have emerged, they share a number of common characteristics namely miniaturisation, automation and ubiquity.

##### 1.4.1. Miniaturisation

The technological achievements in electronic miniaturisation since World War II have transformed the world and given birth to miniaturised sensors and micromechanical devices. Since 1960 we have witnessed an exponential shrinking of electronic components as famously predicted by Gordon Moore in 1965. The old adage "Small is beautiful" could have been coined specifically for technology, as in this sector small equates to fast, cheap and profitable. Smaller devices are generally faster as the signal does not have as far to travel within the device. The miniaturisation of devices has also facilitated the incorporation of

---

<sup>99</sup> [http://ec.europa.eu/food/animal/liveanimals/pets/ganda\\_en.htm](http://ec.europa.eu/food/animal/liveanimals/pets/ganda_en.htm)

<sup>100</sup> Michael MG *et al.* *Computer Communications* 2008;31(6): 1192-1198.

<sup>101</sup> <http://www.spychips.com/press-releases/mexican-implant-correction.html>

<sup>102</sup> <http://finance.yahoo.com/news/PositiveID-Corporation-pz-3900073790.html>

<sup>103</sup> Rajogopakan H and Rahmat-Samii Y. Antennas and Propagation Society International Symposium (APSURSI), 2010 IEEE pg 1-4.

<sup>104</sup> Nuzzolese E *et al.* *Open Dent J* 2010;4:33-36.

<sup>105</sup> Implantable devices raise a number of ethical issues, for a fuller discussion of these, see EGE opinion Opinion n°20 - 16/03/2005 - Ethical aspects of ICT Implants in the Human Body

multiple functions in a single device which has in turn driven down the cost as market penetration is greater for these devices. Personal computers and tablets, smart phones enabled with GPS and cameras have created extensive new markets through miniaturisation. Doubts have however been expressed that we are reaching the physical limits of miniaturisation and that Moore's law (doubling of the number of components on a computer chip in an 18 month period) will not hold beyond 2020 unless nanotechnology steps in to revolutionise current technology<sup>106</sup>. The development of micro- and nano-sensors depends on the further evolution of nanomaterials and nanostructured materials. Inorganic nanowires and nano-crystals exhibit unique electrical and optical properties which can be exploited for sensing. Nano-sensors, already under development, offer the potential to detect processes or events previously undetectable. Nano-sensors have a number of potential applications, including diagnosis and treatment of disease, detection of environmental pollutants, early warning systems in detecting threats to infrastructure as well as security applications (see box below). It is considered technically feasible to deploy and network nano-sensors in many of these fields by 2020<sup>107</sup>.

#### **Nanosensors**

Nanosensors have been in development for almost a decade and can be defined as sensors constructed using nanoscale components, which convey information about nanoparticles to the macroscopic world. These sensors can be manufactured to detect differences in volume, speed, gravity, electrical charge, chemical composition, pressure, temperature or any number of other physical changes.

Nanosensors can be broadly classified into three different areas based on what they sense. Physical nanosensors measure properties like mass, pressure, force while chemical sensors determine the identity or concentration of a chemical substance. Biosensors are used to monitor processes at the molecular level such as cellular communication and antigen/antibody interactions and are sometimes considered as a subset of chemical sensors. Nanosensors can be manufactured in a number of different ways; the three most commonly used methods are top-down lithography, bottom-up assembly and molecular self-assembly. The top down approach involves breaking larger materials into smaller objects; the bottom-up approach employs self-assembly to build up nanostructures by bring individual atoms and molecules together. Molecular self-assembly can be done in one of two ways. The first of these methods uses previously created or naturally occurring nanostructures as the base and immerses it in free atoms which create a larger nanostructure. Alternatively, one begins with a complete set of components which automatically assemble themselves into a nanosensor, a much more difficult proposition than the aforementioned method of self-assembly.

Nanosensors are ultra-sensitive and their small size and potentially low cost means that they can be widely deployed. This makes them ideally suited to applications in the areas of health, security and the environment. The sensing range of a single nanosensor is limited, thus research efforts are underway

---

<sup>106</sup> <http://www.techspot.com/news/48409-physicist-predicts-moores-law-will-collapse-in-about-10-years.html>

<sup>107</sup> Rand Technical Report: The Global Technology Revolution 2020, in-depth analyses. 2006  
[http://www.rand.org/content/dam/rand/pubs/technical\\_reports/2006/RAND\\_TR303.pdf](http://www.rand.org/content/dam/rand/pubs/technical_reports/2006/RAND_TR303.pdf)



to develop an integrated nanosensor device with communication capabilities which should expand the fields of application for nanosensors<sup>108</sup>.

Nanosensors linked to GPS systems allow for real time monitoring of soil and crop conditions. Information gleaned from the autonomous sensors in fields can provide information on soil temperature and moisture content allowing for intelligent decisions to be made in relation to harvesting crops and irrigation management. Winemakers in drought struck Australia have utilised nanosensors to control and monitor production of grapes for fine wine. Nanosensors also have the ability to detect microbial or chemical contamination of a crop and nano-devices are envisaged which could deliver treatment in the early stages of disease<sup>109</sup>.

One of the biggest growth areas for nanosensors has been in the development of biosensors with the aim of early disease diagnosis and better treatment. Highly sensitive biosensors could detect prognostic and predictive biomarker levels earlier in disease stages, distinguish between favourable and unfavourable outcomes of tumours, and guide further disease treatment. Biosensors can be used to monitor glucose levels in diabetics, nitric oxide levels in exhaled air in asthmatics and could be useful as a tool in drug discovery<sup>110</sup>.

Nanosensors also have a role to play in monitoring the integrity of infrastructure. Micro-mechanical systems (MEMS) and carbon nanotube sensors have been embedded into concrete blocks and beams in order to monitor temperature and moisture content, and to detect cracks forming inside the concrete. Signals are transmitted wirelessly so that early warning systems can be put in place regarding the infrastructural integrity of roads, buildings and bridges that might find themselves under strain during adverse conditions, e.g. earthquakes, hurricanes<sup>111</sup>.

Nanosensors have a number of defence and security applications. Chemical and biological nanosensors can be used to detect chemical/biological weapons in concentrations as low as a single molecule. To detect very small amounts of chemical vapours carbon nanotubes, zinc oxide nanowires or palladium nanoparticles are used in nanotechnology-based sensors. These detecting elements work on the basis of changing the electrical characteristics when gas molecule strikes them. With these sensors a few gas molecules are sufficient to change the electrical properties of the sensing elements and hence the detection or monitoring is easy even with a very low concentration of chemical vapours. The SnifferSTAR is a nano-enabled chemical sensor which can be integrated into a micro unmanned aerial vehicle. The UAV provides a mobile chemical detection platform that can be used on either a military battlefield or in civilian applications, and serves as an early warning indicator of chemical warfare attack<sup>112</sup>. Scientists at NASA have developed a small chip about the size of a postage stamp which holds 32 nanosensors, each capable of detecting a different chemical substance. Civilian applications are also envisaged, with plans to place the chemical nanosensors in smart phones so that levels of carbon monoxide and methane could be monitored in people's homes<sup>113</sup>. Material scientists in Germany have developed a nanosensor which detects trace explosives. Currently, the most common methods for identifying trace explosives are ion mobility spectrometry, mass spectrometry and gas chromatography. All three methods are time consuming and require expensive, bulky instrumentation which limits their deployment at strategic locations, e.g. airports. Scientists at TU-Darmstadt have developed a nanosensor capable of detecting a single molecule of pentaerythritol tetranitrate (PETN), an explosive which has been frequently employed by

---

<sup>108</sup> Usibe BE *et al.* International Journal of Materials Engineering 2013;3(1):4-10

<sup>109</sup> Misra AN *et al.* Int J Pure Appl Sci Tech 2013;16(2):1-9

<sup>110</sup> Agrawal S and Prajapati R. Int J of Pharmaceutical Sciences and Nanotechnology 2012;4(4):1528-1535

<sup>111</sup> Saafi M *et al.* J. of Materials and Structural Integrity 2010;4(1):1-24

<sup>112</sup> <http://www.sciencedaily.com/releases/2003/01/030127074837.htm> accessed 11th November 2013.

<sup>113</sup> <http://gizmodo.com/5881097/this-is-nasas-cancer-sniffing-cellphone-sensor/> accessed 11th November 2013.



terrorists including the "underpants bomber" in 2009. It has been suggested that x ray machines at airport security checks could be equipped with such nanosensors to unobtrusively check passengers and their luggage for traces of explosives<sup>114</sup>.

The combination of nanotechnology, wireless sensor networks and MEMS creates a wireless network of nanoscale sensors called motes, so called "smart dust". Persistent surveillance is within reach following the development of "smart dust". Autonomous sensing, computing and communication systems can now be packed into a cubic millimetre (size of a speck of dust) to form the basis of an integrated, widely distributed sensor network<sup>115</sup>. Potential applications envisioned by Kris Pister, who first conceptualised smart dust include defence-related sensor networks such as battlefield surveillance, treaty monitoring, transportation monitoring, and scud hunting. The Smart Dust project at the University of Berkeley led by Pister created a mote measuring the size of a grain of sand in 2002<sup>116</sup>. Scientists at the University of Berkeley and the United States Marines have deployed six motes from a UAV which formed a wireless network, sensing the speed and direction of 142 passing military vehicles and subsequently reported the data to the UAV<sup>117</sup>. Concerns have been raised that with the advent of surveillance equipment invisible to the naked eye, invasion of personal privacy will be easier to achieve in both the public and private domains.

#### 1.4.2. Ubiquity

Ultimately the goal is to make computers ubiquitous by making components smaller and more powerful. So-called ubiquitous computing (also referred to as pervasive computing) promises seamless integration of digital infrastructure into our everyday lives<sup>118</sup>. Ubiquitous computing relies on the convergence of the Internet, advanced electronics and wireless technologies. The goal is to create "smart" things that can explore their environments and communicate with other smart products unobtrusively to provide information and services to their human users. The *physical computing* subdivision of ubiquitous computing has become known as the "internet of things". Technologies such as wireless sensing and RFIDs incorporated into everyday objects allow a shift of information from traditional devices to the physical environment. Everyday objects can be identified, located and controlled *via* the internet. Sensor-based and context-aware systems are becoming readily established in all areas of daily life, ranging from transportation to healthcare and from environmental monitoring to security surveillance. As Weisner, the father of ubiquitous computing has observed, "The most profound technologies are those that disappear. They weave

---

<sup>114</sup> <http://www.sciencedaily.com/releases/2011/07/110726092952.htm>, accessed 11th November 2013.

<sup>115</sup> Anderson M. New Scientist 2013;218(2914):26 Anderson M. New Scientist 2013;218(2914):26

<sup>116</sup> Warneke BA *et al.* Sensors Proceedings of the IEEE 2002;2:1510-1515

<sup>117</sup> Anderson A. The Economist 20th November 2003. <http://www.economist.com/node/2173026> accessed 11th November 2013.

<sup>118</sup> Friedewald M and Raabe O. 2011;28(2):55-65

themselves into the fabric of everyday life until they are indistinguishable from it"<sup>119</sup>. These very characteristics underpin the surveillance capability of this technology. Current surveillance technologies are limited in terms of their reach in monitoring and tracking people. Objects (e.g. roads, floors, doors) embedded with RFID tags and people wearing tagged clothes or carrying smart phones would be "readable" by a wireless network tracking and instantaneously determining the location of individuals and objects of interest in real-time. Privacy advocates are concerned about the "big brother is watching you" aspects of the internet of things while the implications of such extensive integration of computer technology into our everyday lives are not yet clear.

#### 1.4.3. Automation

The enormous quantities of data being generated by technologies applied in the fields of security and surveillance can easily exceed our capability to transmit, process, and use the information effectively, the so called information tsunami. In an effort to derive meaningful information from the data, and in some cases to take action on the basis of the data, many systems have become automated. Since the early 1990's, there has been a proliferation of CCTV cameras and systems in public places, especially in town and city centres. The British Security Industry Authority (BSIA) estimates that there are 4.9 million CCTV cameras in the UK that equates to one camera for every 14 people<sup>120</sup>. Operators struggle with information overload and boredom and CCTV cameras are only effective as long as they have the operator's attention. With the advent of digital cameras, increased storage and processing capacity, automated CCTV surveillance has become a reality.

Automated analysis of CCTV images has been deployed in the area of automated number plate recognition (ANPR); cameras photograph every passing vehicle and software then analyses the photo to identify the license plate. The ANPR system records the time and location and stores this information along with the image and the plate number. Originally the technology was introduced for traffic management on road networks i.e. paying tolls and congestion charges. More recently, it has been used by the police using a camera mounted on their vehicles. This allows the police to match licence plates against a "hotlist" of licence plate numbers which have been entered into the system by virtue of them being from stolen cars or being registered to persons of interest. The latest research in automated surveillance is concerned with recognition of individuals and their intentions<sup>121</sup>. Facial recognition software can automatically analyse video, pick a face from a crowd and identify the individual by

---

<sup>119</sup> Mark Weiser, "The Computer for the Twenty-First Century", *Scientific American*, pp. 94-10, September 1991

<sup>120</sup> <http://www.bsia.co.uk/cctv>

comparison with a database of known faces. The person can then be tracked from camera to camera across wide geographical areas without any human intervention. Automated cameras can also be programmed to identify "suspicious behaviour" or "threats" e.g. an individual entering a restricted access zone or unattended luggage in an airport. This is done by modelling "normal" behaviour and the degree of deviation from the model defines an action or person as deviant. For a discussion on autonomous drones see pg. 75.

### 1.5. Convergence of technologies

The advances we have seen in security and surveillance technologies in the last decade are largely dependent upon the convergence of disciplines such as information technology, nanotechnology, material technology and biotechnology. Integration and cross-functionality of technologies has now become the rule rather than the exception. Consumers can now make calls, access emails, browse the internet, take pictures and get directions all from their smart phone. The persistent trend toward convergence is set to endure; technical foresight exercises predict that the technology of 2020 *"will continue to integrate developments from multiple scientific disciplines in a convergence that will have profound effects on society"*<sup>122</sup>.

### 1.6. Drivers of Technology

The question of whether technological innovation in the area of security and surveillance has/is being stimulated by scientific discoveries (push) or market demand (pull) is difficult to answer. Undoubtedly there have been a number of new developments in this area as outlined above, however some critics have made the point that these technologies are simply looking for problems to solve, rather than responding to a genuine need. Widespread introduction of surveillance technologies such as CCTV, the security benefits of which are modest<sup>123</sup> is one such example. Similarly, it has been argued that the automated and systematic collection of citizen's data by government security agencies is driven by the fact that the information is available and can be stored in an affordable manner<sup>124</sup>. Increasing interoperability has also been identified as a technological driver as the ability to link numerous systems makes it more attractive to those procuring systems<sup>125</sup>. David Lyon has

---

<sup>121</sup> Adams AA and Ferryman J. Security Journal 2013 pp. 1-18. ISSN 1743-4645 doi: 10.1057/sj.2012.48

<sup>122</sup> *Ibid* 40

<sup>123</sup> Welsh BC, Farrington DP. Effects of closed circuit television on crime. Campbell Systematic Review 2008. [http://www.campbellcollaboration.org/news\\_/CCTV\\_modest\\_impact\\_on\\_crime.php](http://www.campbellcollaboration.org/news_/CCTV_modest_impact_on_crime.php)  
[http://www.campbellcollaboration.org/news\\_/CCTV\\_modest\\_impact\\_on\\_crime.php](http://www.campbellcollaboration.org/news_/CCTV_modest_impact_on_crime.php)

<sup>124</sup> Scientific American June 2013 <http://www.scientificamerican.com/article.cfm?id=how-are-the-nsa>

<sup>125</sup> SAPIENT Smart Surveillance State of the Art 2012 <http://www.sapientproject.eu/docs/D1.1-State-of-the-Art-submitted-21-January-2012.pdf> <http://www.sapientproject.eu/docs/D1.1-State-of-the-Art-submitted-21-January-2012.pdf>

argued that the perception of technology as infallible acts as a driver in the introduction of surveillance systems as the public are more accepting of systems not prone to human error. He specifically cites the introduction of biometrics and the increasingly reliance of governments on biometrics to verify identities<sup>126</sup>.

As noted by the authors of the SAPIENT report<sup>127</sup>, quite apart from technological drivers, there are also social, political and economic drivers of the increasing ubiquity of security and surveillance technologies.

#### 1.6.1. Social Drivers

Citizens can be drivers of security and surveillance technologies as it can be seen as a mechanism for keeping ourselves and our children safe and secure. Reports of crime, violence and conflict sow fear and anxiety about personal security. Lyon has discussed this driver in terms of “perceived risk” and the public’s desire for “zero risk”<sup>128</sup>, while Furedi has asserted that a culture of fear is driven by risk perception, “fears about the future are linked to anxieties about problems today”, problems perhaps borne of living in uncertain times (a fuller discussion of fear and trust can be found on pg. 97).

#### 1.6.2. Political Drivers

The political system justifies the introduction of security and surveillance technologies by reference to its obligation to protect citizen’s security and to meet the demands of citizens to feel safe (see discussion on the social contract pg. 88). The proposed introduction of the European System of Border Surveillance has been justified on the basis that it will help prevent irregular border crossings and reduce irregular migration, thereby improving the European Union’s internal security<sup>129</sup>. Co-operation with other governments or authorities can also drive the introduction of new technologies; the introduction of biometric passports in Europe was in large part as a response to the US requirement for this technology to allow entry of European citizens into the US without a visa.

#### 1.6.3 Economic Drivers

Economics is another key driver of the development and introduction of security and surveillance technologies. As part of the Horizon 2020 framework, the EU has allocated €1.6

---

<sup>126</sup> Lyon D Bioethics 2008;22(9):499-508

<sup>127</sup> *Ibid* 48

<sup>128</sup> *Ibid* 49

<sup>129</sup> <http://ec.europa.eu/immigration/tab3.do?subSec=16&language=7>Sen

million for security research for the period 2014-2020. The global surveillance and security market is estimated to be worth \$81 billion per year and individual country markets are growing at a rate of 7-9% per year. Of this, \$11 billion is spent by the military/governments<sup>130</sup>. Worldwide revenue from video surveillance equipment is expected to rise from \$9.6 billion in 2010 to \$20.5 billion in 2016. By 2014, the global market for network based video surveillance will surpass that for analogue<sup>131</sup>. The global market for smart surveillance and video analytics is predicted to increase from \$13.5 billion in 2012 to \$39 billion by 2020<sup>132</sup>. In addition, new civilian markets are sought for technologies developed for military use, the increasing civilian applications for drones is a case in point. An additional factor in the dissemination of security and surveillance technologies is cost reduction which has accelerated consumer uptake. Fingerprint recognition is now the most popular biometric for accessing laptops, mobile phones and PDAs since low cost, small fingerprint sweep sensors can be easily embedded in these devices.

### 1.7. Limits of technology

Increasing requirements for security in many sectors of our society have generated a tremendous interest in biometrics and have raised expectations of biometric technologies. In a recent survey 81% of European citizens polled were in favour of using biometrics in criminal investigations despite the fact that those polled “lack a thorough understanding of the benefits and applications of biometrics technology in their everyday lives”<sup>133</sup>. No biometric recognition system is 100 per cent accurate and all biometric systems are susceptible to a number of different errors, for example, failure to enrol, failure to acquire, false accept error and false reject error. Biometric systems and technologies are vulnerable to both intrinsic failures and failures due to external attacks. Intrinsic failures are associated with the overall system recognition performance, i.e. system errors while adversary attacks are intentional efforts to access or circumvent the system illegitimately through the use of vulnerabilities in the design system e.g. spoofing (circumvention by an impostor). In 2011, the Dutch Minister

---

<sup>130</sup> “Surveillance and Security Equipment: Technologies and Global Markets” (Report number SAS015B)2013. [http://www.bccresearch.com/pressroom/sas/industrial-commercial-demand-surveillance-equipment-reach-\\$83.8-billion-2017](http://www.bccresearch.com/pressroom/sas/industrial-commercial-demand-surveillance-equipment-reach-$83.8-billion-2017) , accessed 9<sup>th</sup> Oct 2013.

<sup>131</sup> IMS Research. The World Market for CCTV and Video Surveillance Equipment 2013. [http://www.imsresearch.com/report/CCTV\\_and\\_Video\\_Surveillance\\_Equipment\\_World\\_2013&cat\\_id=130&type=LatestResearchhttp://www.imsresearch.com/report/CCTV\\_and\\_Video\\_Surveillance\\_Equipment\\_World\\_2013&cat\\_id=130&type=LatestResearch](http://www.imsresearch.com/report/CCTV_and_Video_Surveillance_Equipment_World_2013&cat_id=130&type=LatestResearchhttp://www.imsresearch.com/report/CCTV_and_Video_Surveillance_Equipment_World_2013&cat_id=130&type=LatestResearch) , accessed 9<sup>th</sup> Oct 2013.

<sup>132</sup> ReportsNReports. Intelligent Video Surveillance, VCA & Video Analytics: Technologies & Global Market – 2013-2020. 2013. <http://www.prweb.com/releases/intelligent-video/surveillance-vca-va/prweb10565272.htm> accessed 9<sup>th</sup> Oct 2013.

<sup>133</sup> Steria Survey July 2013 <http://www.steria.com/media/press-releases/press-releases/article/81-of-citizens-in-favour-of-biometric-identification-finds-steria-survey/> accessed 10<sup>th</sup> Oct 2013.

of the Interior suspended the database storage of digital fingerprinting for travel documents on the basis that there was a 21% false rejection rate (fingerprints on the system could not be matched to passport holders)<sup>134</sup>. In 2011, it was reported in France that up to 10% of biometric passports were fraudulently obtained<sup>135</sup>. More recently, the biometric technology (fingerprint) on the iPhone 5 was hacked with 48 hours of the phone being launched onto the market<sup>136</sup>.

Intelligence-driven security fuelled by big data analytics is being applied in the areas of cybercrime, fraud and counter-terrorism. Predictive analytics, along with most predictive models and data mining techniques, rely on sophisticated statistical methods, including multivariate analysis techniques such as advanced regression or time-series models. Undoubtedly, predictive analytics is a powerful tool for identifying trends, patterns, or relationships among data; however it does have its limitations. As pointed out by Jeffrey Rosen, even if models could be developed with an accuracy of 99%, that in trying to identify the 19 hijackers involved in the 9/11 attacks in a US population of almost 300 million, 3 million citizens would be identified as potential terrorists<sup>137</sup>.

## 1.8. Technology Lock-in

There is a deeply ingrained attitude that new is better and technology equates to progress. The more a technology is adopted, the more likely it is to be further adopted. It has been argued that this can lead to “lock-in” of incumbent technologies while alternatives are eschewed<sup>138</sup>. Diverse security technologies have been accepted as a universal security enabler by Governments and intelligence agencies. As observed by Ceyhan, in the age of uncertainty “the adoption of electronic identification and surveillance tools is perceived as the ultimate solution for fighting security”<sup>139</sup>. Lyon has argued that in the case of surveillance, the belief in the technology far outstrips the evidence available that the technology is effective in delivering security for citizens. Thus, “the presence of high technology speaks for itself, somehow guaranteeing its own effectiveness”<sup>140</sup>. The case of CCTV is something of a case in point. The efficiency and effectiveness of security technologies (see related discussion on pg. 100 and 111) need to be assessed in light of their actual rather than perceived impact on

---

<sup>134</sup> <https://zoek.officielebekendmakingen.nl/kst-25764-46.html> accessed 10th Oct 2013

<sup>135</sup> <http://www.leparisien.fr/faits-divers/plus-de-10-des-passeports-biometriques-seraient-des-faux-19-12-2011-1775325.php> accessed 10th Oct 2013

<sup>136</sup> <http://www.bbc.co.uk/news/technology-24203929> accessed 10th Oct 2013

<sup>137</sup> Jeffrey Rosen. *The Naked Crowd* (New York: Random House, 2004) pp. 104-107.

<sup>138</sup> Arthur WB. *The Economic Journal* 1989;99(394):116-131

<sup>139</sup> Ceyhan A. *Surveillance & Society* 2008;5(2):102-123

<sup>140</sup> Lyon D. *Surveillance Studies: An overview*. 2007 Cambridge: Polity Press pg 147

provision of security. This evidence-based approach would ensure that we do not adopt an excessive reliance on technology and give room to complementary approaches.

## 1.9. Privacy Enhancing Technologies

Development and deployment of security and surveillance technologies is considered integral to safeguarding the security of Europeans citizens. It can however also impact on the privacy and freedoms that citizens have a legitimate expectation of (see pg xx for a further discussion of privacy).

### *Privacy by Design*

In the early 1990s, the concept of Privacy by Design (PbD) was developed to address the systemic effects of ICT and networked data systems<sup>141</sup>. The central thesis of PbD is that privacy cannot be protected solely through compliance with regulatory instruments; rather, technologies should be designed with privacy in mind from the outset. Instead of bolting on privacy enhancing features, privacy enhancing tools e.g. minimisation of unnecessary data collection, they should be integrated into systems design. The Dutch Data Protection Authority (RGK) and the Information and Privacy Commissioner for the Province of Ontario, Canada (IPC) in a seminal joint paper in 1995 described Privacy Enhancing Technologies (PETs) as a way to enhance the citizens control over their personal data and prevent unnecessary or unlawful processing of their data<sup>142</sup>.

Privacy Impact Assessment has also been suggested as a useful tool for engineers and software developers to help them take into account potential negative consequences of particular elements of a technology design. The FP7 funded PRISE project has recommended that privacy impact assessments should form part of the considerations of funders. This could be a mechanism for ensuring that public money is spent on research which is in line with European values and fundamental human rights<sup>143</sup>.

### *Privacy in Design*

---

<sup>141</sup> <http://privacybydesign.ca/> accessed 12th Oct 2013

<sup>142</sup> Privacy-Enhancing Technologies: The Path to Anonymity (Volume I) 1995  
<http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=329> accessed on 12th Oct 2013

<sup>143</sup> [http://www.prise.oew.ac.at/docs/PRISE\\_Statement\\_Paper.pdf](http://www.prise.oew.ac.at/docs/PRISE_Statement_Paper.pdf) accessed 12th Oct 2013

Privacy in Design is distinct from PbD in that it concerns itself primarily with raising awareness about the processes through which values and norms become embedded in technological architecture. Privacy in design looks at the normativity of structural choices in an effort to promote transparency and protect rights and values of the citizens.

Constructive Technology Assessment (CTA) was developed in The Netherlands and Denmark and "shifts the focus away from assessing impacts of new technologies to broadening design, development, and implementation processes"<sup>144</sup>. CTA rejects the argument that technology is neutral and instead maintains that technologies can be designed, consciously or unconsciously, to open certain social options and close others e.g. algorithms. Thus, the model emphasises the early involvement of a broad array of actors to facilitate learning about technology and its potential impacts. It reminds the various actors that when they are engineering technology they are also engineering society.

#### 1.10. Challenges

Technologies developed and adopted for security and surveillance applications have a number of shared characteristics; they are becoming smaller, increasingly connected, with varying degrees of automation built in and are being deployed in a ubiquitous fashion. However it is the integration or convergence of these developments which will allow the technologies to reach their full potential and societal impact. While regulation of separate functions e.g. in telecommunications or use of DNA in identifying an individual has been possible, the real challenge will be in regulating combined functions. There is a risk with convergent technologies, including those in the security arena, that there will be a time lag in incorporating such technologies into a regulatory system. Equally problematic is the risk at the other end of the spectrum, which involves duplication in regulatory regimes. To avoid both of these scenarios, policy makers and regulators will need to be aware of developments upstream in the technology pipeline.

Deployment of security and surveillance technologies, irrespective of their origins, was once considered the prerogative of the State or its agencies. This is no longer the case with commercial entities and individuals utilising technologies which allow them to survey their customers and neighbours and draw inferences about future behaviour from past actions. Much of this technology is transformative and offers concrete benefits to individuals and larger society. Reaping these benefits are however dependent upon the proven effectiveness of the technology and its proportionate use.

---

<sup>144</sup> Schot J & Rip A. Technology Forecasting and Social Change 1996;54:251-268



## **Chapter 2      Governance – overview, challenges, possibilities<sup>145</sup>**

### **2.1. The regulatory landscape in the area of security and surveillance**

Security and surveillance are topics covered by numerous regulations in very different areas and to a certain extent also different purposes. Security is primarily an issue for Member States, and therefore, there is a vast range of regulatory instruments that have been introduced in individual countries. It will neither be possible nor necessary to address all of this enormous volume of regulation in detail. For the purpose of this opinion it is crucial to focus on the bigger picture and the future regulatory challenges and possibilities.

In this chapter relevant areas of regulation and the purpose and content of this regulation are outlined. In this context some illustrations of interesting regulations, differences and loopholes in the regulation will also be presented. Based on the description of the regulatory landscape and the loopholes, a number of governance concerns and challenges will be introduced. Finally, some governance instruments will be presented as a kind of “toolbox” and some governance possibilities will be presented.

The regulations protecting human rights, including privacy, are primarily the international and European Human Rights Conventions and the EU Charter of Fundamental Rights. Within these instruments, security can serve both to limit the right to privacy as well as feature as a self-standing right of its own. More specific regulations on data protection are embedded in EU regulation and national laws. Regulations regarding security are also found in the EU context covering particular policy areas, such as aviation, border control and cybercrime. When it comes to surveillance the picture is more scattered and uncertain. The use of surveillance cameras (CCTV) and surveillance of telecommunications are covered by national regulations, and some examples will be presented, including some brief comments regarding national security as the legal background for surveillance. Regulatory challenges posed by new technologies such as drones and facial recognition are briefly outlined and trends regarding whistleblowing will be described. Finally, regulatory challenges in

---

<sup>145</sup> The chapter is primarily drafted by the rapporteurs, but Professor Herman Nys has provided parts of the text, especially regarding human rights.

connection with research on security and surveillance technologies will be briefly touched upon.

As will be seen, the regulatory landscape regarding security and surveillance is fragmented, governed by a patchwork of global, regional, and national regulatory instruments, creating the potential for gaps, loopholes and ambiguities. Furthermore, a fundamental dilemma highlighted by this chapter is that while human rights and privacy are global rights and data protection and certain other regulatory areas are covered by EU law, national security remains primarily a privilege for each member state. This can pose tensions where security functions to limit privacy rights or is presented as a protected value or right.

## 2.2. Human Rights

Human Rights are covered by global and regional conventions, but the effectiveness of their delivery differs according to interpretation and implementation. While privacy forms a crucial part of human rights, the role security plays in justifying an interference with privacy rights is subject to dynamic and evolving interpretation.<sup>146</sup>

Human rights are fundamental principles; closely attached to ethics they aim to confer and protect a set of basic rights for every human being. These aims are reflected in *The Universal Declaration of Human Rights* (UDHR) which forms the basis for global governance in the field. *The European Convention of Human Rights* (ECHR) which followed in its wake was the first legal, international treaty to protect human rights with enforceable mechanisms.

The *European* commitment to the principles of pluralist democracy, human rights and the rule of law covers at least 800 million citizens. Extending the ECHR, the *Charter of Fundamental Rights of the European Union*, which was adopted in 2000 and entered into force in 2009, is structured around the principles of dignity, freedoms, equality, solidarity, citizen's rights and justice. However, while this global and regional governance is paramount, the wording of provisions is often quite vague, making room for different interpretations, as is often the case with ethical principles, see chapter 3.

---

<sup>146</sup> Paul De Hert, Balancing security and liberty with the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11, *Utrecht Law Review*, 2005, 74.

### 2.2.1. Human Rights and Privacy

The right to privacy is an ancient right, with roots in various religious traditions. The principle has found protection as an international human right from the outset. Today privacy is unequivocally recognized as a fundamental human right, which is enshrined in different major international legal instruments: *The Universal Declaration of Human Rights* (Article 12); *The International Covenant on Civil and Political Rights* (Article 17)<sup>147</sup>; *The European Convention of Human Rights* (ECHR) (Article 8)<sup>148</sup>; *The Charter of Fundamental Rights of the European Union* (Article 7)<sup>149</sup> and the *American Convention on Human Rights* (art. 11)<sup>150</sup>. The right to privacy is also complemented by concomitant rights, such as the right to freedom of expression (Article 10, ECHR).

The US is a crucial player in global privacy issues not only because of its global weight and importance, but also because of its vast dominance in terms of companies providing Internet services. The US has a long and strong history of providing protection for privacy, characterized by active and often innovative legislative initiatives. However, it also has a very strong conception of free speech, including freedom of commercial speech, which has been juxtaposed against privacy claims in many cases. This has led to an interesting overall legal framework which in some areas is globally cutting edge while in others, most notably in the area of data protection, is decidedly not so.<sup>151</sup> The 1974 Privacy Act<sup>152</sup> establishes a system of data protection, but only for public authorities.

Beyond Europe and the US, the *global* landscape regarding privacy protection is quite diverse.<sup>153</sup> In the *African Charter on Human and Peoples' Rights*<sup>154</sup> there is no explicit protection of privacy. In *China* there is limited protection of privacy, with no fully-fledged constitutional guarantee, nor proper privacy or data protection law – though the country is seeing increasing pressure for change. Until recently, *South Asia* was decidedly lagging in its safeguarding of data protection and privacy, but recently the situation in India has changed significantly, notably through cases from the Constitutional court and the introduction of a

---

<sup>147</sup> <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>

<sup>148</sup> [www.echr.coe.int/Documents/Convention\\_ENG.pdf](http://www.echr.coe.int/Documents/Convention_ENG.pdf)

<sup>149</sup> [www.europarl.europa.eu/charter/pdf/text\\_en.pdf](http://www.europarl.europa.eu/charter/pdf/text_en.pdf)

<sup>150</sup> [http://www.oas.org/dil/treaties\\_B-32\\_American\\_Convention\\_on\\_Human\\_Rights.htm](http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.htm)

<sup>151</sup> T. Mendel, A. Puddephatt, B. Wagner et al. "Global Survey on Internet Privacy and Freedom of Expression." UNESCO, 2012, p. 87 – 89.

<sup>152</sup> <http://www.justice.gov/opcl/privstat.htm>

<sup>153</sup> UNESCO Global Survey on Internet Privacy and Freedom of Expression, 2012. See [unesdoc.unesco.org/images/0021/002182/218273e.pdf](http://unesdoc.unesco.org/images/0021/002182/218273e.pdf)

<sup>154</sup> [www.achpr.org/instruments/achpr/](http://www.achpr.org/instruments/achpr/)

comprehensive Privacy Bill. In *Argentina, South Africa and Mexico* national constitutions include a freestanding right to privacy.

By default privacy prohibits interferences of the state and private actors in the individual's autonomy: it shields them off from intrusions. The scope and reach of privacy are, however, undetermined, as it is up to judges to decide when privacy interests are at stake and when their protection can rightfully be invoked. In Europe the legal basis for the protection of privacy is found in the European Convention on Human Rights:<sup>155</sup>

*“Article 8 – Right to respect for private life and family life:*

*1. Everyone has the right to respect for his private and family life, his home and his correspondence.*

*2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.*

Europe's very strong protection of privacy is reflected in the practice from the European Court of Human Rights, which is in general both dynamic and progressive in its interpretations of human rights. On numerous occasions this Court has emphasised that the European Convention is 'a living instrument which could be interpreted according to present-day conditions'.<sup>156</sup> In a similar vein the Court has repeatedly stressed that the Convention is intended to guarantee 'not rights that are theoretical or illusory but practical and effective'. This effective method of interpretation opens the way for expanding the protection offered by the Convention and is very promising when considering new technological developments in the field of surveillance that challenge human rights in a way that could not be foreseen during the Convention's original drafting. However, it has been claimed that the Court has

---

<sup>155</sup> [http://www.echr.coe.int/Documents/Convention\\_ENG.pdf](http://www.echr.coe.int/Documents/Convention_ENG.pdf)

<sup>156</sup> This sentence has featured in numerous court judgements since the ECtHR's early days. See G. Letsas, "ECHR as a Living Instrument: its Meaning and Legitimacy" in G. Ulfstein, A. Follesdal and B. Peters (eds), *Constituting Europe: The European Court of Human Rights in a National, European and Global Context*, Cambridge University Press (2013), pp. 106-141.

been somewhat hesitant in applying article 8 to several forms of data processing (written data; biometrical data; visual data) in databases.<sup>157</sup>

The court has ruled that the use of a variety of specific surveillance measures constitutes an interference with the right to private life as articulated in article 8 of the European Convention on Human Rights.

The past 30 years police interception of communications, including the interception of messages sent to an applicant's pager, the judicial interception of communications, bugging of apartments, the recording of voices, the disclosure to the media of footage filmed in a street by closed-circuit television (CCTV), video recordings of a person at her workplace without prior notice, the monitoring of e-mails, and GPS monitoring, were all found to constitute interferences with article 8. More generally, the Court has ruled that the mere storing of information relating to an individual's private life by a public authority amounts to an interference. The subsequent use of this stored information has no bearing on that finding. Last but not least the Court has indicated that such interference exists even when an individual cannot point out that they were individually subjected to it. Such an interference with the right to privacy is as such not per se illegal, according to the Convention and the Court, if the use of the surveillance measure took place in accordance with the law, pursued one or more of the legitimate aims referred to in article 8.2 of the Convention and is "necessary in a democratic society in order to achieve the aim or aims...."<sup>158</sup>

For measures of surveillance to be compliant with the ECHR, they must be based on a particularly precise domestic law, which has to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to such measures. The law should be accessible to the person concerned, who must be able to foresee its consequences for him. When secret surveillance measures are to be used, the Court has developed minimum safeguards that should be set out in statute law in order to avoid abuse of power.

A few cases may illustrate practise:

One case from 2009<sup>159</sup> has implications for the collection, storing, exchange and use of biometric data by all parties to the convention. The UK practice of keeping

---

<sup>157</sup> Paul De Hert, Balancing security and liberty with the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11, Utrecht Law Review, 2005, 74.

<sup>158</sup> R. Bellanova, D. Bigo, V. Coroama et al, 'Smart Surveillance - State of the Art' Report of the SAPIENT project, 2012, p. 88 - 89: <http://www.sapientproject.eu/docs/D1.1-State-of-the-Art-submitted-21-January-2012.pdf><http://www.sapientproject.eu/docs/D1.1-State-of-the-Art-submitted-21-January-2012.pdf>

<sup>159</sup> S and Marper v United Kingdom, 30562/04 [2008] ECHR 1581.

indefinitely the fingerprints and DNA of people not convicted of an offence was seen as a violation of Article 8.<sup>160</sup>

Here the Court found that the length and indiscriminate nature of retention failed to strike a fair balance between public order concerns and privacy rights, and could not be regarded as necessary in a democratic society.

Another case found powers granted to the police by the Terrorism Act 2000 to stop and search persons were in violation of article 8, as they were neither sufficiently circumscribed nor subject to adequate legal safeguards against abuse. As such the Court found the powers not to be “in accordance with the law” in violation of Article 8.<sup>161</sup>

### **2.2.2. Security as justification to limit privacy.**

The interests of security constitute a legitimate aim to limit or infringe human rights. As van Kempen notes, 'Human rights law offers the authorities possibilities to restrict the range of rights or the exercise thereof on account of national security. Examples of such interests are public safety, prevention of disorder or crime or more specifically the defence of any person against unlawful violence or prevention against reoffending, health threats or more specifically the spread of infectious diseases, morals, the economic well-being of the country and/or the fundamental rights and freedoms of others'.<sup>162</sup> In other words the personal security of others may justify the limitation of a human right.

In the European Convention on Human Rights the second paragraph of article 8 provides the possibility to restrict the right to privacy in certain cases. In general the Court has stated that an interference will be considered “necessary in a democratic society” for a legitimate aim if it answers a “pressing social need” and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are “relevant and sufficient”. The Court often does not take a very close look at the potential benefits of surveillance technologies, but statistical figures have been used to criticize the proportionality of phone taps in two cases.

---

<sup>160</sup> See: <http://www.bailii.org/eu/cases/ECHR/2008/1581.html>

<sup>161</sup> see: <http://www.bailii.org/eu/cases/ECHR/2010/28.html>

<sup>162</sup> Piet Hein van Kempen, Four concepts of security – a human rights perspective, Human Rights Review, 2013, p.13.

What is particularly worrying in this context is the broad interpretation of “security” as reason for limiting privacy, which risks becoming a “catch-all” clause. As pointed out by van Kempen<sup>163</sup>:

‘many human rights limitation grounds are interpreted and applied rather broadly and some of them *de facto* even function as catch-all clauses. Moreover, although the scope and meaning of a few limitation clauses can fairly precisely be distilled from the case law of human rights monitoring bodies (...) none of them are specified through precise definitions in either human rights treaties or the associated case law. In addition, both the Human Rights Committee and the European Court for Human Rights have hardly even concluded that the objective of a human rights restriction did not have a legitimate aim within the meaning of the treaty’s limitation clause. Instead they typically review whether the interference was necessary and proportionate to the supposed legitimate aim. Human rights law is thus at most casuistic in its clarification and by far most of the limitation grounds only marginally help to define what national security or any other forms of security exactly encompass (....) It is remarkable that human rights law does not provide a more substantive approach to the legitimate aim requirement in order somewhat to control and limit the politicization or even exploitation of security’.

Van Kempen goes on and finally concludes that human rights law should provide ‘a general and more substantive concept of security as a ground to limit human rights. As part of that concept human rights law needs to emphasize that the referent for security and security policy is ultimately the individual. It should furthermore provide counter-pressure to the tendency to qualify everything as a security problem.’

### **2.2.3. Security as a self-standing human right**

According to the European Council ‘security is in itself a basic right’.<sup>164</sup> Even if this seems a very definitive statement it is not an easy task to evaluate its implications and importance, because there are different concepts of security as a human right. These include a negative individual security against the state and a positive state obligation to offer (individual) security against other individuals.<sup>165</sup>

#### **a. Security as a negative individual right against state intrusion**

Human rights have their origin in definitions of the liberty of the individual against oppression and the exercise of power by the sovereign and later the state. Human rights all imply a negative obligation on the part of the authorities and therefore all human rights intend to offer individuals security against the power of the state. Almost all human rights enumerated in the

---

<sup>163</sup> Idem p.13-15.

<sup>164</sup> European Council, *Internal Security Strategy for the EU: Towards an Internal Security Model*, 2010, p. 19: [http://www.consilium.europa.eu/uedocs/cms\\_data/librairie/PDF/QC3010313ENC.pdf](http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ENC.pdf)

<sup>165</sup> Piet Hein van Kempen, Four concepts of security – a human rights perspective, *Human Rights Review*, 2013, p.16.

European Convention on Human Rights and the Charter of Fundamental Rights are relevant in this perspective of security.

Given that the power of the state as such is infinite, this concept of negative security is of great importance to curtail and control that power. However, understood in this broad sense, human security is also an open and vague concept. The European Council's definition of 'security' overlaps with this broad notion of negative individual security but nevertheless is still broader because there is no indication that it only protects against the state.

Apart from the broad notion of negative individual security against the state, European human rights law also entails negative security in a more narrow and at the same time more explicit sense. The first paragraph of article 5 (Right to liberty and security) of the European Convention of Human Rights states <sup>166</sup>:

1. Everyone has the right to liberty and security of person. No one shall be deprived of his liberty save in the following cases and in accordance with a procedure prescribed by law.

Van Dijk *et al*<sup>167</sup> have pointed to the limited meaning of the notion of 'security of person' in article 5.1: "In article 5 the right to liberty of person and that to security are mentioned in the same breath, while in the following part of the article it is only the right to liberty of person that is elaborated."

It is interesting that article 6 of the Charter of Fundamental Rights of the European Union contains a similar provision as article 5.1 of the European Convention:

*"Everyone has the right to liberty and security of person"*

In their commentary on the Charter of Fundamental Rights the EU Network of Independent Experts on Fundamental Rights points to the principles regarding personal security and states the following<sup>168</sup>:

---

<sup>166</sup> See also article 9.1 of the International Covenant on Civil and Political Rights (ICCPR) of the UN: 'Everyone has the right to liberty and security of person. No one shall be subjected to arbitrary arrest or detention. No one shall be deprived of his liberty except on such grounds and in accordance with such procedure as are established by law'.

<sup>167</sup> P. Van Dijk et al, *Theory and practice of the European Convention on Human Rights*, Antwerpen-Oxford, Intersentia, 4th Edition, 2006, p. 457.

<sup>168</sup> EU Network of Independent Experts on Fundamental Rights, *Commentary of the Charter of Fundamental Rights of the European Union*: [http://ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal\\_en.pdf](http://ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal_en.pdf)



‘More difficult, however, is the definition of the meaning and scope of the right to personal security. The Human Rights Committee interprets the right to security of person in Article 9 ICCPR, since the landmark case of *Delgado Paéz v. Colombia* of 1990, as an independent right with the corresponding State obligation to take reasonable and appropriate measures to protect individuals, who are subject to death threats and other serious threats to their personal safety. Although this interpretation corresponds to the usual meaning of the right to personal security, as understood since the early human rights documents during the French Revolution, the European Court of Human Rights has never attributed any independent significance beyond personal liberty to the right to personal security in Article 5 ECHR notwithstanding the increasing significance of security issues in the modern human rights discourse. ‘

During the drafting of Article 6 of the Charter the term ‘security’ has repeatedly led to controversial discussions, and some members proposed to simply delete it, as it might give rise to different interpretations in some EU member States, such as France, Italy and Germany. The Convention (drafting the Charter), however, *decided to maintain the term in the restrictive understanding of the Strasbourg case-law under Article 5 ECHR*<sup>169</sup>.

A European Commission Staff Working Paper<sup>170</sup> warned that: ‘It would be wrong, however, to understand this right (the right to security of person) as an abstract guarantee ‘to be protected’ by the state and as an alleged right to ‘public security’. Instead, Article 6 of the Charter guarantees the same rights as those guaranteed by Article 5 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (‘ECHR’) and has the same meaning and scope. As to the interpretation of Article 5 ECHR, the European Court of Human Rights has consistently held that ‘*Article 5 contemplates individual liberty in its classic sense, that is to say the physical liberty of the person (...). The phrase ‘security of the person’ must also be understood in the context of physical liberty rather than physical safety (...). The inclusion of the word ‘security’ simply serves to emphasise the requirement that detention may not be arbitrary (...).*’

Van Kempen concludes that ‘the negative right to security (in article 5 of the European Convention and article 6 of the Charter) is at the very most only of marginal importance within the (broader) concept of negative security’.<sup>171</sup>

Based on the arguments above it is probably fair to say that the European Council’s notion of security is not protected by the negative right to security in article 5 of the European Convention and article 6 of the Charter.

## **b. Security as a positive state obligation towards individuals**

---

<sup>169</sup> EU Network of Independent Experts on Fundamental Rights, Commentary of the Charter of Fundamental Rights of the European Union, p. 68.

<sup>170</sup> Commission Staff Working Paper, Operational Guidance on taking account of Fundamental Rights, Commission Impact Assessments, Brussels, 6.5.2011SEC(2011) 567 final, p.8.

<sup>171</sup> Piet Hein van Kempen, Four concepts of security – a human rights perspective, Human Rights Review, 2013, p.11.

This notion of personal security signifies that the protection of human rights requires the state to take appropriate measures to safeguard these rights from violation by others. 'The essence of this concept is thus the provision by the authorities of positive security for individuals within national society against individual officials and –particularly remarkable– other private parties'.<sup>172</sup> Human rights monitoring bodies such as the European Court have been expressly formulating duties of the state to criminalise, criminally investigate, prosecute, criminally try and punish private individuals' conduct that conflicts with the values on which these rights are based. For instance, in order to protect the right to life (article 2 of the European Convention) the European Court holds that the state has the primary duty to put in place effective criminal law provisions to deter the commission of offences against the person.

These obligations are furthermore relevant as regards certain violations of, for example, the right not to suffer torture and ill-treatment, the right to respect for privacy and the freedoms of expression, religion and assembly. Still according to this author 'the development of the human rights concept of positive security against other private parties significantly reinforces the capacity of these individuals and groups to force the authorities to respect them and thus to counter threats with which they are confronted within society.

Moreover, the concept acknowledges that constraints on individuals' freedom, autonomy and capabilities may not be the results of the exercise of state power alone but do in fact also follow from social forces and the conduct of private individuals, groups and organisations. And while certain scholars (van Kempen included) have serious objections against the use of criminal law to enforce these positive obligations, there is nonetheless acknowledgement of a need 'to recognize that overall individual security is an essential prerequisite for the exercise of freedom as such'.<sup>173</sup>

## 2.3 Surveillance regulation

### 2.3.1. Jurisprudence

There is a vast quantity of regulation covering surveillance, however this domain is dealt with primarily at national level and the national legislation on surveillance differs extensively between countries within Europe and around the world. Furthermore, there is little precedent

---

<sup>172</sup> Piet Hein van Kempen, Four concepts of security – a human rights perspective, Human Rights Review, 2013, p.16.

<sup>173</sup> Idem, p.17.

for consensus or cooperation in this field, probably due in part to the novelty of the issue, the emergence of divergent national approaches, and the fact that it is closely connected to (national) security and police matters.

In an EU context there are a number of regulations, resolutions, reports etc. on the topic of surveillance, both regarding CCTV and telecommunications. References can be made notably to the Council Resolution on telecommunications of 1995<sup>174</sup> and to Article 16 of the Treaty on the Functioning of the European Union – movement of personal data across the EU – often called upon in the name of “security” concerns<sup>175</sup>.

### **2.3.2. Surveillance cameras – CCTVs**

The legal regulation of CCTV in Europe takes place at national level. While public area CCTV is not very common in France, Germany, Greece and Spain, the UK makes widespread use of CCTV in public spaces. Many European countries explicitly acknowledge that CCTV surveillance in public spaces creates a conflict with the right to privacy and regulation is often seen as necessary and desirable.<sup>176</sup> A common feature is a permit system for private users wishing to surveil a public space, while the police are often granted a wider ambit in which to use CCTV surveillance. The law can effectively limit CCTV use, and it may provide a forum in which legitimate criticism, concern and limitations can be stated when asking for permission.

Some examples of national CCTV regulation are presented below to give a snapshot of the range of regulatory systems in place in Europe. This is not an overview of all countries and we do not purport to provide a comprehensive review but in order to illustrate the differences among forms of regulation it is important to showcase the following examples.

#### **a. Germany**

In *Germany* the legal situation is complicated by the fact that some areas of the use of CCTV such as the storage and analysis of data gained by optic-electronic devices are regulated at the federal level and some at the level of the states (“Länder”). In general, compared to other member states, Germany holds a relatively strict framework of data protection regulation

---

<sup>174</sup> Council Resolution of 7 January 1995 on the lawful interception of telecommunications (96/C329/01).

<sup>175</sup> See: [http://ec.europa.eu/justice/data-protection/law/treaty/index\\_en.htm](http://ec.europa.eu/justice/data-protection/law/treaty/index_en.htm) and [http://eur-lex.europa.eu/resource.html?uri=cellar:ccccda77-8ac2-4a25-8e66-a5827ecd3459.0010.02/DOC\\_1&format=PDF](http://eur-lex.europa.eu/resource.html?uri=cellar:ccccda77-8ac2-4a25-8e66-a5827ecd3459.0010.02/DOC_1&format=PDF)

<sup>176</sup> Marianne L. Gras: “The Legal Regulation of CCTV in Europe”, 2004.

when it comes to CCTV. The guiding principle is the so-called right to informational self-determination. In its ruling on the population census the Federal Constitution Court “invented” this fundamental right in 1983 by deriving it from Article 2(1) Basic Law (“general right of personality”) in combination with Article 1(1) Basic Law (“dignity”) and applying these entitlements to the field of data protection. Although some specific regulations for mandatory CCTV surveillance in some special areas exist (cash offices, entrances to gambling halls) the private use of CCTV is strictly limited (purpose, proportionality, appropriateness, effectiveness, duty to delete and / or to inform the affected person) according to sect. 6b of the Federal Data Protection Act (BDSG)<sup>177</sup>. The right of an owner of a property to install and use CCTV is constrained by several provisions and, again, by the concurrent right of affected persons to their informational self-determination.

The use of optic-electronic devices by public bodies is governed by the different police laws of the different states and/or their data protection acts. The regulations differ slightly in terms of scope of the use of CCTV, depth of intervention, period of storage, but are all to meet the right to informational self-determination (with the exception of criminal investigation where this requirement is not needed for a defined period of time and purpose).

## **b. France**

In *France*, permission, implementation and monitoring of CCTV installation are given by the National Commission<sup>178</sup> for CCTV created by the law of orientation and programming for the performance of internal Security.<sup>179</sup> The board of this National Commission for CCTV, installed 4<sup>th</sup> January 2012, at the Ministry of Interior, is also responsible for advising and assessing the effectiveness of CCTV according to the Decree of 25 July 2011. As such, it is responsible for making recommendations regarding the characteristics, operation and use of CCTV devices<sup>180</sup>. Its members include five representatives of public and private persons authorized to implement a video surveillance system; five representatives of the Ministry of the Interior; the Inter-ministerial Delegate for private security; a member of the National Computer Board and freedom, two deputies and two senators; four persons nominated as

---

<sup>177</sup> The English version is available at:

[http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG\\_idFv01092009.pdf?\\_\\_blob=publicationFile](http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile)

<sup>178</sup> Commission nationale de la vidéoprotection, <http://www.interieur.gouv.fr/Videoprotection/La-commission-nationale-de-vidioprotection>

<sup>179</sup> Loi d'orientation et de programmation pour la performance de la sécurité intérieure (usually referred to by its acronym LOPPSI), 14 mars 2011.

<sup>180</sup> The National Video Protection Commission is required to prepare an annual report for Parliament evaluating the efficiency of video protection and proposing recommendations.

qualified individuals (a judge, a prosecutor and two persons appointed by the Minister of the Interior because of their expertise in the field of CCTV or civil liberties). Permissions have to be sought via an application procedure addressed to the competent prefecture (department where the system will be installed) by mail or online<sup>181</sup>. Public debate over the use of CCTV in France is divided, split between those who defend this "new tool" as a means to facilitate investigations and reassure the public, and those who see it as an infringement of civil liberties, whose cost to benefit ratio is disproportionate. In October 2013, a Senate report<sup>182</sup> made recommendations for a moratorium on investments relating to CCTV and the creation of a performance indicator.

### **c. Poland**

In *Poland* there is no uniform legislation governing the installation and use of CCTV. Legislation on the safety of large-scale public events (outdoor sports, football matches)<sup>183</sup> requires the installation of and monitoring by CCTV. In addition, uniformed services (border guards, Internal Security Agency, police and municipal guards) are authorized to use CCTV by relevant regulations pertaining to their work. Also, banking law authorizes video monitoring to assure safety of assets and bank customers (Law Gazette 2012, art.1376). Furthermore, local administration (cities, counties) can introduce resolutions authorizing the installation of CCTV in the interest of public safety. For some time now ombudsmen for civil rights and personal data protection as well as NGOs have been urging the Ministry of the Interior and Administration to expedite their work on the development of specific legislation regulating video monitoring, emphasizing that in many cases CCTV have been installed without any legal grounds. Furthermore, recent polls suggest that in 42% of Polish cities there is no available information on which places are being monitored, and in 35% citizens have not been consulted prior to CCTV installation.

---

<sup>181</sup> <http://www.interieur.gouv.fr/Videoprotection/Tele-procedure>

<sup>182</sup> Rapport d'information N° 91 fait au nom de la commission des finances sur les investissements dans la police et la gendarmerie, par M. Jean-Vincent PLACÉ, sénateur (enregistré à la Présidence du Sénat le 22 octobre 2013). Recommendation # 5: Decide on a moratorium on investments relating to CCTV, pending an independent scientific study on the real contribution of CCTV in terms of security (in terms of clearance rate, control against delinquency prevention, sense of security, psychosocial aspects, suppression of human presence, guarantees of civil liberties ...). Recommendation # 6: Create a performance indicator on CCTV devices (e.g. measuring the number of cases solved by this type of device).

<sup>183</sup> Act of 20 March 2009, Law Gazette 2013 art.6114.

#### **d. Portugal**

In *Portugal* video surveillance is regulated by the Data Protection Law<sup>184</sup> and is further covered by a set of specific laws and regulations, depending on the entity and the purpose of the surveillance. Video surveillance by private entities is subject to prior authorization from the National Data Protection Commission, and registration by the Public Security Police. On the other hand, video surveillance handled by public security forces is subject to prior authorization from the Government, following an opinion from the National Data Protection Commission<sup>185</sup>. There are also special regimes for video surveillance in taxis and for road monitoring, but all of them require prior authorization from the National Data Protection Commission or notification to the same authority. The National Data Protection Commission, which is an independent body with powers of authority, is also responsible for monitoring compliance with the laws and regulations in the area of personal data.

#### **e. The Netherlands**

In *The Netherlands* public authorities must make an application to install CCTV cameras to the municipal council, which is considered according to local needs. This implies that surveillance must not be secret (unless required to be so for detection of a specific crime); be for a closely defined purpose to detect or prosecute defined crime or behaviour; and it must be necessary for the owner to perform his or her duties. The duties of a private person are regarded as limited to his or her property. Public places are the responsibility of the mayor assisted by the police. Less intrusive measures must be considered not only before the installation but also periodically in reviewing CCTV surveillance. A complaint about unsuitable surveillance can be made to the local council and by civil writ to a court. In addition, the Data Protection Board has a duty to supervise CCTV surveillance and has inspection powers. In order to consolidate the regulation, the Dutch government has made specific laws for CCTV surveillance and has expressly forbidden the secret use of CCTV surveillance in public places<sup>186</sup>.

---

<sup>184</sup> In English see: <http://www.cnpd.pt/english/bin/legislation/Law6798EN.HTM>

<sup>185</sup> [http://www.cnpd.pt/english/index\\_en.htm](http://www.cnpd.pt/english/index_en.htm)

<sup>186</sup> Surveillance & Society CCTV Special (eds. Norris, McCahill and Wood) 2(2/3): 216-229  
<http://www.surveillance-and-society.org/cctv.htm> and [http://www.surveillance-and-society.org/articles2\(2\)/regulation.pdf](http://www.surveillance-and-society.org/articles2(2)/regulation.pdf)

#### **f. Denmark**

*Denmark* has very strict regulations regarding CCTV<sup>187</sup> - stricter than most European countries. CCTV surveillance is generally forbidden in public areas, when conducted by private persons. There are, however, a number of exceptions for owners of certain kinds of property, such as petrol stations, factory areas, shopping centres, banks, ATM's etc. Moreover, exceptions can be made in certain cases for crime prevention purposes. Such a permit may be granted for 5 years. When surveillance is taking place, information should be given by signposting or in other ways about the surveillance. Public authorities and the police are permitted to use CCTV, and the latter may do so covertly. These exceptions may appear far-reaching, nevertheless the general ban is the point of departure. Denmark's approach to CCTV regulation is, however, rather unique in Europe.

#### **g. United Kingdom**

In the *UK*, the volume of telecommunications surveillance is quite overwhelming (it is estimated that there are 1.85 million CCTV cameras used in Britain, the vast majority by private companies<sup>188</sup>) and at the same time the UK presents an interesting example of very recent governance, in the form of a Code of Practice introduced in 2013.

The UK Home Office issued a "Surveillance Camera Code of Practice"<sup>189</sup> in June 2013 where 12 Guiding Principles, providing guidance on the appropriate and effective use of surveillance camera systems by relevant UK authorities (principally the police and local authorities), who must have regard to the code when exercising functions to which the code relates. Other operators and users of surveillance camera systems in the UK are encouraged to adopt the code voluntarily. According to the UK government, the code is seen as "a significant step in the ongoing process of delivering the government's commitment to further regulation of CCTV, which it believes is a task that is best managed in gradual and incremental stages."<sup>190</sup> The government has indicated the possibility that with time, it may consider including other bodies as relevant authorities who will have to have regards to the code, realising that the CCTV cameras form a complex landscape of ownership and operation.

---

<sup>187</sup> See the paper references in footnote 186 above: The regulation dates back to 1982, but has been revised several times.

<sup>188</sup> <http://www.theguardian.com/uk/2011/mar/02/cctv-cameras-watching-surveillance>

<sup>189</sup> The Code of Practice is issued by the Secretary of State under Section 30 of the 2012 Act.

In the report it is stressed that the government is fully supportive of the use of overt surveillance cameras in public places whenever that use is: in pursuit of a legitimate aim; necessary to meet a pressing need; proportionate; effective, and; compliant with any relevant legal obligations. The stated purpose of the code is to ensure that individuals and wider communities have confidence that surveillance cameras are deployed to protect and support them, rather than spy on them. The government considers that wherever overt surveillance in public places is in pursuit of a legitimate aim and meets a pressing need, any such surveillance should be characterised as surveillance by consent, and such consent on the part of the community must be informed consent and not assumed by a system operator. Here the government draws an analogy with so called “policing by consent”, in other words the public's implicit consent to be policed by law enforcement authorities and the legitimacy of those authorities which derives from the transparency of their powers, demonstrated integrity in exercising those powers and their accountability for doing so. The code has been developed to address concerns over the potential for abuse or misuse of surveillance by the state in public places, with the activities of local authorities and the police the initial focus for regulation. To support the practical application of the guiding principles by a system operator, the Surveillance Camera Commissioner will provide information and advice on appropriate and approved operational and technical standards.

The guiding principles are centred on the following elements:

1. A specified purpose is needed which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. Effects on individuals and their privacy should be taken into account.
3. As much transparency in the use of a surveillance camera system as possible.
4. Clear responsibility and accountability for all CCTV activities.
5. Clear rules, policies and procedures must be in place before CCTV is used.
6. No more images and information should be stored than what is strictly required.
7. Access to retained images and information should be restricted.
8. CCTV's operators should consider any approved operational, technical and competency standards relevant to a system and its purpose.
9. Security measures should be taken to safeguard against unauthorized access and use.
10. Review and audit mechanisms should be in place to ensure legal requirements, policies and standards are complied with.
11. kept up to date.

---

<sup>190</sup> Home Office (2013) Surveillance Camera Code of Practice, available at: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/204775/Surveillance\\_Camera\\_Code\\_of\\_Practice\\_WEB.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf)



### 2.3.3. Telecommunications surveillance

Seen from a *global* perspective the fact that telecommunications data are storable, accessible and searchable has not to a very large extent led to comprehensive regulation governing their disclosure to and use by State authorities, even if analysis of such data can be both highly revelatory and invasive, particularly when data is combined and aggregated. In many countries, existing legislation and practices have not been reviewed and updated to address the threats and challenges of communications surveillance in the digital age. The absence of laws to regulate global communications surveillance and sharing arrangements has resulted in ad hoc practices that are beyond the supervision of any independent authority. Today, in many states, access to communications data can be conducted by a wide range of public bodies for a wide range of purposes, often without judicial authorization and independent oversight. In addition, States have sought to adopt surveillance arrangements that purport to have extra-territorial effect.<sup>191</sup>

UN Special Rapporteur *Frank La Rue* has voiced a critique of the lack of regulation or the inadequacy of vague regulation leading to the legitimization of intrusive surveillance techniques without oversight or independent review:

“In most States, legal standards are either non-existent or inadequate to deal with the modern communications surveillance environment. As a result, States are increasingly seeking to justify the use of new technologies within the ambits of old legal frameworks, without recognizing that the expanded capabilities they now possess go far beyond what such frameworks envisaged. In many countries, this means that vague and broadly conceived legal provisions are being invoked to legitimize and sanction the use of seriously intrusive techniques. Without explicit laws authorizing such technologies and techniques, and defining the scope of their use, individuals are not able to foresee – or even know about – their application. At the same time, laws are being adopted to broaden the breadth of national security exceptions, providing for the legitimization of intrusive surveillance techniques without oversight or independent review.”..... “Whereas traditionally communications surveillance was required to be authorized by the judiciary, increasingly this requirement is being weakened or removed. In some countries, interception of communications can be authorized by a governmental minister, their delegate, or a committee. “

He stressed the special situation regarding national intelligence services:

“In many cases, national intelligence agencies also enjoy blanket exceptions to the

---

<sup>191</sup> Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, United Nations, General Assembly, 17 April 2013 /A/HRC/23/40): [http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40\\_EN.pdf](http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf)

requirement for judicial authorization. For example, in the United States, the Foreign Intelligence Surveillance Act empowers the National Security Agency to intercept communications without judicial authorization where one party to the communication is located outside the United States, and one participant is reasonably believed to be a member of a State-designated terrorist organization.” In addition, Germany, the UK and Sweden are identified in the report (see below)

In a *European* context it is primarily the responsibility of the member states to provide regulation in the area of telecommunications surveillance. Several European countries have provisions that make it mandatory to obtain specific and detailed judicial authority before wiretapping or intercepting of electronic communication<sup>192</sup>, but regulations regarding telecommunications present a varied picture.

*German* law allows warrantless automated wiretaps of domestic and international communications by the State’s intelligence services for the purposes of protecting the free democratic order, existence or security of the State. In *Sweden*, the Law on Signals Intelligence in Defence Operations authorizes the Swedish intelligence agency to intercept without any warrant or court order all telephone and Internet traffic that take place within Sweden’s borders.<sup>193</sup> In the *United Kingdom* the Secretary of State authorizes interception of communications<sup>194</sup>.

An interesting example of different approaches in this area is provided when comparing Germany and the USA.<sup>195</sup> Both contain detailed rules that regulate the surveillance of telecommunications by domestic law enforcement agencies and a well-developed law of “information privacy”. However, Germany has in some ways created a superior legal regime for regulating telecommunications surveillance. The German constitution protects telecommunications secrecy in its article 10, which has been interpreted in a series of important decisions by the Constitutional Court as protecting not only telecommunications content, but also telecommunications proceedings. The German constitution thus places substantial limits on the ability of the legislature to enact laws that limit Article 10 or other basic constitutional rights. A statute is void if it infringes upon Article 10’s core protections for telecommunications privacy, if it is against “human dignity” as protected by the Basic Law, or

---

<sup>192</sup> Benjamin J. Goold, University of Oxford: "Editorial: Making sense of Surveillance in Europe". *European Journal of Criminology*, Vol. 6, 2009, p. 115-117.

<sup>193</sup> Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,

<sup>194</sup> See, for example, the website of the Commissioner for the interception of communications, <http://www.iocco-uk.info>, and the code of practice for the interception of communications published by the Home Office in 2002: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/97956/interception-comms-code-practice.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97956/interception-comms-code-practice.pdf); ISBN 978-0-11-341281-5

<sup>195</sup> Paul M. Schwartz, *German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance*, 54 *Hastings L.J.* 751 (2002), Available at: <http://scholarship.law.berkeley.edu/facpubs/1184>

if it infringes the “rule of law”, which by the Constitutional Court has been used to develop the further “principle of proportionality”.

These examples of surveillance regulation indicate that the picture is scattered. There appears to be a tendency for very vague and unspecified notions of “national security” to have become an acceptable justification for the interception of and access to communications in many countries. It is probably fair to say that much regulation is outdated, not taking the new picture of surveillance into account, and with legislation failing to keep pace with the changes in technology.

## 2.4. Specific Regulatory Areas

### 2.4.1. Data protection

The concept of data protection is of far more recent vintage than privacy, essentially finding its genesis in the increasing collection of personal data about individuals by government. The advent of computers and then of the Internet, greatly spurred on the development of the concept of data protection. The core concept behind data protection is that individuals have a right to control the collection and use of data through which they may be identified (personal data). Like privacy data protection is subject to certain constraints, of which an obvious one is police investigations into crime. Data protection may be contrasted with privacy inasmuch as the core notions underpinning it are fairly clear and garner wide consensus, albeit with some important variations.

On a global level the United Nations has set out Guidelines on 10 key principles of data protection, which are relevant primarily to national legislation, but are also binding on international organizations, with appropriate modifications. They apply to publicly and privately held computerized files containing data on individuals, and may be extended to cover manual files and/or data on legal persons. The Guidelines include Lawfulness and Fairness; Accuracy; Purpose-Specification; Interested Person Access; Non-Discrimination and Security. The guidelines recognize that there may be a need for exceptions from the first 5 principles, but only as necessary to protect national security, public order, health and morals, or the rights and freedoms of others. They call for the designation of an independent supervisory authority with responsibility for ensuring respect for the principles, along with

systems of sanctions for breach of the rules. They also call for limits on circulation of information to countries which do not offer comparable safeguards.<sup>196</sup>

While the European Court of Human Rights has dealt with the protection of personal data as an integral part of the right to privacy, at EU level the right to data protection is seen as an autonomous right. Personal data are protected by the law even if the right to privacy is not at stake. Article 8 of the Charter for Fundamental Rights unambiguously states that “everyone has the right to the protection of their personal data”. Data protection is both broader and more specific than the right to privacy since it does not only aim at concretising the protection of privacy, but simply applies every time personal data are processed.

The Data Protection Directive formulates the conditions under which data processing is legitimate. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to the data that has been collected. The Data Protection Directive does not apply to the processing of personal data “concerning public security, defence, State security, and the activities of the State in areas of criminal law”. The rules are subject to control by an independent authority. The Data Protection Directive can be complemented by specific regimes for data protection for specific sectors.

As pointed out by *González Fuster*, data protection is also limited when data processing concerns national security:

‘Unsurprisingly, security has always also played different roles in EU personal data protection law. It can notably function as limit of its scope of application as it does in the proposed regulation and directive on data protection (see EGE opinion nr.26): they are to apply only to the processing of personal data in the course of activities falling under the scope of EU law, which explicitly excludes data processing concerning “national security”.<sup>197</sup>

The formulation of this limitation has been criticized by the European Data Protection Supervisor who believes the meaning of the expression is unclear:

‘As far as the exception for ‘activities falling outside the scope of Union law’ is concerned, the EDPS wishes to express a more general comment. While ‘national security’ falls outside the scope of Union law, it is not always fully clear what this notion covers, as it depends on Member States national policy. At national level, the use of the wording ‘national security’ or ‘state security’,

---

<sup>196</sup> United Nations, General Assembly Resolution 45/95 of 14<sup>th</sup> December 1990, Guidelines for the regulation of computerised personal data files.

<sup>197</sup> Gloria Gonzalez Fuster, Security and the future of personal data protection in the European Union, Security and Human Rights, 2012,n° 4, 339.

depending on Member States, with a different scope of application, can also be confusing. Obviously, the EDPS does not contest the exception, but he considers that it should be avoided that it is unduly used to legitimise the processing of personal data outside the scope of the Regulation and the Directive, for instance in the context of the fight against terrorism.<sup>198</sup>

On April 8th 2014, the European Court of Justice declared the Data Retention Directive<sup>199</sup> which obliges Internet service providers and telecom operators to retain data and information of European citizens using electronic communication networks as "invalid."<sup>200</sup> While the Court recognised that retention of personal data for the purposes of investigating crime was compatible with the Charter of Fundamental Rights, it found that the obligations set out in the Directive were disproportionate and contrary to Articles 7, 8 and 52(1) of the Charter. In particular the Court was concerned that the notion of serious crime had not been delineated and that the data retention period (6 months to 2 years) was too general and not related to the specific objective being pursued. The court found that *"the wide ranging and particularly serious interference of the directive with the fundamental rights at issue is not sufficiently circumscribed to ensure that that interference is actually limited to what is strictly necessary"*.

"37. It must be stated that the interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is, as the Advocate General has also pointed out, in particular, in paragraphs 77 and 80 of his Opinion, wide-ranging, and it must be considered to be particularly serious. Furthermore, as the Advocate General has pointed out in paragraphs 52 and 72 of his Opinion, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.

At the national level there exists a variety of data protection legislation, however in the EU member states the comprehensive EU data protection provisions form the legal basis of this regulation.

---

<sup>198</sup> Opinion of the European Data Protection Supervisor on the Data protection reform package, 7 March 2012, Brussels, 15.

<sup>199</sup> Directive 2006/24/EC.

<sup>200</sup> see:

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=900848>.

## 2.4.2. Aviation security, border control, cybercrime

### a. Aviation security

There are numerous regulations regarding aviation. The purpose of these provisions is security, and the experience from security checks in the airports shows that this area is getting complicated. New technological tools regarding security have come into use and have to a certain extent been covered by regulation and/or resolutions etc. Body scanning is a telling example, with regard to which the European Parliament has stressed that “people undergoing checks should receive comprehensive information in advance, particularly regarding the operation of the scanner concerned, the conditions in place to protect the right to dignity, privacy and data protection and the option of refusing to pass through the scanner”.<sup>201</sup> Reservations with regard to the use of body scanners have been expressed by the European Data Protection Supervisor, the Article 29 Working Party<sup>202</sup> and the EU Fundamental Rights Agency.<sup>203</sup>

Less visible but no less pervasive, aviation security measures also include the gathering and exchange of data on flight passengers known as Passenger Name Records (PNR). Travel information gathered by carriers and stored in airlines reservation and departure control databases are transferred to law enforcement authorities for the stated purpose of countering organised crime and terrorism. The EU has signed bilateral PNR Agreements with the United States, Canada and Australia.<sup>204</sup> A 2011 proposal by the European Commission for an EU PNR scheme which would oblige air carriers to provide EU countries with the data of passengers entering or leaving the EU was voted down by the European Parliament’s Civil Liberties Committee in 2013 due to concerns over the proposal’s compliance with principles of proportionality, impact on data protection and potential for profiling of passengers.<sup>205</sup>

---

<sup>201</sup> European Parliament resolution of 6 July 2011 on aviation security, with a special focus on security scanners (2010/2154(INI)).

<sup>202</sup> See: [http://ec.europa.eu/justice/data-protection/article-29/index\\_en.htm](http://ec.europa.eu/justice/data-protection/article-29/index_en.htm)

<sup>203</sup> Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports Brussels, 15.6.2010, COM(2010) 311.

<sup>204</sup> Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ L 215/5, 11.08.2012; Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data, OJ L 82/15, 21.03.2006; Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, OJ L 186/4, 14.07.2012.

<sup>205</sup> Proposal for a Directive of the European Parliament and Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32, 02.02.2011.

## **b. Border control**

The border has become a site of intensifying surveillance and has seen a proliferation of security technologies deployed. At EU level, the Schengen Information System (II), the Eurodac database and the Visa Information System (VIS) are large databases, which include the storage of biometric data, aimed at controlling migration flows and identifying and sorting legal and irregular migrants, as indicated in Chapter 1. The Schengen Information System II entered into operation on 9 April 2013 replacing the first generation SIS with a more complex, investigative instrument; SIS II contains data on irregular migrants, lost and false travel documents and wanted or missing persons and stores digital images and biometric data. At the time of the publication of the Commission's proposals on SIS II, the EDPS expressed concern over whether full consideration of the principles of proportionality and necessity had been taken into account, noting the absence of an impact assessment examining potential infringements on individuals' fundamental rights.<sup>206</sup> These concerns were pertinent given the practical and legal obstacles encountered by third country nationals attempting to access, correct or delete personal information held on the first generation Schengen Information System.<sup>207</sup>

On 28<sup>th</sup> February 2013, the European Commission presented further proposals for an Entry Exit System (EES) and a Registered Traveller Programme (RTP) for the Schengen Area, collectively known as the "Smart Borders Package"<sup>208</sup>. The Entry Exit System proposal proposes a centralised storage system for entry and exit data of third country nationals admitted for short stays to the Schengen area. This includes storage of biometrics subject to a transitional period of three years following introduction of the EES. The Article 29 Working Party on data protection has expressed serious concerns about whether the Entry Exit System *"meets the standards of necessity and proportionality necessary to justify its impact on the right to protection of personal data as set out in Article 8 of the EU Charter of*

---

<sup>206</sup> Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the establishment, operation and use of the Second Generation Schengen Information System (SIS II), OJ C 91/38, 19.04.2006.

<sup>207</sup> Brouwer, E. (2008), *The Other Side of the Moon: The Schengen Information System and Human Rights – A Task for National Courts*, CEPS Working Document, No.288, April 2008. See also Opinion of the EDPS on SIS II, in which he cites the case of a US lawyer wrongly identified and detained as a terrorist because his fingerprints matched those found in the bombings on Madrid.

<sup>208</sup> Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union COM(2013) 95.

*Fundamental Rights*".<sup>209</sup> Similarly, the EDPS has raised concerns in a strongly worded Opinion on the Commission's proposals:

There is no clear evidence that the Commission Proposals to create a smart border system for the external borders of the EU will fulfil the aims that it has set out... [O]ne of the stated aims of the proposals was to replace the existing 'slow and unreliable' system but the Commission's own assessments do not indicate that the alternative will be sufficiently efficient to justify the expense and intrusions into privacy<sup>210</sup>.

In addition to the concerns raised over the compliance of EU large-scale databases with principles of necessity and proportionality, there is an open question as to whether these EU databases – ostensibly aimed at border control - comply with the purpose principle. The possibility for law enforcement authorities to access data on asylum seekers (EURODAC) and migrants (SIS II and potentially also the EES) opens the way for databases to be used for purposes beyond their originally designated functions. Scholars have identified the potential for such technologies to blur the distinction between immigration, criminality and law enforcement, warning that individuals registered for immigration reasons may become at greater risk of being targeted for law enforcement measures and secret surveillance. The potential for data processing which singles out one group of individuals for stricter monitoring than others to breach principles of non-discrimination have been underscored by the Court of Justice.<sup>211</sup> These concerns are echoed by the EDPS in its Opinion on the Smart Borders proposals:

The general trend to give law enforcement authorities access to the data of individuals, who in principle are not suspected of committing any crime, is a dangerous one. The EDPS strongly recommends that the precise added value of such access, compared with access to existing biometric databases, be identified.<sup>212</sup>

Finally, the European Border Surveillance System (EUROSUR) became operational in December 2013.<sup>213</sup> EUROSUR aims to interlink the maritime surveillance systems of EU member states into a shared information-sharing and analysis architecture. The system draws on the use of surveillance technologies (including satellite imagery and sensors) to track ports, vessels and maritime zones in order to build a "common pre-frontier intelligence

---

<sup>209</sup> [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp206\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp206_en.pdf)

<sup>210</sup> EDPS (2013) Smart borders: key proposal is costly, unproven and intrusive, 19 July 2013, Press Release 2013/08.

<sup>211</sup> Case C-524/06 *Huber v Germany* [2008] ECR I-9705.

<sup>212</sup> EDPS (2013) Smart borders: key proposal is costly, unproven and intrusive, 19 July 2013, Press Release 2013/08.

<sup>213</sup> EU Regulation No 1052/2013 of 22 October 2013 establishing the European Border Surveillance System (Eurosir), OJ L 295/11, 06.11.2013.



picture”.<sup>214</sup> EUROSUR’s official purposes are both security-based - to fight cross border crime, control unwanted mobility – but also humanitarian - to improve rescue at sea and prevent tragedies caused by the sinking of unseaworthy vessels carrying migrants across the Mediterranean. The Meijers Committee, the Standing Committee of Experts on International, Immigration and Refugee Law, noted the following:

Assessing the content of the current proposal for a Regulation establishing the European Border Surveillance System, the Meijers Committee not only has doubts with regard to the necessity and efficiency of the proposed measures (also considering the high permanent costs involved), but is also very concerned with regard to the effects of Eurosur for the fundamental rights of asylum seekers and refugees, including the right to privacy and data protection. In particular, the Meijers Committee warns against the risks of increased surveillance as this might also increase the human costs of undocumented migration: border surveillance indeed will have an impact on migration routes but not on the root causes of migration.<sup>215</sup>

The Committee emphasised that the aim of the EUROSUR proposal to increase situational awareness also means that there is an increased responsibility under international refugee law and the Search and Rescue regime based on the International Convention on Maritime Search and Rescue. In a similar vein, the UN Special Rapporteur on the Human Rights of Migrants, Francois Crépeau has raised a number of questions and concerns with regard to the new system:

The Special Rapporteur regrets that the proposal does not, however, lay down any procedures, guidelines, or systems for ensuring that rescue at sea is implemented effectively as a paramount objective. Moreover, the proposed Regulation fails to define how exactly this will be done, nor are there any procedures laid down for what should be done with those “rescued”. In this context, the Special Rapporteur fears that EUROSUR is destined to become just another tool that will be at the disposal of member States in order to secure borders and prevent arrivals, rather than a genuine life-saving tool.<sup>216</sup>

### **c. Cybercrime**

As regards the regulation of cybercrime, the Council of Europe Convention on Cybercrime of 23 November 2001 and the Additional Protocol to the Convention on Cybercrime, of 28 January 2003<sup>217</sup> provide a solid foundation. This Convention is the first international treaty on

---

<sup>214</sup> Ibid.

<sup>215</sup> Note of the Meijers Committee on the proposal for a Regulation establishing the European Border Surveillance System, 12.09.2012.

<sup>216</sup> Report of the United Nations Special Rapporteur on the human rights of migrants, François Crépeau - Regional study: management of the external borders of the European Union and its impact on the human rights of migrants, 24 April 2013, A/HRC/23/46.

<sup>217</sup> <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> and <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>.

crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation. It also contains a series of powers and procedures such as the search of computer networks and interception.

The explanatory memorandum to the Convention<sup>218</sup> notes that

“The revolution in information technologies has changed society fundamentally and will probably continue to do so in the foreseeable future. Many tasks have become easier to handle. Where originally only some specific sectors of society had rationalised their working procedures with the help of information technology, now hardly any sector of society has remained unaffected. Information technology has in one way or the other pervaded almost every aspect of human activities.”

The Convention serves as a guideline for any country developing comprehensive national legislation against Cybercrime and as a framework for international cooperation between State Parties to this treaty. It has also been taken as a legal reference point for the EU, which is currently developing a substantial body of policy to increase cyber-security.

The latest EU developments are the Commission Communication on Cyber security strategy of February 2013<sup>219</sup> which outlines the EU's vision on how to enhance security in cyberspace and sets out the actions in that area, and the new EU Directive 2013/40 on attacks against information systems which came into force on 3 September 2013<sup>220</sup>. The Directive aims to tackle large-scale cyber-attacks by requiring Member States to strengthen national cyber-crime laws and introduce tougher criminal sanctions.

### **2.4.3. Whistle-blowing**

Whistle-blowing is not confined to issues of security and surveillance, but the actions of Edward Snowden have served to highlight the gaps in systems intended to ensure that

---

<sup>218</sup> <http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm>

<sup>219</sup> <http://ec.europa.eu/dgs/connect/en/content/cybersecurity-strategy-european-union>

<sup>220</sup> Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA Official Journal L218/8 14/8/2013: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF>

actions by states in the name of national security meet legal requirements, and that where individuals believe that legal restrictions have been ignored, that there exist mechanisms to ensure that they have recourse to appropriate systems to address their concerns.

A recent report from Transparency International<sup>221</sup> contains an overall assessment of the adequacy of whistle-blower protection laws of 27 member countries of the EU. Only four European Union (EU) countries have legal frameworks for whistle-blower protection that are considered to be advanced: Luxembourg, Romania, Slovenia and the United Kingdom (UK). Of the other 23 EU countries, 16 have partial legal protections for employees who come forward to report wrongdoing. The remaining seven countries have either very limited or no legal frameworks. Moreover, many whistle-blower provisions that are currently in place contain loopholes and exceptions. The result is that employees who believe they are protected from retaliation could discover, after they blow the whistle, that they actually have no legal recourse. Encouragingly, several EU countries in recent years have taken steps to strengthen whistle-blower rights, including Austria, Belgium, Denmark, France, Hungary, Italy, Luxembourg, Malta, Romania and Slovenia. Countries that have issued proposals or have announced plans for proposed laws include Finland, Greece, Ireland, the Netherlands and Slovakia. Political will is, however, lacking in many countries.

Transparency International urges all EU countries to enshrine comprehensive whistle-blower rights into their laws and begin a public dialogue on this matter. While that report focuses on the fight against corruption, many of these principles are very relevant in the security and surveillance context and should be duly scrutinized in this framework.

The European Commission and Member States should ensure that an effective and comprehensive whistle-blower protection mechanism is established in the public and private sectors, as also called upon by the European Parliament in October 2013.

Transparency International also provides a set of principles as “best practices for laws to protect whistle-blowers and support whistleblowing in the public interest”. Principle 19 provides for whistleblowing in the area of national security or official secrets.

19. National security/official secrets – where a disclosure concerns matters of national security, official or military secrets, or classified information, special procedures and safeguards for reporting that take into account the sensitive nature of the subject matter may be adopted in order to promote successful internal follow-up and resolution and to prevent unnecessary external exposure. These procedures should permit internal disclosures, disclosure to an autonomous oversight body that is institutionally and operationally independent from the security sector, or disclosures to authorities

---

<sup>221</sup> Transparency International, Whistleblowing in Europe, Legal Protection for whistle-blowers in the EU, 2013.

with the appropriate security clearance. External disclosure (that is, to the media or civil society organisations) would be justified in demonstrable cases of urgent or grave threats to public health, safety or the environment; if an internal disclosure could lead to personal harm or the destruction of evidence; and if the disclosure was not intended or likely to significantly harm national security or individuals.

#### **2.4.4. Drones**

As drone technology is still relatively new, it is no surprise that a regulatory framework governing their use is very limited. Nevertheless, it poses an important challenge for regulators.

The European Commission adopted the Communication "A new era for aviation - Opening the aviation market to the civil use of RPAS in a safe and sustainable manner" on 8 April 2014. This Communication sets out the Commission's views on how to address civil drones, or remotely piloted aircraft systems (RPAS), operations in a European level policy framework intended to enable the progressive development of the commercial drones market while safeguarding the public interest.

It builds on studies and preparatory work examining the legislative situation with regard to drones in the EU Member States, focussing on civil uses.<sup>222</sup>

A wider perspective, also encompassing other uses of these technologies, is provided in the vignette on drones, below.

---

<sup>222</sup> Those documents are available on: [http://ec.europa.eu/enterprise/sectors/aerospace/uas/index\\_en.htm](http://ec.europa.eu/enterprise/sectors/aerospace/uas/index_en.htm)

## Drones

Unmanned aerial vehicles (UAVS), or unmanned aerial systems (UAS's) also known as drones, are remotely piloted aircraft that can be as large as a Boeing 737 or as small as an insect. Advances in flight and radio technology in the 1970's allowed for the development of drones, most notably by the Israeli Air force. These pioneer drones were used for reconnaissance missions in the 1991 Iraq Wars and later models including the "Predator" routinely flew over the Balkans in support of NATO operations in the region<sup>223</sup>. The first armed drone was the MQ-1B Predator which conducted its first attack using hellfire missiles in Yemen in November 2002<sup>224</sup>. Following the 2001 terrorist attacks in the US, there was a shift from using drones for surveillance purposes only, to their use in targeted strikes in remote regions of Afghanistan and Pakistan. In 2007, the MQ-9 Reaper was launched which is capable of flying nine times further than and twice as high as the Predator. It uses a number of sensors (including infrared) for targeting and is fitted with a colour TV camera and image intensified TV camera which provide a live feed<sup>225</sup>. It is specifically intended as a "hunter/killer weapon system", rather than for surveillance.

Traditionally drones have been considered to be ideally suited for doing tasks which were "dull, dirty and dangerous", the so called 3 Ds<sup>226</sup>. Advanced telecommunications technologies allow drones to operate at high altitudes, for long periods of time, over considerable distances. Thus, surveillance missions, considered to fall into the dull and dangerous categories take advantage of the capacity of drones to loiter over areas for long periods of time (anywhere from 18-82hrs) without placing personnel in harm's way. Due to the unmanned nature of drones, they can also be useful for "dirty" tasks such as flying into areas which have been affected by a chemical/biological attack or by a natural disaster.

Drones have now become the weapon of choice in counter-terrorism and over the next 40 years they are expected to replace piloted aircraft. In 2002, the US Department of Defence had 167 drones in operation; by 2010 that had increased to 7000 in operation worldwide. Since 2009, the US military has trained more unmanned aircraft pilots than traditional fighter pilots<sup>227</sup>. Drone strikes have been made in Afghanistan, Pakistan, Yemen, Somalia, Libya, Gaza and Iraq. Estimates for the number of civilians killed by drone strikes vary considerably as much of the data is compiled by interpreting news reports whose credibility may vary. According to the Bureau of Investigative Journalism somewhere between 416 to 951 civilians have been killed by CIA drone strike in Pakistan since 2004; 168 to 200 of those deaths were of children<sup>228</sup>.

The next generation of drones will not alone be unmanned but will be programmed to make mission critical decisions on an autonomous basis. Drones have been developed which can take off and land automatically, without any intervention of the controller on the ground. The X-47B was commissioned by the US navy and in May 2013 it capability to launch and land from the deck of an aircraft carrier was tested. BAE systems in the UK are developing the Taranis unmanned semi-autonomous combat air vehicle demonstrator to attack aerial and ground targets. The UK Ministry for Defence have confirmed that initial flight trials have already taken place in South Australia<sup>229</sup>. The advent of autonomous technology coupled with the offence use of Predators and Reapers has raised the spectre of "lethal autonomous robotics", weapons system that once engaged could select and engage targets without any human intervention. Research is being undertaken at the Georgia Institute of Technology's School of computing to develop ethical architecture for autonomous drones. By programming drones to use information on previous engagements e.g. area of destruction, they could adjust their "behaviour" e.g. choice of weapon in future engagements.

---

<sup>223</sup> Deri, AR. Intersect 2012;5:1-16

<sup>224</sup> <http://news.sky.com/story/139261/cia-acted-alone-in-yemen-strike> accessed 14th November 2013

<sup>225</sup> <http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104470/mq-9-reaper.aspx> accessed 14th November 2013

<sup>226</sup> Attributed to Peter Singer Director, Centre for 21st Century Security and Intelligence

<sup>227</sup> Committee on Oversight and Government Reform 2010

<sup>228</sup> <http://www.thebureauinvestigates.com/category/projects/drones/monthly-updates/> accessed 8th January 2014.

<sup>229</sup> <http://www.janes.com/article/28899/taranis-makes-maiden-flight> accessed 14th November 2013

Combat use of UAVs and the prospect of autonomous drones have raised a number of issues about the legality of drone strikes, the changing nature of warfare and accountability. Christof Heyns, the UN special rapporteur on extrajudicial killings described drone strikes as a form of global policing which could serve to undermine rather than strengthen international security<sup>230</sup>. Heyns has also called for a global moratorium on the "testing, production, assembly, transfer, acquisition, deployment and use" of lethal autonomous robotics until further regulations are put in place to govern their use<sup>231</sup>. In an accompanying interim report by the UN's special rapporteur on human rights and counter-terrorism, Ben Emmerson questioned the legality of drone strikes and called on States to respect the full range of applicable international law, to be transparent in their use of drones and to investigate allegations of unlawful killings<sup>232</sup>. Concerns have been raised that the advent of drones will alter the perceived cost of war. The detachment facilitated by drone strikes may lower the threshold for war for both the political system and the general public and that the essential element of restraint due to the high cost of war both in economic and human terms may be undermined. The development of autonomous drones is even more ethically challenging as these machines will in principle decide whether or not to kill human beings. Krishnan has argued that this elevates drones "ontologically and maybe even morally from the mere object to a subject capable of morally meaningful action"<sup>233</sup>.

Drones may be deployed in a variety of contexts and for a wide range of purposes. The number of countries with UAV systems for military, commercial or civil use grew from 41 countries in 2005 to 76 countries in 2011<sup>234</sup>. Teal Group's 2012 market study estimates that worldwide spending on UAVs, in all sectors, will exceed US\$ 89 billion in the next ten years<sup>235</sup>.

While drones are generally thought of as military weapons, more recently civilian applications have emerged. UAVs have been deployed in search and rescue operations, for monitoring crowds at sporting events, for traffic surveillance, threat detection of major infrastructure and wide life population monitoring. Potential civilian uses of drones within the European Union has been widely discussed. The Commission Working paper on a European strategy for the development of civilian applications of drones states that there are over 400 such applications in development across the EU<sup>236</sup>.

Environmental and ecosystem applications of drones can range from precision agriculture to mapping

<sup>230</sup> [http://justsecurity.org/wp-content/uploads/2013/10/UN-Special-Rapporteur-Extrajudicial-Christof-Heyns-Report-Drones.pdf?utm\\_source=Press+mailing+list&utm\\_campaign=6de0426c90-2013\\_10\\_17\\_Heyns\\_drones\\_report\\_UN&utm\\_medium=email&utm\\_term=0\\_022da08134-6de0426c90-286021377](http://justsecurity.org/wp-content/uploads/2013/10/UN-Special-Rapporteur-Extrajudicial-Christof-Heyns-Report-Drones.pdf?utm_source=Press+mailing+list&utm_campaign=6de0426c90-2013_10_17_Heyns_drones_report_UN&utm_medium=email&utm_term=0_022da08134-6de0426c90-286021377) accessed Jan 9<sup>th</sup> 2014

<sup>231</sup> [http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A-HRC-23-47\\_en.pdf](http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A-HRC-23-47_en.pdf) accessed Jan 9<sup>th</sup> 2014

<sup>232</sup> <http://www.lawfareblog.com/wp-content/uploads/2013/10/Emmerson-Report.pdf>, accessed Jan 9<sup>th</sup> 2014

<sup>233</sup> Armin Krishnan, *Killer Robots: Legality and Ethicality of Autonomous Weapons*. Burlington: Ashgate Publishing Company, 2009) pg 33

<sup>234</sup> United States Government Accountability Office 2012.

<http://dronewarsuk.files.wordpress.com/2012/09/us-gao--noprolieration-of-uavs.pdf> accessed 8th January 2014.

<sup>235</sup> Teal Group 2013 Market Profile and Forecast World Unmanned Ariel Vehicle Systems

<http://tealgroup.com/index.php/aboutVteal/tealVgroupVinVtheVmedia/3/66VtealV>

<http://tealgroup.com/index.php/aboutVteal/tealVgroupVinVtheVmedia/3/66VtealV> accessed 8th January 2014.

<sup>236</sup> Commission Staff Working Document: Towards a European strategy for the development of civil applications of Remotely Piloted Aircraft Systems (RPAS) Sept 2012.

<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>  
<http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2013438%202012%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F12%2Fst13%2Fst13438.en12.pdf>

coastline erosion to species and habitat monitoring. Drones equipped with cameras, communication sensors can not only capture images but can provide real time data on natural disasters and can collect and transmit meteorological data. Drones can fly into risky and treacherous areas not accessible to humans or manned aircraft. Drones have been used to collect wind speed data from the eye of hurricanes and the National Aeronautical and Space Administration (NASA) have deployed drones into the sulphur dioxide plume over the vent of the Turriabla Volcano in Costa Rica to collect data on temperature, ash height and gas concentrations which helped them predict the direction of the volcanic plume<sup>237</sup>. Drones were also used to assess damage and measure radiation levels following the damage to nuclear reactors in Fukushima, Japan. Drones are specifically being designed by Japan in cooperation with the International Atomic Energy Agency (IAEA) to monitor radiation around the tsunami-crippled Fukushima nuclear power plant and it is hoped they will be operational by 2015<sup>238</sup>.

So called "eco drones" have been used to monitor deforestation and poaching in Africa, Asia and South America. The Brazilian government invested US\$350 million in purchasing 14 drones for use by Sao Paulo Environmental Police to monitor deforestation in the Amazon, illegal fishing and mining operations<sup>239</sup>. In 2012, Google awarded the World Wildlife Fund (WWF) a US\$5 million grant to use drones, along with other technologies, to monitor movement of wildlife and track poachers. Remote aerial surveys and ranger patrols informed by analytical software will confer an advantage on rangers involved in the protection of endangered species. It is hoped that use of innovative technology such as drones will curb the illegal trade in wildlife which according to the WWF is worth US\$7-10 billion annually<sup>240</sup>.

The rapid advances in drone technologies have also sparked interest from law enforcement agencies as it would allow them to bolster their surveillance capacity. Drones could be introduced for a fraction of the cost of manned vehicles and helicopters which are limited in areas they can access. Drones equipped with cameras, communication interception and listening devices, and by linking images with facial recognition software, could continuously track individuals in a public space. The Office of Justice Programs (OJP) and the Office of Community Orientated Policing Services (COPS) in the US have provided US\$1.2 million to seven local law enforcement agencies to purchase drones for testing or use<sup>241</sup>. Drones were considered particularly suited to law enforcement because this type of aircraft had the capability to "manoeuvre covertly in areas where individual expectations of privacy are not well-defined, such as in the immediate vicinity of residences." The American Civil Liberties Union (ACLU) has expressed concerns that increased domestic deployment of drones will eventually result in routine aerial surveillance which would profoundly change the character of public life. The ACLU has called for limits and regulations to be put on law enforcement use of drones in order to avoid a "surveillance society in which our every move is monitored, tracked, recorded and scrutinized by the authorities"<sup>242</sup>.

Privacy concerns are exacerbated by developments in drone miniaturisation. Researchers have turned to birds and insects as models and have mimicked their complex aerodynamics and navigation techniques to produce micro air vehicles (MAVs). Due to their small size they can access confined spaces and navigate their interiors more effectively than ground robots, all without those under observation knowing they are there. The Defense Advanced Research Projects Agency (DARPA) in the USA has funded the development of a tiny drone called the "nano hummingbird" whose purpose is for

<sup>237</sup> <http://www.nasa.gov/topics/earth/earthmonth/volcanic-plume-uavs.html#.UtAaSvs7RM0> accessed Jan 10<sup>th</sup> 2014

<sup>238</sup> <http://www.iaea.org/newscenter/focus/fukushima/japan-report2/japanreport120911.pdf> accessed Jan 10<sup>th</sup> 2014

<sup>239</sup> Brazilian Eyes In The Sky Focus On The Disappearing Rainforest. Scientific American Oct 26th 2011

<sup>240</sup> <http://worldwildlife.org/stories/google-helps-wwf-stop-wildlife-crime> accessed on January 12th 2014

<sup>241</sup> <http://www.justice.gov/oig/reports/2013/a1337.pdf> accessed Jan 10<sup>th</sup> 2014

<sup>242</sup> <https://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf> accessed on January 12th 2014



stealth surveillance; flying through open windows and doorways. It can fly up to 11 miles per hour and can hover for up to eight minutes. With a wingspan of just six and a half inches and weighing 19g (less than a single AA battery), the hummingbird includes a video camera and communications links<sup>243</sup>.

The ability for pervasive surveillance using drone technology will not be limited to Governments, or organisations in the future. The personal drone revolution is piggy backing on the popularity of existing consumer technology particularly smart phones. Their small efficient batteries, GPS receivers and cheap memory chips have all become components of micro drones. Mass produced, miniature electronics have made drones small and cheap enough to be accessible to the individual. The French company Parrot have sold over half a million of the AR drone 2.0 since its launch in 2010. It can be operated by a smart phone or tablet and can be purchased on Amazon for around \$250. Online communities have sprung up on the internet of do-it-yourself drone enthusiasts, raising the spectre of skies full of drones for personal uses ranging from aerial photography to spying on your neighbours.

In the USA, it is illegal for to operate a drone above 120 metres and beyond the line of sight for any non-military purpose unless authorisation has been granted by the Federal Aviation authority (FAA). Between 2007 and February 2013, the FAA has issued 1,428 licences to federal and law enforcement agencies, as well as universities engaged in research projects<sup>244</sup>. In anticipation of growing drone use, Barack Obama signed the FAA Modernisation Act into law in February 2012, which tasks the FAA with opening American airspace to unarmed drones by 2015. In November 2013, the FAA published a Roadmap for Integration of Civil Unmanned Aircraft Systems in the National Airspace System<sup>245</sup>.

As in the USA, drones flying in European airspace are restricted to flying to altitudes of 120 metres, away from buildings and people and within the line of sight of the operator. The systematic use of drones for civilian purposes within the EU is currently hampered by the absence of a clear regulatory framework, incorporating rules for certification and operational control as well as data collection and transfer. Flight authorisation for drones are issued on a case by case basis and are limited to segregated airspace. A number of Civil Aviation Authorities in Member States have issued national regulations which are not necessarily aligned, thereby further contributing to the fragmentation in EU wide regulatory approach. The European Commission conducted a consultation on the future of remotely piloted aircraft systems (RPAS) between 2009 and 2012. One of the outcomes of this consultation was the establishment of a European RPAS Steering Group tasked with designing a roadmap for the safe integration of RPAS for civilian uses into European airspace by 2016. The steering group produced their final report in June 2013, in which improvements to the existing regulatory framework were identified and a strategic R&D plan was presented, identifying research activities and technologies necessary for the safe integration of RPAS into European airspace. The roadmap also addresses the societal impact of drones and recognises that public acceptance of this technology is dependent upon proper levels of responsibility and accountability.

On Nov 19th 2013, the defence ministers of seven EU member states (France, Germany, Greece, Italy, the Netherlands, Poland and Spain) signed a letter of intent requesting the European Defence Agency (EDA) to study the requirements and costs of a future EU surveillance drone that could be produced after 2020. The European Council at its December 2013 meeting "welcomed cooperative projects supported by the European Defence Agency in the areas of remotely piloted air systems"<sup>246</sup>.

---

<sup>243</sup> <http://www.avinc.com/nano> accessed on January 12th 2014

<sup>244</sup> United States Government Accountability Office Feb 2013 <http://www.gao.gov/assets/660/652223.pdf> accessed on January 12th 2014

<sup>245</sup> [http://www.faa.gov/about/initiatives/uas/media/UAS\\_Roadmap\\_2013.pdf](http://www.faa.gov/about/initiatives/uas/media/UAS_Roadmap_2013.pdf), accessed on January 12th 2014

<sup>246</sup> <http://european-council.europa.eu/home-page/highlights/security-and-defence-policy-high-on-the-agenda-at-the-european-council?lang=en>, accessed on January 12th 2014



## 2.4.5. Research

An ever growing number of people today have access to research materials, technologies or knowledge suitable for misuse. Furthermore, science today is progressing in areas (e.g. security research proper but also synthetic biology, nanotechnology) where misuse could have substantial and widespread impacts for humans, animals, plants, economies and societies. Action by public authorities, with due attention to ‘who guards the guardians’, is of paramount importance.

Research is traditionally more or less unregulated, but some restrictions are in place. EU funded research is subject to ethical evaluation, where research ethics is taken into account. In “*A comprehensive strategy on how to minimize research misconduct and the potential misuse of research in EU funded research*” two of the main areas of concern regarding misuse are “*Application and development of surveillance technologies*” and “*Data mining and profiling technologies*.” It should a.o. be ensured that EU standards on data protection are met by non-EU applicants and to ensure that technical and/or organizational safeguards are introduced so that results can only be employed in an EU ethics standards compliant manner.

The issue of research security and of the potential misuse of research has received renewed attention in recent years, notably as a consequence of the impact such misuse has had on the general public and as a consequence of the growing realization of its potential impact.

The Amerithrax case in the United States<sup>247</sup> in 2001 has not only cost the lives of 5 persons but also created economic damage estimated to be in the area of 1 billion Dollars (cf. *2010 report on misconduct and potential misuse of research*). The need to safeguard against such misuse has led to numerous legislative initiatives in various countries. It has also stimulated the discussion among scientists, scientific institutions and publishers to establish and implement codes of conduct to minimize the risks of misuse of research. Several funding institutions have developed and established such oversight mechanisms to ensure that the risks for such misuse are minimized.

In addition to the context of terrorist and unethical military use of research other areas of potential misuse have created concerns in recent times. Stigmatization and discrimination of individuals or groups of individuals is one example. National legislators in several countries, for example, have introduced new legislation safeguarding against such misuse in the context of genetic data.

---

<sup>247</sup> <http://www.fbi.gov/about-us/history/famous-cases/anthrax-amerithrax>

The recent gain-of-function experiments in Europe have also shed new light on the importance of re-thinking and establishing appropriate oversight mechanisms for research activities susceptible to being categorised as Dual Use Research of Concern (DURC) – research which is intended for benefit, but which might easily be misapplied to do harm.

Another key example is the potential misuse of modern Information and Communication Technologies for unethical purposes which has been the driving force for legislators to continuously update and develop new legislation mainly in the context of personal data protection to safeguard against such misuse. However, as research progresses sophisticated new tools are developed, that may allow the re-personalization of previously anonymous data (e.g. deep mining, image reconstruction technologies). To balance the needs between security and the risks to privacy for such technologies will remain a continuous challenge for ethics reviewers as well as legislators.

## 2.5. Regulatory concerns, challenges and possibilities?

The regulatory concerns seen from an ethical perspective are mainly:

- \* How are the ethical principles balanced in the regulation?
- \* From an ethical perspective, is more protective regulation needed?
- \* How can the global challenges be dealt with?
- \* Which governance possibilities should be considered?

### 2.5.1. How are the ethical principles balanced in the regulatory landscape?

The regulatory landscape seems to be focusing primarily on global protection of *human rights*, including *privacy*, but with quite different levels, accuracy and efficiency of protection.

*Privacy* protection is growing globally. Protection within the European context seems more profound than elsewhere, with more precise exceptions and a range of interpretations from the European Court of Human Rights. Nevertheless, the importance of privacy protection is still conditional on the ability to keep pace with the development in technologies and to secure a “reasonable” balance between privacy and interests of national security, public safety, prevention of crime etc.

Despite the widespread recognition of the obligation to protect privacy, the specific content of this right has not been fully developed when it comes to the balance against security. The lack of explicit articulation of the content of this right has contributed to difficulties in its application and enforcement. As the right to privacy is a qualified right, its interpretation

raises challenges with respect to what constitutes the private sphere and in establishing notions of what constitutes public interest. The rapid and monumental changes to communications and information technologies experienced in recent decades have also irreversibly affected our understandings of the boundaries between private and public spheres.

The UN Special Rapporteur Frank La Rue stresses that “national security and criminal activity may justify the exceptional use of communications surveillance technologies. However, national laws regulating what would constitute the necessary, legitimate and proportional State involvement in communications surveillance are often inadequate or non-existent. Inadequate national legal frameworks create a fertile ground for arbitrary and unlawful infringements of the right to privacy in communications and, consequently, also threaten the protection of the right to freedom of opinion and expression.”<sup>248</sup>

The crucial regulatory dilemma is the tension and balance between protection of privacy and autonomy on one hand and restrictions based on protection, national security and criminal activity on the other. This dilemma is primarily the very general, uncertain and often undocumented notion of “security” as a legal reason for limiting privacy. More clarity and expansion of the documentation and more explicit balancing seems to be crucial points for the legal challenge seen from an ethical perspective. Moreover, security plays a role as a negative right to be protected against intrusion from the state, but does not seem to imply the stated principle of security as a positive right. Finally, the absence or inadequacy of governance in the area of surveillance presents a problem.

### **2.5.2. Is more regulation needed?**

Loopholes therefore exist primarily in the field of implementing privacy, balancing privacy against security and introducing governance schemes in the area of surveillance, including drones.

As regulation in the area of surveillance is scarce - also in an EU context - it should be considered whether more regulation or other forms of governance would be appropriate.

On the *global* scale the United Nations Special Rapporteur on the promotion and protection

---

<sup>248</sup> Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, United Nations, General Assembly, 17. April 2013 /A/HRC/23/40). Human Rights Council, twenty-third session, p. 3:  
[http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40\\_EN.pdf](http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf)

of the right to freedom of opinion and expression, Frank La Rue has expressed concerns about surveillance in the area of telecommunications etc.<sup>249</sup> The aim of his report is “to identify the risks that the new means and modalities of communications surveillance pose to human rights, including the right to privacy and the freedom of opinion and expression.” Some of his concerns are also relevant in the European context. He stresses the need for more regulation in the area of surveillance: “Communications techniques and technologies have evolved significantly, changing the way in which communications surveillance is conducted by States. States must therefore update their understandings and regulation of communications surveillance and modify their practices in order to ensure that individuals’ human rights are respected and protected.”

“Communications surveillance should be regarded as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy and threatens the foundations of a democratic society. Legislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority. Safeguards must be articulated in law relating to the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law.

Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State. Recognizing that advance or concurrent notification might jeopardize the effectiveness of the surveillance, individuals should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath.

Legal frameworks must ensure that communications surveillance measures:

- (a) Are prescribed by law, meeting a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee their application;
- (b) Are strictly and demonstrably necessary to achieve a legitimate aim; and
- (c) Adhere to the principle of proportionality, and are not employed when less invasive techniques are available or have not yet been exhausted.

States should criminalize illegal surveillance by public or private actors. Such laws must not be used to target whistle-blowers or other individuals seeking to expose human rights violations, nor should they hamper the legitimate oversight of government action by citizens.”

The proposals made by the UN Special Rapporteur are of interest to the European context, even if they are primarily focusing on the global challenges.

---

<sup>249</sup> Ibid.

The current legal systems (in Europe and elsewhere) were not designed for contemporary techniques of surveillance. This has as a consequence, that the regulation is not coherent and that a number of problems remain unsolved. This is obvious when the global situation is taken into account, but also to some extent covers the EU situation. The national regulations seem to have the same problem, not being geared for the new technologies and uses and regional and global solutions are missing. The topic is, however, on the agenda in many countries and thus it may be timely to propose regulation in the area.

### **2.5.3. How should the global challenges be dealt with?**

One of the starkest lessons to be drawn from recent disclosures regarding mass surveillance is the need for a global solution regarding security and surveillance. The growing frequency of global data transfers in the context of security and law enforcement cooperation poses a risk where there is an absence of common privacy and data protection standards. Moreover, recent evidence points to practices of ‘privacy shopping’ by state services wishing to capitalise on weak regulatory oversight and loopholes in the legal regimes of international partners. However, realising an international solution poses significant challenges given the many efforts to reach global consensus on global governance in a number of areas, where the need for global solutions are acknowledged.

Based on these experiences and a realistic approach, it may be a better process to make bilateral agreements with as many countries as possible. It would be obvious to start with other EU countries and of course the US is also a natural partner for consensus building with the EU (countries). In this respect public diplomacy would form an appropriate point of departure.<sup>250</sup> In this direction, the European Parliament has issued a strong call for the EU and US to continue negotiations on a framework agreement on data protection in the field of police and judicial cooperation and to review existing EU data transfer agreements with the US.<sup>251</sup>

---

<sup>250</sup> M. Leonard, *Public diplomacy*, London, 2002; J. Melissen, ed. *The New Public Diplomacy, Soft Power in International Relations*, New York, 2005; J. S. Nye, *Soft Power. The Means to Success in World Politics*, New York, 2004.

<sup>251</sup> European Parliament LIBE Committee report on the US NSA surveillance programme, surveillance bodies in various member states and their impact on EU citizens’ fundamental rights and on transatlantic cooperation in Justice and Home Affairs.

#### 2.5.4. Which governance possibilities should be considered – the “tool-box”?

The tension between privacy and the (new) technologies has primarily been approached by using four instruments: Technology, Education, Self-regulation and Law.<sup>252</sup> In this chapter focus has been on governance solutions, but other tools can also be relevant.

*Technology governance* is based on the presumption that the problem of the global character of information can best be circumvented by solutions that come from technology itself. Thus the problem of personal information being disseminated worldwide through information and communications networks, that is when technology involves processing operations carried out by different actors located in different countries under different jurisdictions, can best be overcome. In such cases it becomes difficult to identify correctly any applicable privacy or data protection rules and to have access to those authorities entitled to enforce them. A well-known way of using technology in this respect is *Privacy enhancing technologies (PET)*, where the risk of contravening privacy principles and legislation is reduced by a specific technology. Other well-known technology governance instruments are Privacy by Design (PdB), Privacy in Design (PiD), Privacy Impact Assessment (PIA) and Surveillance Impact Assessment (SIA).

*Self-regulatory governance* works to promote (virtuous) behaviour by involving stakeholders and establishing bottom-up soft regulations. Usually self-regulatory governance relies on a mix between market and self-regulation. Corporate Social Responsibility (CSR) and governmental incentives for research can drive technology forwards towards more ethical development. Ethical codes and CSR have, however, limited importance in the security field. An example is the UK Code on CCTV mentioned above and other soft law instruments, including codes of conduct could be set in place.

*Traditional regulation* is effective in the sense that hard law can be enforced, but there are also challenges. One challenge concerns universal norms, which often tend to be too vague, abstract and difficult to operationalize. A good example is the principle of proportionality, where reasons come in many forms and traditions, and there can be disagreements about how to weight competing interests and the metrics to be used for assessing outcomes. Legislation may be interpreted and thus specified by Court decisions.

In the area of *surveillance* the EU may take initiatives to place this on the agenda and encourage the member states to enact or revise regulations in the area. It seems important

---

<sup>252</sup> "Ethical and Regulatory Challenges to Science and Research Policy at the Global Level." European Commission, 2012.

to make sure that not only public surveillance but also surveillance by private parties is subject to regulation. A more process-oriented approach might be to start with self-regulatory measures - soft law. The UK Code of Conduct and experiences from other areas may serve as an inspiration.

*Consent* is often used as precondition for actions, but in the area of surveillance, border control etc. this presents a problematic solution, as the purpose of surveillance and border control often cannot be fulfilled, if consent is claimed. Therefore regulation is called for to secure other forms of protection.

*Human Rights* and protection of *privacy* are crucial in the regulatory picture now and probably also in the future. If privacy is seen as paramount it may be considered to expand, specify, control and implement privacy to a further extent. Europe seems to be at the forefront when it comes to privacy and data protection. Global collaboration would be fruitful in this respect as many of the challenges are global. However, to kick-start the global solutions, bilateral consensus-making, based on public diplomacy may be the best way forward at this stage.

Expansion might be part of a global procedure, trying to achieve more consensus on the extent and content. Specification may be relevant regarding balancing of privacy against security etc. Based on the proposal from the UN Special Rapporteur it may be a proposal that the right to privacy can be subject to limitations, if they inter alia, include the following elements: The restrictions are provided by law; the essence of a human right is not subject to restrictions; restrictions must be necessary in a democratic society; and must conform to the principle of proportionality, must be appropriate to achieve their protective function, must be the least intrusive instrument amongst those which might achieve the desired result, and must be proportionate to the interest to be protected. Control and implementation may also be on the agenda.

Exchange of experience between the Member States to try to achieve a wider consensus should be set in place. Moreover, a special person or institution to control, criticise, propose and persuade might turn out to be fruitful.

## **2.6 Conclusion**

The EU regulatory landscape regarding security and surveillance as a whole seems scattered and uncertain in many ways. The primary EU governance instruments have as a purpose to protect human rights, including privacy and data protection. While human rights and privacy to a large extent are global rights, the EU is at the forefront when it comes to

strong protection of privacy and data - partly as a consequence of the European Court of Human Rights and its dynamic interpretations. There are also a number of EU governance instruments regarding aviation, border control and cybercrime – also to some extent as global provisions.

The challenges and possibilities are primarily the following:

1. There is a difficult tension and balancing between human rights and privacy on the one side and national security and crime prevention on the other side. Privacy is being limited for security reasons, but often the governance provisions are very vague and the solutions casuistic. This challenge could be met by providing more robust rules in the area introducing more precise conditions for the balancing.
2. Some areas of national security and surveillance, which largely remain the competence of the member states, present challenges regarding protective governance measures. Of special interest are surveillance cameras – CCTV – and surveillance regarding telecommunication. The national regulations differ, but it seems to be a common concern that the governance measures are not sufficiently robust and protective. The possibility could be to make sure, that limitations and permits are in place regarding CCTV and oversights and judicial review regarding surveillance of telecommunications.
3. New technologies introducing surveillance, such as drones, present challenges as the current regulation may not be adequate.
4. Whistleblowing is on the agenda, and in many European countries expanding of governance measures to protect whistle-blowers are leading to expanded protection using traditional regulation.
5. More international cooperation on the governance level could lead to an improved legal protection in crucial areas.



## Chapter 3 Ethical analysis

### 3.1. Historical and socio-political perspectives

#### 3.1.1. The evolution of the concept of security

##### Sine-cura in pre-modern reflection

An initial underpinning of the contemporary notion of security is the *sine cura* (from Latin *securus* “without care, safe” from *sine* or *se cura*, from *se* “free from” and *cura* “care”, also “concern, trouble”). In this antiquity context, this state of security, of peace of mind, was the goal that diverse philosophies of ‘ataraxy’ (stoicism, epicurism, scepticism) were striving for. Three elements of tension are particularly important to note with regard to the inception of the concept. Firstly, the tension between security as freedom from worry, insouciance, carefreeness and security as carelessness, indifference, incaution.<sup>253</sup> Secondly, the emphasis placed in this context on the subjective and internal dimensions with regard to achieving this state of security (in contrast to extraneous realities). Thirdly, the duet of very different notions of security that followed from this early development: the first one brings us to the way in which security is most commonly understood today referring to a condition of safety, of being protected, free from danger; the second one refers to security as a condition of false or misplaced confidence in one’s condition or position (James Der Derian remarkably evidenced this meaning of security through quotes from, for instance, Shakespeare’s *Macbeth* – “security is mortals’ chiefest enemy” – and a number of sermons from the sixteenth to the nineteenth century, highlighting the way in which the word was used negatively where one must guard against the sin of security or suffer the consequences) and is thus in a way antithetical to the first.<sup>254</sup>

---

<sup>253</sup> Michael Dillon, *Politics of Security: Towards a Political Philosophy of Continental Thought*, London: Routledge, 1996.

<sup>254</sup> The developments in this section on the evolution of the concept of security build upon Frédéric Gros, *Le Principe Sécurité*, Paris: Gallimard, 2012 and Jim Dratwa, “Risque, Rixe, Rhizome: Guerre et Paix avec l’Analyse des Risques et les Organisations Internationales”, *Techniques et Philosophies des Risques*, ed. G. Hottot & C. Kermisch, Paris: Vrin, 2007.

## **Social contract, security and the role of the State**

In ancient and medieval thought the concept of security was subordinated to the achievement of ethical and religious ends of the individual and political community. The problem of security becomes central with the secularisation of modern political thought and the birth of the modern state. The State is the place where security is guaranteed; security is justified –and ruled– by the so-called ‘reason of State’.

The early 16<sup>th</sup> century dramatically transformed the (European) security framework. Security shifts to being considered a political problem, relating to external protection from war and violence. Machiavelli (*The Prince*, 1513) analysing the phenomenon of security of state (principality), envisaging security as a reaction to risks, threats, challenges and dangers to guarantee safety for the citizens in the state, identifies it with the exercise of absolute political power.

Thomas Hobbes (*Leviathan*, 1651) considers the state of nature as the original condition in which the instinctive individual acts freely and selfishly according to his own interests (self-preservation). Hobbes thematises the transition from the state of nature to a civil state as essential to overcome the intolerable condition of constant danger, conflict and aggressiveness (*homo homini lupus*), which creates individual fear and social insecurity. The recognition of man’s natural desire for security justifies the civil state: in order to secure self-protection (conservation of life and peace) a social contract is agreed, that is a pact of *unionis* and *subjectionis*; the citizens associate and, at the same time, renounce a part of their freedom, delegating it to the sovereign who acquires an absolute power in order to guarantee security. Security becomes the goal of the citizens and the moral justification of the absolute power of the state and of the citizens’ limitation of freedom: the willingness to submit to an absolute political sovereign is justified only by the preservation of security, that is preservation of life and peace, protection from (fear of) death and violence.

Spinoza (*Political Treatise*, 1677) considers security as the origin and purpose of the state: the state comes into being because social order (peace) - ensured through the threat of force - is a necessary (albeit not sufficient) condition for the realization of the individual’s desire for safety (self-preservation) and wellbeing.

In opposition to the absolutist perspective, John Locke (*Second Treatise of Government*, 1690) interprets the concept of security and social contract in a liberal framework: the state of nature is a condition in which innate natural laws exist (life, health, liberty, property, equality)

which, due to their precariousness, must be guaranteed by the constitution of a social state, through a social contract. Precariousness means insecurity in the state of nature due to the absence of the state that guarantees – through laws and judicial impartial punishment with regard to the transgression of laws – security. Security is identified with peace (the preservation, maintenance and reinforcement of natural rights), that is conservation of life and health, enjoyment of liberty and property, preservation of equality.

Even if it is in a different theoretical context (of absolutism and liberalism), in the school of natural law security is theorized with some common elements: 1) condition and legitimation of political power; 2) justification of the social contract as a voluntary renunciation of a part of freedom in order to be safe and free in a peaceful society; 3) protection from external threats (violence, war).

It is in the 19<sup>th</sup> century that 'political security' is enriched through 'social security' and the welfare state as such. The notion of welfare state is intimately connected to both individual security and state security. The German term Sozialstaat ("social state"), for example, has been used since 1870 to describe state support programs devised by German Sozialpolitiker ("social politicians") and implemented as part of Bismarck's reforms. The literal English equivalent "social state" never caught on in Anglophone countries, until the Second World War, when Anglican Archbishop William Temple (author of the book *Christianity and the Social Order*, published in 1942) popularized the concept using the phrase "welfare state", contrasting wartime Britain's welfare state with the "warfare state" of Nazi Germany.

### **Post WWII, mutually assured destruction and international relations theory**

It is important to pay attention not only to the evolution of the geopolitical configurations but also to the evolutions of the *Weltanschauungen* (visions of the world), narratives and modes of thought with which they are understood or made sense of.

One should note the close association of the Cold War with the advent and establishment of 'security studies' as such as a discipline or academic field. In that regard, WWII marked a watershed in the presumed interest and capacity of states to protect their own citizens from physical harm. Whereas the original principle of sovereignty was a peculiar bargain whose chief benefit was reducing the likelihood of interstate war and, by extension, the mass killing (or other harm) of people, after WWII it became conspicuously necessary to abridge the principle of sovereignty in order to protect the lives of ordinary people (minorities notably) who in previous centuries would have been protected (as a matter of principle, at least from

physical harm) as supports to state power. This also sparked a great deal of contestation over the meaning of 'security' (and indeed over whether states – the classic unit of attention for international relations theory – remain as useful as foci of interest and explanation).

It is important to bring to light the connections between the 'social contract' examined above and the tensions discussed subsequently in the opinion between different framings of security, with regard to "trade-offs" as well as with regard to individual security in relation to state security. Firstly, social (or political) contract arguments classically posit that individuals have consented, either explicitly or tacitly, to surrender some of their freedoms and submit to the authority of the sovereign (or to the decision of a majority) in exchange for protection of their remaining rights. Here it is crucial to note that the social contract thus traces the "original sin", the original trade-off which underpins those that follow.<sup>255</sup> Focussing now on Hobbes' conceptualisation, as indicated above, the social contract was an occurrence in the course of which individuals came together and ceded some of their individual rights so that others would cede theirs – i.e. a mutualised trade-off. This resulted in the establishment of a sovereign entity, the state. Yet the system of states grown out of the social contract was also anarchic in that states had no leadership with respect to each other. The same way that, in the state of nature, the individuals had been sovereigns guided by self-interest and the absence of rights, so states now acted in their self-interest in competition with one other. As in the state of nature, states were thus bound to be in conflict because there was no sovereign over and above the state capable of imposing some system on everyone (such as social-contract laws) by force. It is on those bases that Hobbes' work served as a foundation for the realist theories of international relations – as advanced by E.H. Carr and Hans Morgenthau – in the middle of the Twentieth Century.

Giorgio Agamben – in his oeuvre as in his intervention on the occasion of the public Open Round Table in the context of the development of the present Opinion – draws attention to an array of grave difficulties whenever engaging with security. In *Homo Sacer: Sovereign Power and Bare Life* and in *State of Exception*, Agamben traces the concept of "state of exception" (*Ausnahmezustand*) used by Carl Schmitt (whose "Sovereign" is the one who has the power to decide the state of exception) to Roman *justitium* and *auctoritas*. Whereas

---

<sup>255</sup> It should also be noted here that "the name social contract (or original contract) often covers two different kinds of contract, and, in tracing the evolution of the theory, it is well to distinguish them. Both were current in the 17th century and both can be discovered in Greek political thought. ... [The first] generally involved some theory of the origin of the state. The second form of social contract may be more accurately called the contract of government, or the contract of submission...." J. W. Gough, *The Social Contract*, Oxford: Clarendon Press, 1936, pp. 2-3. In other words the first is concerned with the origin of the state, while the second concerns the

Schmitt aims to include the necessity of state of emergency under the rule of law, Agamben demonstrates on the contrary that all life cannot be subsumed under the law. Agamben examines the increases of power which governments resort to in supposed times of crisis. In such times of crisis, he refers to these extensions of power as *states of exception*, in which matters of citizenship and individual rights can be put down or disqualified in the process of extension of its powers by a government – albeit in the name of ensuring security. The political power over others acquired through the state of exception places a government (or branch of government) as all-powerful, operating outside of the laws. During such times, certain forms of knowledge are then favoured and accepted as true and certain voices are heard as valued and valuable, while others are not. This oppressive distinction is of great importance with regard to the production of knowledge. The process of both acquiring knowledge, and suppressing certain knowledge, is a violent act in times of crisis. Furthermore, Agamben examines how the suspension of laws in a state of exception – of emergency or crisis – can become a continued state of affairs.

Giorgio Agamben also draws attention to how modern liberal economics has contributed to push from a prevention perspective towards a “laissez faire” approach in which one has to manage the effects (rather than the causes) of issues or risks or crises – and consequently to surveil and control – in the name of security. An underlying question is whether this is compatible with democracy.

### **Post September 11 and post March 11**

These evolving geopolitical configurations can also be seen in regard to evolving conceptions of security. While classical approaches to security (materialist approaches in security studies in international relations) focus on the material dispositions of the threat including the distribution of power, military capabilities and polarity, the ‘securitization’ approach scrutinizes how a certain issue is transformed by an actor into a matter of security. Such a move enables such an actor to use extraordinary means in the name of security. An example from this securitization scholarship is the immigration debate in the United States, notably. Concerns of terrorist infiltration are regularly cited as grounds for the tight control of borders. Because it is easier to ‘securitize’ an issue (i.e. frame it as a security issue) following September 11, this concern for safety and security has taken attention away from the socio-economic factors at play in international migration and from the ‘root causes’ discussion.

---

contract – the *modus vivendi* – between the ruler(s) and the ruled, between the governed and the government. This duality of the social contract is at the heart of David Hume's critique of the concept.

Similar trends have been discussed with regard to the European context, where the rationale for strengthening of border control and establishing border surveillance technologies are bound up with the fight against transnational criminal threats such as terrorism, drug trafficking, and human trafficking and smuggling. A securitisation dynamic has thus been discussed with regard to the way in which the undesired form of human mobility known as irregular migration is re-framed in a European setting and placed on a continuum of threats alongside organised crime and terrorism – and against which practices of surveillance, control and penalisation are brought in or endorsed as necessary and legitimised.

Against this backdrop, the turn of the millennium or the end of the 20th century also marks, in the European imaginaries, a milestone on the journey of (re)unification of the continent and of its people(s), the curtain dropping on the Iron Curtain, and the hopeful move away from a period not only of division but also of totalitarianism (under the yoke of a state apparatus underpinned by pervasive intelligence and security services), away from the good intentions paving a road to hell, not just under Nazism and Stalinism. Still holding those turned pages in their hands, Europeans bear in mind Ceaușescu's *Securitate* – and indeed that *Stasi* (the *Staatssicherheit* secret police) literally means "State Security".

### **Security research, risks and the state**

Security not only forms part of the fabric of the human rights framework, it is also the cornerstone of the social contract ; be it for Hobbes, Locke, Spinoza or Rousseau, all those theorists of politics have made civil safety, civil security, the motive and end of the social contract,<sup>256</sup> as discussed above. Civil security denotes, in this perspective, the right for everyone to be preserved from the risk of violence. In counterpoint, this also lays the groundwork defining a state which holds, in Max Weber's terms (in *Politics as a vocation*), the monopoly on the legitimate use of violence or force. Furthermore, it finds a particular resonance in a context of 'risk society' as reflected upon by Ulrich Beck, where – contrary to the 'industrial society' where the determining issue was the (un)fair distribution of goods – the determining issue is the distribution of 'bads', of risks. What sort of *state of safety* are the members of the risk society calling upon? What would it mean for the state to successfully claim a monopoly on the legitimate use of risk? And on the legitimate assurance of security? And then what if the state was to 'unbundle' – disaggregate or sell away – its oligopolistic prerogatives or claims as to the legitimate use of force?

---

<sup>256</sup> Kriegel B., "Le risque de développement", Philosophie Politique 11, Paris, PUF, 2000; Guéry F., "Risque, Assurance, Sécurité", Philosophie Politique 11, Paris, PUF, 2000.

Sciences and technologies are at the heart of the relation between the Public and the State as mediated through notions of legitimacy and security. This powerful finding – dating back to Max Weber and even Aristotle – has been compellingly documented in the work of James C. Scott (Scott 1998) as well as Yaron Ezrahi (Ezrahi 1990).<sup>257</sup> His is a characterization of the democratic state as ceaselessly seeking to legitimate itself through scientific and technological performances (e.g. large scale projects, ‘modernisations’, institutionalization of scientific expert advice). The classical promise of Progress is a marker of these ties between science and the state, jointly resting on that very promise. In contemporary settings this mustering of research and development and innovation takes the stylised form of twin undertakings, one to unlock competitiveness, growth and jobs and the other to address grand societal challenges. Both of these undertakings are further meant to feed one another, the latter through generating new business opportunities delivering the former, and the former through generating more capital to invest in the latter.

The flipside of this arrangement is the matter of unwanted and/or unanticipated consequences, be they framed as ‘externalities’ or ‘risks’ as above. Hence also the crucial and oft-obfuscated matter of the distribution of the benefits, costs and risks of these endeavours of sciences and new technologies (and of course hence the need to develop adequate ethical and regulatory frameworks for all such endeavours).

In turn then, it is the obverse of that flipside that is represented by security research<sup>258</sup> and the development of security technologies. They carry in themselves –albeit as a project or promise– the advanced resolution of the above predicaments. Yet they also carry in themselves the ambiguities and tensions constitutive of the very concept of security (and it is precisely those constitutive tensions that have been scrutinized in the previous sections of this Chapter).

### **Rise of the Human Security Doctrine**

Traditional security paradigms, under the head of ‘national security’ or ‘state security’, pertain to a state's ability to defend itself against external threats. This follows the philosophy of international security predominance since the Peace of Westphalia in 1648 and the rise of

---

<sup>257</sup> Scott, James C., *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*, New Haven, CT: Yale University Press, 1998; Ezrahi Y., *The Descent of Icarus: Science and the Transformation of Contemporary Democracy*, Cambridge, MA: Harvard University Press, 1990.

<sup>258</sup> It is interesting to consider here the notion of ‘research as policymaking’ – i.e. that on occasions surveillance policies begin life as research projects (EUROSUR being here a prime example). The funding of security and surveillance technologies and projects sometimes evades having an open debate which takes into consideration the politically sensitive nature of the problems that these technologies are intended to solve.

the nation-states. While international relations theory classically spans many variants of traditional security, the fundamental trait that these variants share is their adherence to the primacy of the nation-state.

Human security, in contrast to those approaches, holds that the proper referent for security should be the individual rather than the state. This paradigm for understanding global vulnerabilities holds that a people-centred view of security is necessary for national, regional and global security.

In part responding to the gaps in the human security doctrine, the notion of 'societal security' is an interesting enrichment with respect to other understandings of security, and has made some inroads primarily in the field of international relations and security studies (with migration as a common sub-theme). Rather than the individual as the primary referent of security, this perspective examines society as the object of security threats, with society here understood as the set of values, customs, shared experiences, economic institutions and legal and artistic traditions – essentially the organic and collective life of a community. Societal security has been defined as "the ability of society to persist in its essential character under changing conditions and possible or actual threats" (Buzan, Waever and De Wilde, 1998).<sup>259</sup> Societal security, like human security, aims to respond to the changing landscape of threats which no longer reflect the traditional state-security logic. It focuses less on keeping external threats out or ensuring protection from physical harm than on the need for societal resilience against insecurity. Societal security moves beyond an individual-centred notion of security and puts a primacy on the societal sources of well-being.

With regard to human security as such, the United Nations Development Programme's 1994 *Human Development Report* is considered a milestone publication in the field of human security, with its argument that insuring "freedom from want" as well as "freedom from fear" for all persons is the best path to tackle the problem of global insecurity. The Report argues that the scope of global security should be expanded to include threats in seven areas: *economic security, food security, health security, environmental security, personal security, community security, political security*.

In 2003, the United Nations established the *Commission of Human Security*, whose 'Human Security Doctrine' (HSD) became the reference point for most security strategies. The HSD

---

<sup>259</sup> Buzan, Barry, Ole Waever, and J. de Wilde, eds. *Security: A New Framework for Analysis*, Boulder, CO: Lynne Rienner, 1998.



argues for a paradigm shift from understanding security based on tangible assets (such as national borders, goods, properties) to one based on intangible human values.

In 2004, the *Study Group on Europe's Security Capabilities* convened by Javier Solana put forth the 'Human Security Doctrine for Europe' as a policy framework for the European Security Strategy, building on the above UN approach.

While the HSD carries genuine wisdom and seemingly comprises more ethically elaborate features than traditional 'national security' doctrines, it proceeds by conflation and circularities which may both obfuscate the tensions inherent to the 'security' concept and expand its scope towards totality. In this equivocal move, which also places security as the ultimate *telos*, 'securitization' takes on a striking new form and the 'state of exception' (or state of emergency) finds a striking new justification.

### **3.1.2. The tensions structuring/pervading the notion of Security**

What can be seen from this short overview over the history and political conceptualization of security is that the tension between the private and social sense of security, and the political, public, and military sense. At the turn of the Millennium, the hope was certainly to broaden the political, public concept in order to embrace the social approach to security. This was in line with the Millennium Goals, which addressed the challenge of global poverty and the lack of development. Security in the 'social' sense was regarded as one, if not the most important means to international peace.

But it took only one decade for the 'older' framework to re-emerge and re-define the concept of security in the 'political' understanding of securing the public sphere. Individuals felt threatened after several terror attacks and the rise in prominence of international terror groups. Security threats became the 'other side' of globalization, and the notion that politics must respond to these threats by increasing the measures of surveillance gained momentum. Whether this was the appropriate response, and whether the threat by terror groups was used in order to develop a security system that enabled states to surveil citizens to previously unknown degrees, is beyond this report; this will certainly be scrutinized by historical studies. But it is clear that a more societal approach ended up demoted following the 9/11 attacks. And as surveillance technologies became more and more sophisticated, it seemed indeed possible to provide the means to secure the public sphere in this sense. Different from 20<sup>th</sup> century security policies, however, globalization turned the 'national public sphere' into a *global* public sphere, a public sphere that ignores national borders and/or national laws.

Political philosophy throughout modernity has argued that at least in democratic states, the elected representatives are bound by the 'people's will', and that they are therefore held accountable for their actions. This has turned out to be a challenge under the new security policies, and justifications of secrecy and non-transparency have turned once again to the argumentation of 'exceptional circumstances' or 'state of exception'. The question today is whether this argumentation has in fact become the defining argumentation for the politics of security, how accountability can be maintained, and how two decisive changes can be interpreted: these are, on the one hand, the intersection of political and private uses of security & surveillance technologies, and on the other hand, the development of ICT-based practices in our social life. Both developments challenge the view that the 'sovereign' is making all the decisions concerning security. Rather, it is exactly the inter-relation of sovereignty and non-sovereignty of the elected representatives (and of states, corporate entities, individuals) that needs to be re-defined.

Another change concerns the transnational nature of ICT: security and surveillance need to be addressed first as 'internal affair' of the member states of the European Union, second as transnational practices which go beyond the democratic control of a member state but also beyond the European Union, and third as international affairs based upon international treaties. The tensions between the subjective, social, and political concept of security will play out on all three levels.

The overall subjective or private sense of 'feeling secure' in one's environment, the social concept of 'having secured' or 'securing' the necessary means of one's existence, and the political provision of public security cannot be separated. The very fact that they are entangled with each other, may, especially in view of recent experiences, render one approach more prevalent than the others, and yet: they need to be continuously correlated and balanced against each other.

## 3.2. Ethical Concerns, Considerations and Concepts

### 3.2.1. Security, surveillance, fear and control

*“Perhaps encouraged by technological advancement, scientific progress, miraculous breakthroughs in medicine, or a steady decrease in crime, we may have become so infected with dreams of invulnerability or possible deathlessness that we would deny our very human nature. The obsessive concern for security could be read as an attempt to distract ourselves from a frightening admission of our mortality, an apotropaic gesture aimed at warding off what can never be prevented, or a vain hope in the perfect efficacy of our calculations.*

*In her recent memoir, *Insecure at last*, Eve Ensler frustratingly relates the problem of security to a desire to transgress our human finitude:*

*‘What does anyone mean when they speak of security? Why are we suddenly a nation and a people who strive for security above all else? In fact, security is essentially elusive, impossible. We all die. We all get sick. We all get old. People leave us. People surprise us. People change us. Nothing is secure. And this is the good news. But only if you are not seeking security as the point of your life.’*<sup>260</sup>

After the revelations of the Prism activities many were shocked. Shocked because of the loss of the sense of trust, dignity and privacy. Shocked because fundamental human rights are at stake. The revelations regarding the surveillance of EU heads of state all the more emphasize that there is a serious ethical crisis with severe political repercussions. It also emphasizes that the EU needs to make clear where it stands ethically speaking. Strong concerns have been expressed about surveillance of European officials, as reflected in this statement by the EU Parliament Committee on Foreign Affairs:

*“The European Union and the United States are strategic partners, and this partnership is critical for the promotion of our shared values, our security and our common leadership in global affairs. However, trust in the partnership has been negatively affected and needs to be restored. The EU, its member States and the European citizens have expressed deep concern at revelations of large-scale US intelligence collection programmes, in particular*

---

<sup>260</sup> John T Hamilton, *Security, Politics, Humanity and the Philology of Care*, Princeton UP, 2013, 28

*as regards the protection of personal data. Mass surveillance of private communication, be it of citizens, enterprises or political leaders, is unacceptable*<sup>261</sup>.

European officials have similarly expressed doubt about whether to continue the existing *Safe Harbour* agreement for transfer of personal information to the US, under which companies are able to comply with the stricter EU privacy laws.<sup>262</sup> Although the precise impact on such future negotiations is unclear, such statements show the linkage between intelligence collection decisions and international trade negotiations.

The revelations and the debate that followed made people realize that as surveillance seems to permeate all spheres of life, the public space, the working environment, even private lives, not only that of heads of state but also that of ordinary citizens; our relations with neighbours, friends, allies, fellow citizens, employers, providers of services, and governments are at stake. Detection gates at airports, GPS in mobile phones to track persons, cameras to watch the public in malls, museums and the streets, employers who install key stroke devices, Google glasses that send images to one's pc, the collection of data on the use of credit cards, customer cards or online shopping habits, computer searches, and the development of algorithms to analyse these data, the collection of digital fingerprints: people are monitored, tracked and evaluated. Modern technologies cater to gather information from the big data analysis to apps one can install when one suspects one's partner of adultery. Why are individuals, organisations, governments interested in knowing what people do? The most important reason brought forward is security and in order to provide security one needs to influence and even control. This fundamentally influences the social fabric of societies and alliances. In the words of Canadian professor of sociology David Lyon<sup>263</sup>:

*"Today's surveillance processes and practices bespeak a world where we know we are not really trusted. Surveillance fosters suspicion and thus threatens social cohesion and solidarity. (...) some of this, you object, may seem like simple prudence. But how far can this go? Social relationships depend on trust and permitting ourselves to undermine it in this way seems like slow social suicide."*

---

<sup>261</sup> European Commission, Communication from the Commission to the European Parliament and the Council. Rebuilding Trust in EU-US Data Flows, 27 November 2013 and [http://export.gov/safeharbor/eu/eg\\_main\\_018476.asp](http://export.gov/safeharbor/eu/eg_main_018476.asp)

## Airport Security Theatre

More than 1.4 billion passengers pass through Europe's airports every year. It is estimated that this will increase to 2.7 billion passengers by 2030<sup>264</sup>. Since the events of September 2001, passengers have become accustomed to carrying no more than 100ml bottles of liquids in their hand luggage, taking their shoes off as they move through newly installed body scanners and having their hands and luggage swabbed for traces of explosives. Each of these security measures were introduced following a specific security threat at an airport. The European Commission introduced the limitation on the volume of liquids and gels that could be carried in hand luggage in 2006, after the failed attempt to blow up several aircraft at Heathrow airport; the so called "liquid bombers".

The reactive nature of these measures, the significant cost entailed in their introduction and the inconvenience experienced by passengers has been the focus of much criticism. Bruce Schneier, amongst others has argued that many of the airport security measures introduced following 9/11 are simply a form of "security theatre"<sup>265</sup>. The public shocked and frightened by the events wanted something done to restore their feeling of being safe in going about their everyday business. Politicians had to be seen to be taking action in this regard, irrespective of whether the specific action would actually result in people *being* safer.

It is questionable whether the reactive measures adopted will in fact prevent future attacks. As commentators have pointed out, terrorists will simply find other means or other venues in which to perpetrate their acts. Moreover, successful breaches of existing airport security have been reported by a number of journalists, eager to demonstrate that a small amount of ingenuity is all that is required to bypass security checks<sup>266</sup>. The internet is replete with examples of how current security measures can be thwarted.

Effectiveness of security measures rather than an avoidance of fear should be the basis for engendering public trust. Trust is crucial to almost any type of situation in which either uncertainty exists or undesirable outcomes are possible<sup>267</sup>. As observed by Baroness Onora O'Neil in her 2002 Reith Lectures on trust<sup>268</sup>, "*Confucius told his disciple Tzu-kung that three things are needed for government: weapons, food and trust. If a ruler can't hold on to all three, he should give up the weapons first and the food next. Trust should be guarded until the end: without trusts we cannot stand*".

Long before the Federal Aviation Authority in the US lifted their ban on use of smartphones, computers and kindle readers during take-off and landing, passengers were disregarding the prohibition based on a distrust of the information that the practice was dangerous. Nick Bilton in a series of articles in the New York Times challenged regulators on the scientific basis for the ban<sup>269</sup>. No such case could be made and the FAA lifted the ban in November 2013.

If people are being compelled or prohibited from doing something on the basis of public security, there needs to be solid scientific data to support the contention, otherwise public trust is undermined and legitimate, evidence based interventions can be eschewed by a sceptical public.

---

<sup>262</sup> There are, understandably, different views across and within institutions in that regard.

<sup>263</sup> D. Lyon, Surveillance Society, 2008

<sup>264</sup> <https://www.aci-europe.org/policy/fast-facts.html> accessed 9<sup>th</sup> February 2014

<sup>265</sup> <https://www.schneier.com/essay-292.html> accessed 9<sup>th</sup> February 2014

<sup>266</sup> <http://www.theatlantic.com/magazine/archive/2008/11/the-things-he-carried/307057/3/>

<http://www.vanityfair.com/culture/features/2011/12/tsa-insanity-201112> accessed 10<sup>th</sup> February 2014

<sup>267</sup> Fukuyama F. 1995. *Trust: the social virtues and the creation of prosperity*. The Free Press, New York.

<sup>268</sup> <http://www.bbc.co.uk/radio4/reith2002/lecture1.shtml> accessed 9<sup>th</sup> February 2014

<sup>269</sup> <http://bits.blogs.nytimes.com/2011/11/27/disruptions-fliers-must-turn-off-devices-but-its-not-clear-why/> accessed 9<sup>th</sup>

February 2014

### 3.2.2 Control, security, protection

Dystopic fictional scenarios such as George Orwell's 1984, with the Orwellian fear of being punished for 'thoughtcrime', political writings as Bentham's Panopticon, and the present debate on security have to do with control, the knowledge necessary to be in control, what living in a state of permanent surveillance means, as well as about both the technological and moral limits of control. What does it do to individuals? Do they not flourish in freedom and the liberty to pursue their goals? Do they not flourish if they can trust people? The opposite of control is trust. If one trusts one's citizens or employees, surveillance should not be necessary and not be directed at them. To be surveyed by a person or an organization one trusted is ethically particularly more painful as one is surveyed by someone or some instance with whom one believed one shared a relationship based on trust.

The US President's Review Group on Intelligence and Communications Technologies, whose report 'Liberty and Security in a Changing World', was published in December 2013, comments on the measures to increase surveillance in the aftermath of the dramatic events of 9/11:

*"Human nature being what it is, there is inevitably a risk of overreaction when we act out of fear. At such moments, those charged with the responsibility for keeping our nation safe, supported by an anxious public, have too often gone beyond programs and policies that were in fact necessary and appropriate to protect the nation and taken steps that unnecessarily and sometimes dangerously jeopardized individual freedom."<sup>270</sup>*

The most important argument brought forward to justify different surveillance measures concerns the security of citizens: "Terrorists and criminals attack innocent outsiders, and surveillance is necessary to prevent them from harming those in need of protection. It is not about control but about protection" – or so the argument runs. Through surveillance one strives to attain the goal of security in the war against terror and crime. Watching and watching over, however, are not necessarily the same.

The theme of security, control and freedom is as old as human societies that have since time immemorial tried to keep the 'flock' within the gates and walls for their individual protection and the protection of the society itself, and 'the others' out. The need for control can also be fuelled by fear, panic and distrust. Control has to do with power and how those who survey influence the behaviour of the surveyed. As described in chapter 1, the technologies function

in a global world, not in a single society. There is an interconnectedness of technologies and ethical problems that of course influences the debate.

### Google Glasses

Technical developments such as smartphones, car-navigation systems and portable laptops have increased the ability of individuals to efficiently navigate life, both online and offline. A significant proportion of the inhabitants of the 28 EU member states use such technologies on a regular basis, and their use continues to grow as such technologies become more integrated in daily life. One of the newest developments is the creation of 'wearable computing devices' such as the 'Google Glass' project (note the singular). This technology developed by the Google[X] lab, a facility which is shrouded in a cloud of secrecy, focuses on developing futuristic consumer products such as space elevators and driverless cars. Although some of these technologies are far from being launched the Google Glass glasses are expected to be commercially available before the end of 2014.<sup>271</sup>

Google Glass is essentially a computer built into the frame of a pair of glasses that integrate the main functions of a phone, laptop and tablet and places them into an individual's peripheral vision. The 1.3 cm display (half-inch) enables the user to take and share pictures and videos, video-chat, translate, surf the web and receive real-time information about their surroundings on the go through voice-commands. These type of glasses have long been around in the imagination of Hollywood, from 'Lieutenant Commander Geordi La Forge' in Star trek to 'Cyclops' in X-men, action heroes have been seen spotting wearable computers with a head-mounted display (HMD). According to Google the glasses provide a glimpse of the future: it aims to change the way people think about software and how it can be integrated in daily life, eventually aiming to function as an augmented brain.

The advantages of Google Glass seem obvious, overlaying data directly atop a user's field of vision makes navigating, taking pictures, replying to messages or translating easier. Its potential is even greater: imagine a situation in which a bystander to an accident can help a victim before professional help arrives through the glasses' display of first aid and a direct video-chat with emergency services. Yet, the project is controversial. Apart from the functions mentioned above that enable hands-free use of already commonly used technology, Google and other software developers are developing apps that allow the user to scan a crowd to find her friends, even if these friends have no intention of being found. Some people argue that this is nothing new in an era where almost everyone uses their phone or tablet to record and upload episodes of their lives. But there is a distinct difference between taking a picture with Google Glass and any other technical device: the glasses do not come with significant storage capacity. The default mode of the glasses is for data to be automatically uploaded to cloud servers, where it can be aggregated and analyzed by Google. In essence this means that the data gathered is not controlled or owned by the people wearing Google Glass. Google manages the data and could eventually use it to make personalized advertising displayed on the glasses screen based on what an individual sees in their real-life environment, as it is advertising that provides the main revenue for the company. Although surveillance of citizens by the state has become a normal part of modern life, discussions needs to be had about the desirability of surveillance by private companies.

---

<sup>270</sup> President's Review Group on Intelligence and Communications Technologies 'Liberty and Security in a Changing World, 2013, p53

<sup>271</sup> Sources:

<http://www.google.com/glass/start/> (google glass website)

<http://www.techradar.com/news/video/google-glass-what-you-need-to-know-1078114>

<http://www.bbc.co.uk/news/technology-22538854>

<http://www.guardian.co.uk/technology/us-news-blog/2013/may/17/congress-caucus-google-glass-privacy>

<http://www.guardian.co.uk/technology/2013/mar/06/google-glass-threat-to-our-privacy>

Especially, considering that Google Glass, when hacked, could give strangers access to your most personal information. Because what the wearer sees, the hacker sees.

Another issue revolves around consent. It can be argued that the people who use Google Glass have given their implicit consent to Google for using their data. They are willing to give up some aspects of their privacy for the advantages that this technology brings. But although the wearer of Google Glass consented to being permanently plugged-in to Google's digital world, people inadvertently captured 'on tape' have not. So, even if the Google Glass user has made a fully informed decision about the preservation and handling of their data, they cannot consent to the use of data concerning others they collected images of, unintentionally or on purpose. What this example serves to illustrate is that new technologies such as Google Glass can have far reaching consequences for personal privacy both of users and those surrounding them.

### 3.2.3. Public and private

The debate is not only about state and governments control and protection. Also huge commercial interests are at stake. Big data enables massive amounts of personal data to be processed and linked to other areas and analysed to produce new interferences and findings. The World Economic Forum referred to personal data as "the new oil". They were not the first group to make explicit the economic relevance of personal data and society's increased reliance on data as a tool for economic growth. There is a clear tension between on the one hand the economic opportunities provided by the increase of available data on potential consumers and on the other hand the need for protection of privacy. Service providers want to target their users with publicity and for that use the knowledge they gather through surveillance.

The traditional distinction between public and private surveillance is complicated as American Harvard Law professor Neill Richards pointed out: *"Government and non-government surveillance support each other in a complex manner that is often impossible to disentangle. At the outset, the technologies of surveillance – software, RFID chips, GPS trackers, cameras, and other cheap sensors – are being used almost interchangeably by government and non-government watchers. Private industry is also marketing new surveillance technologies to the state"*.<sup>272</sup>

Interestingly enough, commercial providers (Apple, Google, Microsoft) have recently written to the US authorities requesting a change in the access of government to their data.

---

<sup>272</sup> NM Richards, the dangers of surveillance - Information Society Project - <http://www.yaleisp.org/sites/default/files/Richards.pdf>



*“We understand that governments have a duty to protect their citizens. But this summer’s revelations highlighted the urgent need to reform government surveillance practices worldwide. The balance in many countries has tipped too far in favour of the state and away from the rights of the individual — rights that are enshrined in our Constitution. This undermines the freedoms we all cherish. It’s time for a change”*<sup>273</sup>

### 3.3. Ethical principles

The European Union is a community of values. These values are embedded in The *European Convention of Human Rights (ECHR)* that was the first legal, international treaty to protect human rights with enforceable mechanisms. Extending the ECHR, The *Charter of Fundamental Rights of the European Union*, which was adopted in 2000, and entered into force in 2009, is structured around the principles of dignity, freedom, equality, citizens’ rights and justice.

Underlying the Convention and the Charter is the principle of dignity. *Dignity* is at the heart of ethics and is also of crucial importance regarding the debate on security and surveillance. There is a close relation between the principle of dignity and the principles the Group brings forward in this chapter. The core ethical principles that underpin the EGE’s recommendations on security and surveillance are the following:

- Privacy and freedom
- Autonomy and responsibility
- Well-Being and/or human flourishing
- Justice

In addition to these basic principles, two procedural principles must be added in order to enable trust between individuals and companies and the state and/or states:

- Transparency
- Efficacy and proportionality

These principles should be seen as principles that both help to establish security and principles that lead to restraints regarding security and surveillance instruments. Based on these principles, the regulation and practice of human rights protection in the area of security are described and some remarks on responsibility are made.

---

<sup>273</sup> see: <https://www.reformgovernmentsurveillance.com> for information on the open letter to the US

## **Dignity, privacy, freedom and human flourishing**

### *Dignity*

Human dignity is a universal value. There are different philosophical interpretations of the concept of human dignity in the present pluralistic ethical debate, but it is universally recognised in the context of human rights framework, that human dignity expresses the intrinsic worth and fundamental equality of all human beings. This is reflected in Art. 1 of the Charter of Fundamental Rights of the European Union, which states “Human dignity is inviolable. It must be respected and protected”.

Dignity – applied to the context of security - requires the protection of and respect for physical and psychological integrity, the assurance of safety as the condition for being able to pursue one’s ends and psychological integrity to ensure the right to autonomy.

### *Privacy*

Privacy is a central notion in the ethical debate on surveillance and security and intricately connected to dignity. Human beings need their own space, both literally as well as figuratively speaking, in order to realise their capabilities and flourish as human beings. Dignity means to respect the need to have one’s own space, one’s secrets. Robbing a person of his or her privacy is robbing him or her of their dignity.

The right to Privacy is described in article 8 of the ECHR:

#### *“Article 8 – Right to respect for private and family life*

1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.*

*Privacy* etymologically derives from the Latin *privatus*, past participle of *privo*; “I deprive”, “I cut away”. Privacy thus refers to the state of being separated, secluded from others, in contrast to the state of being public or common”. A basic underlying idea is the right to be left

alone. This of course is an important notion but does not cover the present day complexities. Privacy has also been conceived as an “exclusion device – as a tool to fend off the unwanted gaze”.<sup>274</sup> According to the *Encyclopaedia of Privacy*, it describes and demands “limits on the appropriation of others’ peaceful seclusion, personal information, intimate choice, and identities”. Although the term “privacy” cannot be found in all languages, the experience of privacy is a “cultural universal”, “an essential part of human flourishing and well-being”.<sup>275</sup>

Privacy means the right to protect actions and thoughts that persons want to keep to themselves and is closely related to intimacy. Observing persons in situations considered as intimate and personal such as cameras recording one’s sexual activities, or other intimate behaviours, can be humiliating and degrading. There is an extensive philosophical debate on different forms of privacy and definitions of privacy. Scholars distinguish between physical (related to physical protection), psychological (related to personal autonomy), economic (related to property), informational (related to personal information), and decisional (related to decisional power) privacy<sup>276</sup>.

In the context of this opinion all these areas are relevant, e.g. CCTV cameras interfere with physical privacy, data mining has to do with informational privacy, border control technologies may impact on physical and psychological privacy, and telephone and email recording touch upon psychological and informational privacy.

Privacy has changed over time by giving shape to a right that is increasingly geared towards enabling the free construction of one’s personality – the autonomous building of one’s identity, and the projection of fundamental democratic principles into the private sphere.

### *Privacy in modern society*

There is no agreement on the role and meaning of privacy in modern society. Some hold the extreme “Privacy is dead, accept it” view. They bring forward the argument that privacy is a means of controlling information that should commonly be shared since in the web e-privacy cannot properly be defended. This view, called the “post-privacy-movement” also advocates that actively giving up privacy would determine the flourishing of a personal and social virtue

---

<sup>274</sup> Mireille Hildebrandt, Antoinette Rouvroy (2011) “Law, Human Agency and Autonomic Computing: The Philosophy of Law Meets the Philosophy of Technology” Routledge, 26 Aug 2011, p187.

<sup>275</sup> Adam D Moore (1965) “Privacy Rights: Moral and Legal Foundations” Pennsylvania State University Press, ISBN 978-0- 271-03685-4, Pg 56

<sup>276</sup> Report on challenges for the EU

based on people's freedom to introduce and share whatever data on their own lives they desire. Also according to this view, such an approach should encourage people to cultivate more tolerance between attitudes and the behaviour of others.<sup>277</sup>

The opposite view states that the assumption that in the present era it is difficult to guarantee privacy is not a convincing reason to abandon the necessary protection of individuals' privacy. It emphasizes that a private sphere is a source where one is not required to immediately meet public expectations and conventional lifestyles.<sup>278</sup>

The overarching tendency seems to be that privacy seems to be very much alive. There may be shifts, however, into what one wants to keep private. "Most people are used to giving out personal data to shop online or use social networking sites. But they're equally worried about how this data will be used, and don't always feel in control."<sup>279</sup>

### *Nothing to hide?*

An argument often brought forward in the debate about surveillance and privacy is that those who have nothing to hide have nothing to worry about. Either their privacy will not be intruded, or they need not see measures as intrusions of privacy in the first place; only the ones having something to hide are at risk of invasions of their privacy. Though quite popular this is not a convincing argument. Everyone has something to hide, in the sense that certain thoughts, images and acts are intimate and private. If one has nothing to hide in the sense that one is not doing or planning something bad or criminal, one still may cherish one's secrets and one still may experience certain technologies and the ensuing exposure as embarrassing or humiliating, e.g. because it implies being touched, or because one feels one is treated as a criminal. Certain thoughts and acts are nobody's business. The idea that they have 'nothing to hide' may lead to a certain naiveté in the way people themselves handle their own data. Some people may be willing to share data, not realising that what they think is innocuous information, contributes to a system that is not innocuous anymore.

### *Consent*

---

<sup>277</sup> see, for example, [http://events.ccc.de/congress/2008/Fahrplan/attachments/1222\\_postprivacy.pdf](http://events.ccc.de/congress/2008/Fahrplan/attachments/1222_postprivacy.pdf) entitled "Embracing Post-Privacy: Optimism for a future where there is nothing to hide"

<sup>278</sup> see for example, Special Eurobarometer 359: [http://ec.europa.eu/public\\_opinion/archives/ebs/ebs\\_359\\_en.pdf](http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf) and [http://europa.eu/rapid/press-release\\_IP-11-742\\_en.htm?locale=en](http://europa.eu/rapid/press-release_IP-11-742_en.htm?locale=en)

<sup>279</sup> Commissioner Reding quoted in [http://europa.eu/rapid/press-release\\_IP-11-742\\_en.htm?locale=en](http://europa.eu/rapid/press-release_IP-11-742_en.htm?locale=en)

Is it, however, not possible to relinquish one's right to privacy by consenting to being surveyed, filmed, e.g. in television programmes? Does consent provide a justification for limiting privacy? There is no simple answer to this question. Sometimes agreement means that there is indeed no invasion of privacy, e.g. if one allows a person to read one's emails. Sometimes, however, such consent may be very fragile as people agree in a superficial or naïve way. One's ticking a box in order to get access to a website or a service provides illustrative examples of this.

Sometimes the circumstances are such that one does not really have a choice but to 'consent' as otherwise one is deprived of the means to participate in modern life.<sup>280</sup>

Vis-à-vis the mega data, mega surveillance, global tracking, CCTV, and other controls, individuals may feel insignificant and powerless. They may therefore accept all kinds of measures and comply, not because they actually agree and therefore consent, but because they were led to believe that it is for the best, or have no idea of the ramifications or because they cannot change them anyway. One may feel that as an individual citizen one has little or nothing to say in the matter of surveillance. It is one of the many decisions by governments and commercial actors that individuals can but accept and abide by. If one wants to travel by air, one must pass the security. You want to shop: you are being filmed and recorded on CCTV. You want to profit from your customer card: the supermarket will know about your dietary habits. You have a mobile phone: you can be tracked. You surf on the internet: the places you go to will be known to the provider.

The debate following the Prism revelations has been a strong wake-up call that may have changed the complacency of many as well as their views on privacy.

---

<sup>280</sup> "In modern society, individuals, for practical reasons, have to use credit cards, e-mail, telephones, the Internet, medical services, and the like. Their decision to reveal otherwise private information to such third parties does not reflect a lack of concern for the privacy of the information, but a necessary accommodation to the realities of modern life. What they want — and reasonably expect — is both the ability to use such services and the right to maintain their privacy when they do so. As a matter of sound public policy in a free society, there is no reason why that should not be possible"

The President's Review Group on Intelligence and Communication Technologies (2013) The NSA Report: Liberty and Security in a Changing World . Princeton University Press ISBN 978-0- 691-16320-8 and [http://www.whitehouse.gov/sites/default/files/docs/2013-12-12\\_rg\\_final\\_report.pdf](http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf)

## Autonomy, intellectual privacy and individual responsibilities

Central ethical principles in the debate surrounding security and surveillance are autonomy and freedom. These are again closely connected to privacy in the sense that a lack of privacy curtails one's freedom and that the freedom not to be the subject of surveillance is part of the privacy notion. The important idea is that individuals ought to be free to think what they want, to express their views, to travel and to interact with whom they want to interact.

The aforementioned legal scholar Neill Richards stresses the notion of intellectual privacy. If people are being continuously surveyed and monitored they will behave differently, they will adapt to what they think is expected of them and they may fear to use their capacity to think of new ideas given the fact that behaving differently may have serious and negative consequences (from being an outcast to ending up in jail or being silenced). Surveillance can be harmful because *"it can chill the exercise of civil liberties, and because it gives the watcher power over the watched.... Such intellectual surveillance is especially dangerous because it can cause people not to experiment with new, controversial or deviant ideas. To protect our intellectual freedom to think without state oversight or interference, we need ... "intellectual privacy."* A similar argument is brought forward by J. Cohen, professor at the Georgetown Law Centre, *"Environments that disfavour critical independence of mind, and that discourage the kinds of tinkering and behavioural variation out of which innovation emerges will, over time, predictably and systematically disfavour innovation, and environments designed to promote consumptive and profit-maximizing choices will systematically disfavour innovations to promote other values. The modulated society is dedicated to prediction but not necessarily to understanding or to advancing human material, intellectual and political wellbeing."*<sup>281</sup> Autonomy and freedom are of the highest importance in this debate as surveillance technologies may threaten these principles.

Autonomy implies responsibility on the part of the individual as well. Citizens have a responsibility to be aware, alert, critical and informed, e.g. when they sign privacy waivers. They need to be aware of the consequences of sharing data (their own or those of others), they need to reflect on what they consider to be private and an area not to be intruded by government or commercial players, to be kept secure and confidential, and what they are willing to divulge. In order to make informed decisions citizens need information, and a choice, a real choice and therefore of course need to be informed, by governments, by

---

<sup>281</sup> J.E.Cohen "What Privacy is For" Harvard Law Review , Vol. 126, No. 7 see:  
<http://www.slaw.ca/2013/01/31/thursday-thinkpiece-cohen-on-privacy/>

providers of services. Education concerning these issues, both in terms of knowledge as well as reflection, on the practical and moral dimension is of the highest importance and needs to be part of every curriculum in the EU.

It is also important that citizens take part in the societal debate on the limits of security and surveillance. What price do they consider to be reasonable when it comes to security, where and when should freedom and privacy prevail, even at some risk for security. These are fundamental political issues that need the public's participation. The President's Review Group on Intelligence and Communications Technologies expresses its worries as follows:

*"One ... concern is that law-abiding citizens who come to believe that their behavior is watched too closely by government agencies ... may be unduly inhibited from participating in the democratic process, may be inhibited from contributing fully to the social and cultural life of their communities, and may even alter their purely private and perfectly legal behavior for fear that discovery of intimate details of their lives will be revealed and used against them in some manner."*<sup>282</sup>

### **Justice, non- discrimination and the usual suspects**

The principle of justice is interpreted in many different ways in different contexts. In the context of this opinion the focus lies on non-discrimination. Surveillance technologies and the analysis of the data are based on distinguishing certain characteristics or behaviours as different, 'suspicious' or 'wrong'. Using certain words in an email or telephone conversation, wearing a hooded sweater, and having a beard is stigmatised in certain times and places. That, and there is ample evidence, leads to what is called social sorting: some people are 'sorted' out, others are not. The 'usual suspects' are distinguished from the 'innocent' rest of the world. This gives rise to serious problems of justice as individuals or groups may be stigmatized, based on simple prejudice or (too) general or even faulty statistical methods. Innocent people will find themselves, probably over and over again, in a position of being a suspect as such a stigma is almost impossible to 'shake off'. There is serious misery and wrong in being a 'false-positive'. Such stigmatisation has very serious social consequences in terms of travelling, employment, the way people are treated in daily life. It may seriously threaten diversity. People might conform to certain habits or codes, not because they want to or truly embrace them, but because they don't want to be targeted as suspects. It also has

---

<sup>282</sup> US president's Review Group on Intelligence and Communications Technologies, 2013, 112

dire consequences for social cohesion and the very notion of citizenship. David Lyon in his dialogue with Zygmunt Bauman warns *“And while the loss of privacy might be the first thing that springs to many minds when surveillance is in question, arguably privacy is not the most significant casualty. The issues of anonymity, confidentiality and privacy should not be ignored, but they are also bound up with those of fairness and justice, civil liberties and human rights. This is because, as we shall see, social sorting is primarily what today’s surveillance achieves, for better or for worse. (...) the logic of statistics and software that drives today’s surveillance produces outcomes that are uncannily consistent. Not merely – and egregiously – do ‘Arabs’ and ‘Muslims’ find that they are subject to far more ‘random’ scrutiny than others at airports, but also, as Oscar Gandy demonstrated, the social sorting achieved by contemporary consumer surveillance constructs a world of cumulative disadvantage”*.<sup>283</sup> Extreme care and high demands regarding the criteria and the statistics on the basis of which selections are made are necessary.

## **Transparency**

The need for and the ethical importance of transparency have been stressed in the past decennia, also by the EGE. It is a crucial principle that emphasizes the importance of openness on policy making and implementation. What is done, how are the decisions to do what is done made, who does what? Transparency allows for democratic control.

Of course, when it comes to surveillance measures the translation of the principle of transparency into policy may be complicated. There is a difference between openness about the way in which decisions are reached (e.g. the procedure to have specific persons suspected of criminal activities surveyed) and the principles underlying such decisions, and openness about concrete measures, such as the actual surveillance of actual persons, that only will ‘work’ if a certain secrecy is being maintained, given that being transparent would defy the objective. Of course the ‘need for secrecy’ -argument can and has been misused in order not to divulge measures or actions. Transparency is not, as it sometimes seems to have become, an easy panacea for everything that is politically complicated or sensitive.

The EGE stresses the need and importance of transparency but also expresses two caveats. Being transparent about something does not itself justify that decision or act. It is a necessary condition to enable the debate on the justification, not a sufficient condition for the justification. Transparency may sometimes lead governments or providers of services to hold that citizens have actually agreed to measure x, whereas citizens feel that they have no

---

<sup>283</sup> Zygmunt Bauman and David Lyon, *Liquid Surveillance*, Polity press 2013, 13-14 ISBN 9780745662824 and as



choice but to undergo the consequences of measure x. E.g. if there is an obligation to announce that CCTV is being used, that is transparent, but does not answer the questions: is the use of CCTV in this context justified, and do those who are filmed feel that they have any significant choice in the matter? The EGE is of the opinion that both procedural as well as material conditions are needed.

### **Efficacy and proportionality and balancing**

The EGE stresses that in order to develop or justify policy one needs to know to what extent the measures designed to provide security in fact accomplish that goal. Surveillance measures have been taken based on the hope that they would increase security, or to give the public the feeling that they were safe, or to show that ‘measures are being taken’ whereas there was no evidence that they actually increased security, or that it was clear whose security was at stake. In certain scenarios, the introduction of security technologies and surveillance systems takes on a path-dependent character, with little public debate over the value and necessity of proposed measures. Justification of policies and measures presupposes that it is clear how effectiveness of surveillance is defined, and how effectiveness is measured.

In addition, any reduction in privacy to increase security may create new forms of insecurity. The creation of centralised data banks that facilitate law enforcement can also expose personal data to new risks related to misuse and theft. Technological body searches (e.g. metal detectors, advanced “body scanners”) that in theory should prevent terrorist attacks may in practice aggravate worry on the part of search subjects and create a false sense of security that leads to a relaxation of other security procedures

If measures are shown to be effective, then the balancing question must be addressed: how to balance security with privacy, autonomy and justice. No simple arithmetic formula is available for such balancing. The US President’s Review Group on Intelligence and Communications Technologies comment that there should be no balancing for certain principles:

*“In a free society, public officials should never engage in surveillance in order to punish their political enemies; to restrict freedom of speech or religion; to suppress legitimate criticism and dissent; to help their preferred companies or industries; to*

*provide domestic companies with an unfair competitive advantage; or to benefit or burden members of groups defined in terms of religion, ethnicity, race, and gender.”<sup>284</sup>*

---

<sup>284</sup> US president’s Review Group on Intelligence and Communications Technologies, 2013,

## Chapter 4      On the Notion of Trade-Off

In our inquiry into the ethics of security and surveillance technologies, we were confronted with recurrent and prevalent ways to approach, conceptualize and discuss this issue area. Yet the way the ethical questions are framed matters tremendously, because it will orient not only the approaches taken but also the answers that are possible within the chosen framework, while these might differ considerably in another framework.

As we will see below, the most pervasive framing of security and surveillance is the notion of *trade-off* and in particular the trade-off between two goals, security and freedom (with freedom expressed, for example, in the right to privacy). In one version of this narrative, security and surveillance are considered as requirements of the state to protect the lives and basic freedoms of all citizens, and this, it is argued, requires some trade-off between the right to be protected and the rights to move and/or act freely in a given society. In another narrative, new technologies are connected to competitiveness, jobs and economic growth, which require to ‘trade’ away freedom rights – both at the level of the polity in order to remove hindrances to the success of particular companies (premised on certain uses of big data) and at the individual level in order to utilize the opportunities provided by such companies, especially online services.

These framings guide, structure and constrain the reasoning—and policy responses to security and surveillance technologies, corralling them towards limited options and avenues, which profoundly impact our societies.

It is thus an important part of our task, in this Opinion, to scrutinize and shed light on the ‘way we think now’, on the framings of the options we have, unpack them, and thus open up new possibilities for thought and public policy as well as individual and collective actions. Our aim is to take a step back and reflect upon what these framings make visible and what they leave out or obfuscate.

## 4.1. Balancing rights

Before venturing further into the unpacking of the trade-off narratives, there is a key misunderstanding to defuse and avoid here: Human dignity is the core principle of the European moral framework, and as such it cannot be 'traded off'. Although there are many different meanings associated with the concept of human dignity, none of which captures every dimension of it, dignity is intimately associated with freedom and responsibility. For what is at stake in the contractual interactions, for example, between an individual and companies, and in the relationship between the state and the citizen, is exactly the equilibrium between freedom and responsibility.

The rights we are discussing in the context of security and surveillance technologies, such as the right to privacy and the right to data protection, or the right to information and transparency, are not absolute rights; they must be balanced against other rights and balanced against the rights of other persons or groups. In modern political theories, the latter 'balancing' is left to the authority of the state, who regulates the different freedoms in view of the justice for all. Hence, in this balancing, the interrelation of ethical and juridical reasoning go hand in hand, and (political) theories of justice have addressed this broadly over the last decades. Without turning to one particular theory of justice, as a starting point in our reflection we can say that an agent necessarily prioritizes his or her values because of the internal hierarchy they have for a person. In the tradition of human rights, one may now argue that certain values are expressed in the form of rights, and these come with the claim that an agent cannot do without them in order to maintain the conditions of his or her agency, or his or her well-being.<sup>285</sup> Theories of justice demand, furthermore, that an equilibrium be found in and for inter-personal affairs. Individual rights are therefore necessarily entangled with the question of justice, if we understand justice as the theory that deals with the interpersonal reconciliation between different rights claims of persons. Given that justice requires at the same time a political theory, i.e. a theory of the state, this means that a state will ask: whose rights are to be addressed, and which rights are to take priority, both in

---

<sup>285</sup> Cf. for example: Alan Gewirth: *Reason and Morality*, Chicago 1978 who argued that the transition from values to rights is necessary from the point of view of the agent, and is the presupposition for the agent's 'willingness' to grant others exactly the same conditions for their agency. Gewirth coined them as rights to freedom and well-being, and provided a (formal) hierarchy of basic rights, non-subtractive rights, and additional rights. While there is considerable debate on the relationship between dignity and rights, and 'basic' or 'natural' human rights and other kinds of rights, such as political (freedom) rights, or legal rights, this can be

general and in particular contexts or under specific circumstances?<sup>286</sup> Some kind of balancing, weighing, or choice between priorities, it seems, is always necessary.

In this regard, taking the important example of the fundamental right to the protection of personal data under Article 8 of the Charter of Fundamental Rights of the European Union, it “is not, however, an absolute right, but must be considered in relation to its function in society”.<sup>287</sup> Article 52 (1) of the Charter thus accepts that limitations may be imposed on the exercise of rights such as those set out in Articles 7 and 8 of the Charter. But it is crucial to look at the constraints to these limitations, set up as specific criteria: limitations must be provided for by *law*, *respect* the essence of those rights and freedoms and, subject to the principle of *proportionality*, are necessary and genuinely meet *objectives of general interest* recognised by the European Union or the *need to protect the rights and freedoms of others*.<sup>288</sup> A similar situation prevails in the European Convention on Human Rights system.<sup>289</sup> In effect both the European Court on Human Rights and the Court of Justice of the European Union (ECJ/CJEU) have repeatedly stated that a balancing exercise with other rights is required when applying and interpreting Article 8 of the Convention and Article 8 of the Charter. Key rights that can come into conflict with the fundamental right to the protection of personal data are, notably, the rights to freedom of expression and information, the rights of access to documents, the freedom of the arts and sciences (Article 13 of the Charter), and the protection of property (Article 17 of the Charter). These examples demonstrate that we have a rich jurisprudence and a long history of scholarship both in ethical and in legal philosophy concerning the balancing and prioritizing of rights.

So, why then are the trade-off narratives that confront us when entering into the area of security and surveillance technologies of a different nature?

---

left to philosophical debate; for our purpose here, it suffices to acknowledge that any theory of rights requires to argue for the prioritization between the *kinds* of rights, and the *equal* application of rights to all individuals.

<sup>286</sup> Waldron argues that the law and dignity are so tightly inter-related exactly because a person who is capable of reasoning must, at least in principle, be in a position to comprehend the laws. Law-givers must respect this capability to ask for reasons, and they respect the dignity of the citizens in doing so. Denying citizens the transparency or the reasons why they should apply certain laws therefore lacks this respect – and can only be justified if ‘secrecy’ is itself required to apply a given law. This is the case for certain activities of ‘secret services’ in the name of security or other superior interests of the state.

<sup>287</sup> See, for example, CJEU, Joined cases C-92/09 and C-93/09, *Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, 9 November 2010, para. 48.

<sup>288</sup> *Ibid.*, para. 50.

<sup>289</sup> For this discussion cf. Handbook on European data protection law, FRA, 2014.

## 4.2. The trade-off between security and freedom

*«You cannot have 100 percent security and also then have 100 percent privacy ... We are going to have to make some choices as a society. ... There are trade-offs involved.»*

(US President Barack Obama, San Jose, California, 7 June 2013).

A classic, dominant 'trade-off' narrative stems from the genuine task of the state to secure the life and human rights of citizens. Part of the reason why state sovereignty is (still) valued so highly concerns exactly this task. So, do we have to trade-off privacy against our basic right to security, or, put more generally, do we have to give up our freedom rights in order to maintain the basic protection of our lives?

The difference between this trade-off scenario and the one explored in the following section below, is that in the case of security we do not choose whether we want to participate or not. Security is a matter of state institutions finding an equilibrium between rights *of* persons, on the one hand, and rights *among* persons, on the other hand. For often, security means that the limitation of the freedom of one person (or group) secures the freedom of another, or vice versa: because someone is profiled either 'positively' (European citizens's passport are checked faster than global citizens at the EU border control, for example), or 'negatively' (in many cases, belonging to a particular group, nationality, ethnicity, or religion triggers the scrutiny of examination), others either benefit or bear the burdens of the established measures. In the case of positive profiling, the line between reasonable preference and undue privilege is hard to draw, as in the case of negative profiling it is hard to draw the line between reasonable special treatment and undue discrimination. Unless the law-giver (the state) is able to articulate the reasons – and criteria – to its citizens why specific choices are made, it does not respect its own relationship with the citizens. This state-citizen relationship, as we said, is based (and must be based) upon the respect for their dignity, i.e. their capability to comprehend and comply with the laws that are set up to serve all of them. Sometimes, this respect is expressed in the terminology of trust; this is certainly correct but what is at stake goes much deeper than this terminology might suggest. Respect for the comprehensibility of any state measures becomes easily sensitive in the area of security and surveillance. As Waldron aptly shows, the stakes are particularly high in the trade-off between liberty and security:

For what is traded off in that case is not just economic interests or mundane freedoms, like the freedom to drive without a seatbelt. Often what

is traded off is something that was previously regarded as a right, and the loss of that right may simply be imposed on the people affected. Members of a minority are detained without trial, or spied upon, or beaten or humiliated during an interrogation, and all to make the rest of us more secure. This is troubling because rights are supposed to be guarantees given to individuals and minorities about the outer limits of the sacrifices that might reasonably be required of them. Rights are supposed to restrict trade-offs, not be traded off themselves.<sup>290</sup>

We need to ask, then, what exactly is the function of human rights in the act of balancing? Whose rights are being traded? And which rights? And: do human rights not function as restrictive 'sign posts', indicating exactly how far the state can go without having the permission of the very individuals whose rights are 'sacrificed' for the good of the others? May one person's life, safety, security, and freedom be traded for the security of the other? Or is it possible to maintain that both security and freedom can be maintained in the 'age' of new security and surveillance technologies, if states are willing to re-examine their policies, set up at the beginning of the 21<sup>st</sup> century without embracing all ethical problems sufficiently? These are difficult questions, and there will not be easy answers. But this is what the trade-off narrative does rhetorically: it underestimates the difficulty associated with the sensitive equilibrium between freedom and security.

#### **4.3. The trade-off between "jobs and growth" and "privacy and freedom"**

A second prevalent 'trade-off' narrative takes the form of an economic framing where jobs and economic growth are opposed to freedoms and notably to the right to privacy. What is more important? Competitiveness, growth and jobs, or considerations regarding privacy, data protection, informational self-determination, and individual freedoms?

For example, avenues opened by new information and communication technologies in general, and the set of approaches comprised under the heading of 'Big Data' in particular, hold tremendous promise in terms of competitiveness, jobs and growth. The mantra of this school of thought is along those lines: *Big Data is Big Business. It is vital to our prosperity, to our competitiveness, growth and jobs. We should choose between holding on to outdated notions of privacy and making way for -and indeed sharing in- this new economic boon.*

---

<sup>290</sup> J. Waldron: Is this torture necessary? New York Review of Books, 2007, Vol. 54/16, 40.

With respect to the technologies indicated in Chapter 1, such as technologies of traceability and control, on-line and mobile applications, machine to machine communication, Internet of Things, as well as cross-correlation data analytics, this narrative touches not only on new ways to produce growth but also on new ways to produce knowledge, i.e. 'intelligence' (in the service of security) as well as scientific knowledge. This involves both private companies, in potentially oligopolistic situations, and public authorities, and it is not limited to cross-correlation data analytics but extends to predictive analytics and algorithms.

References are made in this regard to the NSA PRISM programme, to tensions pervading the activities of Google and Facebook among others, but also to the early and foretelling statement in 1999 by Scott McNealy, then CEO of Sun Microsystems, that "you have zero privacy anyway. Get over it."

The advocates of this perspective are thus eager to push back the hindrances to growth and innovation that they, at least in part, relate to the rights to privacy, data protection, and informational self-determination.

It should be noted that this 'trade-off' framing operates at two levels: at the level of the polity, with regard to removing hindrances to the success of particular businesses, and at the individual level, in order to utilize the opportunities offered by such companies.

In the above scenario, the choice concerns one's action in relation to companies. We still may opt to refrain from certain services in order to maintain the privacy rights we value more than the freedoms we gain from using the internet, communicating via social media, and so on. However, the more prevalent these services get, the fewer alternatives individuals have *not* to participate in the social practices, and the more difficult it will become to choose freely what services one wishes to use. At a certain point, the desire (or need) to participate socially and/or economically will surpass the desire for privacy – and for the state or law-giver to turn a blind eye to *this* conflict undermines the individuals' right to opt for life-styles they may otherwise have every reason to choose. The framing of the trade-off disguises, then, that the loss of privacy that we all experience when we participate in the new economy and in the new means of communications is not necessary; it only reflects the reluctance to set up regulations that would balance individual rights over the gains of companies, on the basis of transparent and comprehensible criteria. The effort that has been shown in the area of data protection is a good example of how to set up such criteria, and this effort –while still incomplete– is certainly welcome.



In the discourses on security and surveillance technologies, one can find alternatives to the trade-off narrative. In the following, we will address first the 'positive-sum' and 'win-win' paradigms; and second the evolving approach premised on notice and on choice (consent) at the time of data collection (which addresses issues raised by security and surveillance in market-relations, if not with regard to state security).

#### **4.4. Alternative to the trade-offs? 'Positive-sum' or 'win-win' paradigms**

The above developments indicate the difficulty and complexity of those tangled stakes and priorities.

But what if we did not have to confront those tough choices? What if we could have it both ways?

Such is precisely the appealing narrative of the advocates of the 'positive-sum' or 'win-win' paradigms.<sup>291</sup> Indeed their claim is that by resorting to relevant technologies (privacy enhancing technologies, technologies implementing privacy by design), there is no need to make those tough choices anymore.

Those approaches hold tremendous promise. Yet this leads to a series of questions, pointing to the shortcomings of this postulation.

First of all, can one really –as is advocated by the champions of these paradigms– do away with the (ethical/political/etc.) "balancing"? To put it another way, can the advocated 'positive-sum' or 'win-win' paradigm shift obviate the need to consider the weight of what is (at risk of) being lost or subtracted – as well as the weight of what is to be gained?

At this stage a second matter arises: if an approach and discourse were to deny the need for that balancing, while balancing were in fact needed, would it not be the case that this approach is obfuscating the balancing? In those circumstances it would indeed be obfuscating the balancing. This leads to ask, on the one hand, whether it is desirable that the balancing be denied and, on the other hand, whether it is desirable that the balancing be obfuscated. This also leads to a more practical question: would it be desirable that the balancing be entrusted to and carried out by one exclusive body?

---

<sup>291</sup> A very interesting, thorough and well done exposition is offered in Ann Cavoukian, *Privacy by Design*, Office of the Information & Privacy Commissioner of Ontario, Canada, 2013.

Hence a third front of reflection for action: is it not more desirable that the gains and losses and risks be recognized, as well as the distribution thereof? Is it not more desirable that the balancing be acknowledged and that it be carried out in plain sight, with involvement of the parties concerned and/or explicit justification of the choices being made?

Otherwise, the fact is that there is a risk of depriving the rest of society and individual citizens of their ethical reflectivity as regards issues to do with security, privacy, what matters to them and the common good (i.e. there is a risk to generate effects of disempowerment). Furthermore there may be such a risk too in the very notion –and practices– of 'privacy by design', embedding the ethical reflectivity, the perplexity, the pause for thought, the evaluative critical gesture, the valuation and the choosing, inside a technology, algorithm or device. That is, a risk of confiscation and neutralization of all individuals' ethical potency.

Otherwise, the fact is that there is also a risk of instilling a false sense of security – although it could be that this sense of security is precisely what is sought in the first place.

#### **4.5. Alternative to the trade-offs? Lessons from privacy based upon notice and consent**

There are yet other alternatives with regard to the institutionalization of the rights concerned, and indeed they were established long before the advent of the latest technologies discussed in Chapter 1. It is important to revisit these options in order to assess how they could be further developed in and for the present context.

This section considers the predicament of data protection and privacy, indeed the predicament of informational self-determination, so as to draw out key insights, and to develop further the principles and criteria required for today's and tomorrow's technologies.

The *Guidelines on the protection of privacy and transborder flows of personal data* adopted by the Council of Ministers of the Organisation for Economic Co-operation and Development on 23 September 1980<sup>292</sup> mark an important milestone in the early identification of – and reaction to – privacy and security concerns, and the threats and transformations foreseeable at the time. While they were particularly judicious and timely –or indeed ahead of their time– in their own right, the 1980 Guidelines provide a framework how to reflect upon data

---

<sup>292</sup> For the complete text of the 1980 OECD Guidelines and accompanying explanatory comments, see: [www.oecd.org/internet/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm](http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm)

For the revised Guidelines of 2013, see: <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>

protection and privacy to date and beyond.<sup>293</sup> The OECD guidelines identified eight key principles:

1. *Collection Limitation Principle* — There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. *Data Quality Principle* — Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. *Purpose Specification Principle* — The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. *Use Limitation Principle* — Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 [3] except:
  - a) with the consent of the data subject; or
  - b) by the authority of law.
5. *Security Safeguards Principle* — Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
6. *Openness Principle* — There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. *Individual Participation Principle* — An individual should have the right:
  - a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
  - b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
  - c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
  - d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
8. *Accountability Principle* — A data controller should be accountable for complying with measures which give effect to the principles stated above.

The Guidelines are a testament to the increasing and well-entrenched focus, from the 1970s to the beginning of the 21<sup>st</sup> century, on an individual's authority over his or her data, based upon the principle of freedom and self-determination. It translates into the emphasis *on notice and on choice (consent) at the time of data collection*, while demanding of those who retrieve data to meet several standards aimed at protecting the freedom rights of the users. Frameworks for data protection and privacy were built on this cornerstone in many regions of the world (including the EU and the US), predicated on the notion of a transaction in which an entity provides notice to an individual about an intended data collection, that individual

---

<sup>293</sup> In 2013 these guidelines were revised without any paradigm shift.

exerts their right to an informed choice as to whether to allow that collection, following which the subsequent use of the data is limited by the terms of that notice (with the important role, in that regard and in the context of the principles indicated above, of the principle of purpose limitation).

One result of this framework was, practically speaking, the lengthy notices to scroll through without a second thought in order to give one's consent, i.e. in order to reach the "I agree" button at the bottom of the screen and click on it.

The limitations of this model will be familiar to most readers, albeit at an intuitive level.<sup>294</sup>

Other shortcomings regard the *exercising* of this right.

On the one hand, this touches on the notion of 'choice' which, as discussed above must rest on meaningful alternatives.

On the other hand, it is a remarkable fact that –notably with regard to redress– the right is in fact not exercised (even though there has been a shift in the burden of proof, in the EU notably, so that in the transaction indicated above it is not upon individuals to prove a breach). Privacy Commissioners receive next to no complaints. The majority of privacy breaches remain unknown, unregulated, unchallenged. At any rate, a focus on notice and consent at time of collection –or indeed more broadly regulatory compliance alone– is unsustainable as the exclusive model for ensuring the future of privacy.

What are the alternatives then?

One avenue pursued pertains to technological fixes, embedding privacy in the design of products and services, e.g. through deidentification/anonymization/pseudonymization of personal data.

Another avenue consists in shifting the focus from data 'collection' to 'use', i.e. from notice and consent at time of collection towards data uses. It should be noted that a crucial stake in this context is the effects this could have on the principles and practices of *purpose specification and limitation*.

A first related but distinct aspect –with regard to a move from collection to uses– consists in shifting the balance of responsibilities, currently weighing heavily on data subjects, towards

---

<sup>294</sup> In addition to which, very concretely, reading is often deliberately made difficult by using capital letters only. This discourages consumers in addition to the often idiosyncratic legal terminology.

greater responsibility for data users – including a focus on institutional responsibility for "data stewardship" rather than mere regulatory compliance.

A second related but distinct aspect consists in moves towards a risk analysis scheme. This can be seen as a proposed improvement or as a way to sweeten the bitter pill of abandoning purpose specification and limitation.<sup>295</sup> One element in this regard is the possible development of a process of risk assessment to evaluate the different proposed uses, as well as of sets of measures to minimize the risks.

Here the learning pertaining to risk analysis, together with that pertaining to impact assessment (in relation to privacy impact assessment), are again important to bear in mind, as discussed in the following section.

#### **4.6. Going beyond the trade-off:**

*Any person – and any society – that would sacrifice freedom for security deserves neither*

(Benjamin Franklin)

##### *Understanding the terms of the trade*

In scrutinizing the trade-off as a frame, as a narrative or metaphor or as a worldview guiding policy choices and institutional developments, it is important to take it seriously in order to delineate –and ultimately move beyond– its limits.

So what does a "trade-off" mean, what does it imply? At the core, it indicates that something will be given up and that something will be gained. Indeed it indicates that something is given up in order that something else is gained. It is a trading off.

*"If we want a greater measure of security, then we need to give up some of our privacy and other freedoms." "In exchange for more jobs and growth, we have to give up on some of our human rights."*

But what is gained and what is lost? Very specifically, with regard to choices as to the taking up and deployment of new security and surveillance technologies, what exactly is the "greater measure of security" that is gained?

---

<sup>295</sup> Notably in the work supported by Microsoft Corporation, see Fred H. Cate and Viktor Mayer-Schönberger, Notice and Consent in a World of Big Data: Microsoft Global Privacy Summit Summary Report and Outcomes, November 2012.

It is incumbent upon us to ask whether in fact the very notion of gain should not be seen as problematic in the absence of a robust form of assessment, of valuation or evaluation. Hence a need to question at the very least the cost and the effectiveness of such endeavours, and ultimately the framing of these endeavours where *choice* or *alternatives* as such may seem cast out.

Another key dimension to pay attention to is the "we" in the italicized propositions above. Who is the "we"? That is to say, how are those decisions (with regard to the taking up and deployment of new security and surveillance technologies) arrived at, or to put it in simpler terms, by who are those decisions made. This needs to be pushed further: in the terms of the trade, is the "we" that gives away the same "we" that cashes in in return? In the crispest form: who gains, who loses, who decides, who *knows*?

### *Simplicity and risks*

As a case in point it is interesting at this stage to refer to this example given by Bruce Schneider:<sup>296</sup>

<< You can have as much security as you want, as long as you're willing to accept the trade-offs. Shortly after 9/11, a reporter asked me: "How can we prevent this from happening ever again?" "Easy," I replied. "Simply ground all the aircraft." It's a ridiculous notion, but we could ensure that the attack could never be repeated if we're willing to accept the trade-off. >>

This indicates, no matter how inadvertently, the dire limitations of the trade-off worldview. For alongside the ridiculousness explicitly drawn attention to there, the idea that this extreme measure ("ground all the aircraft") would in fact "ensure that the attack could never be repeated" is itself particularly incongruous or lacking breadth of view. If aircrafts were to be grounded, attacks could still be conducted through other means unfortunately.

"Easy. Simply violate everyone's privacy and individual freedoms." No one is quoted as offering this solution. Rather, this sombre perspective underscores the simplicity of certain discourses, together with the tenuous border between the possible and the actual, as well as the contrast between such simplicity and the difficulty of effectively addressing the security needs.

---

<sup>296</sup> Bruce Schneider, the renowned cryptographer and CTO of Counterpane Internet Security, author of *Applied Cryptography* and of the best-selling primer on infosecurity, *Secrets & Lies*, was interviewed –following the release of *Beyond Fear*– by Lawrence M. Walsh, the managing editor of *Information Security*. Article dated November 2013, retrieved on 16 December 2013 at: <http://searchsecurity.techtarget.com/feature/Bruce-Schneider-Beyond-Fear-Searching-for-rational-security>.

It is also interesting to note, in passing, that Bruce Schneider's experience and expertise have eventually led him to a process that he describes as fitting neatly within the risk assessment and risk management framework. More generally, the risk analysis scheme is indeed the dominant reference in the area of information security as well as of systems and infrastructures security. This scheme comes with its own history, institutionalizations and difficulties. At the end of all of those, its blind spot remains a much more intricate nexus of trade-offs than the dichotomies and one-sided diets can allow for: on the one hand the trade-offs not just between risks or between a risk and a cost, but between costs, risks and benefits as well as between the distributions thereof; on the other hand the sharp and untenable divides between risk assessment and risk management, between science and policy, between knowledge and decision.

### *The measure of all things*

As indicated above, it is incumbent upon us to ask whether the notion of gain (at the heart of the trade-off) should not be seen as problematic in the absence of a robust form of assessment, of valuation or evaluation.

Beyond the minimal requirement of scrutinizing the cost and the effectiveness of such endeavours (i.e. of choices as to the taking up and deployment of new security and surveillance technologies) – minimal requirement that is, far too often, not even met – the questions pertaining to the assessment are the following: what is gained, what is lost, by whom, how is this framed and measured and shared, by whom, and how is this articulated to decision-making processes.

The evaluation framework must necessarily comprise the assessment of the *pros* as well as the *cons* (and ins and outs, lock-ins, limits and constraints, SWOTs i.e. strengths, weaknesses, opportunities, and threats) of specific security investments. This is not enough, however, as what is needed is to have evaluations that are comparative and not focussed on a specific technology or specific security investment; not focussed on a 'technological fix' or 'security solution' when the issue might be differently framed and indeed differently addressed.

It is also important that such ex ante evaluations of security investments provide an authentic aid to decision-making rather than legitimise a set of pre-defined policy options. Indeed any framing in the form "there is no choice, there is no alternative, there is no need and no room for debate and justification, we simply have to do it" cannot be condoned.

This points to the dialectics of means and ends in which security and surveillance are set. Whereas security is initially presented as a means to enable or ensure individual and collective flourishing (with surveillance, in turn, as a means towards security), what is often witnessed – or indeed obfuscated – is the creeping displacement of security which becomes an end in itself. Security is thus mistakenly taken as synonymous with, or an instantiation of, the common good.

At the heart of the above difficulties is precisely the issue of general interest and common good, bearing in mind that allocation of resources is also a matter of justice and solidarity. These difficulties are compounded by the dearth of public debate on security as a means, on the choice of means (including surveillance technologies) to enhance security, and on the ends towards which it is put. In fact public debate (understood as such and as a shorthand for the mustering of other facets of the democratic apparatus) is a necessary component of the evaluative framework outlined above.

The present Opinion is also a part of this reflexive and informed sustained debate, which it calls for.

Having scrutinized the rich conceptual fabric of security and surveillance, with their ins and outs and diverse facets (relating to vigilance, vulnerability, secrecy, control, fulfilment, etc – cf. Chapter 3), it is important in this context to draw attention to another dimension of the question of *root causes*. It is important to counterpoint the Matthew effect at play within (and between) societies by considering the socio-economic disparities – indeed the grave matter of inequalities broadly construed – as a determinant of the ratcheting up in which security and surveillance are set. This is to be considered at individual level (with the notion of property and the importance attached to the protection of private property) as well as with regard to state security, also extending to the supra-national level, European notably.

What is Europe ultimately to protect? To secure? From Kiev to Lampedusa, and also through to Athens and even to Sidi Bouzid, those are acute question to address.

#### *Towards recommendations as to security and surveillance technologies*

Surveillance by the state, national security, law and order surveillance, intelligence gathering, corporate surveillance and scooping of privately shared data are often interlinked and function as 'security and surveillance assemblages'. While this sombre reality should be recognized, it should not be succumbed to in analytical and prescriptive terms. In other words, the different strands of the assemblages have to be disentangled and addressed



specifically, in accordance with their different uses. Since different agents have different responsibilities, the principles need to be translated into more context-sensitive criteria, in order to meet the needs of companies, on the one hand, and the state, on the other hand.

But it is also at that juncture that the trade-off narrative constitutes a misleading framework: the equilibrium found in the one context, i.e. corporate data usage and data sharing, may not be applicable in the other, i.e. state security, exactly because the individual cannot opt in or opt out. The question, then, becomes how the individual can be respected in his or her rights to privacy and security when the very protection of these rights require their violation – what seems to be a ‘normal’ process of prioritization easily turns into a contradiction and it is for *this* reason that the rights must not be ‘traded’ but, quite the contrary, must restrict the trade-off.

The EGE’s recommendations aim at identifying criteria of accountability and oversight in order to protect the freedom of individuals together with their security. It remains to be seen whether it is possible to overcome the ‘trade-off’ metaphor and return to the traditional metaphor of prioritization of rights – a metaphor that does not give up on any of the rights, even though it acknowledges that priorities may differ not only between individuals but also differ in different contexts. As trust reflects the sense of a general acceptance or, put differently, the societal affirmation that a good equilibrium has been found between individual freedom and privacy, and justice and social security, mistrust reflects exactly the opposite: the sense of a general unease and potential renunciation or, put differently, the societal objection to the imbalance between freedom and privacy, and justice and social security.



## Recommendations

The EGE has been asked to formulate an opinion on the ethical implications of security and surveillance technologies. This is a timely but difficult task, as these technologies represent very different purposes, are performed by different actors, entail different stages and forms of intrusion on human rights and lead to different uses.

The increasing availability of large amounts of information and the growth of communication networks have been major factors in the globalisation of the 20th century. Another feature of a globalised world is the feeling of insecurity, a lack of trust and a low tolerance of risk. Shootings in schools, cinemas and shopping centres, explosives on the underground, trains and aeroplanes, abduction of children, beatings and robberies of older people have served to increase our sense of feeling unsafe in our own communities. This perception persists despite the fact that all objective measures tell us that there has never been a safer time to live. The desire of Governments to respond to the perception of a feeling of insecurity amongst its citizens has undoubtedly driven securitization approaches adopted in Europe and elsewhere.

Security, employed in the rather narrow sense, involves protection from physical harm or the threat of harm and is a fundamental component of well-being. Through the social contract, States have committed to provide security for the citizenry in exchange for the power to curtail individual liberty. This is however, but one aspect of the security paradigm. Protecting physical integrity is necessary but not sufficient. Security needs to be viewed in the broader context which encompasses both human and societal security. This requires us to expand our considerations from the role of the State to that of individuals, communities and commercial entities. Europe is a community of shared values where we strive to safeguard dignity, autonomy, freedom and justice through our Human Rights Framework. This provides an environment in which the person can flourish through creativity, innovation, development of strong personal relationship with others and their contribution to their communities. Education, health, democracy, environment and equality are all essential elements in realising the goal of a secure Europe.

The rather limited approach to achieving security, most especially when it comes to the narrow interpretation of state security, has been to engage in the narrative of trade-offs, the classic example being the trade-off between freedom, often embodied as privacy, and security. While a proper balance needs to be struck between competing principles or values when they come into conflict, there are some core principles such as human dignity which simply cannot be traded away. This requires us to move beyond the rhetoric of trade-offs and into a more nuanced approach where security technologies and measures are assessed on the basis of proportionality and effectiveness and rights are prioritised rather than traded.

The EGE recognises that an entirely legitimate manifestation of state power in a democratic society is to have agencies that according to strict legal limitations are permitted to use surveillance as a means of safeguarding the security of its citizens. The EGE would also assert that elements of secrecy and discretion are an intrinsic aspect of the **dignity** of human life. Infringement by a public authority of a person's right to privacy must be **justified** and

should be subject to judicial oversight. Surveillance must be **necessary** and **proportionate** in order to ensure an appropriate connection between the actions taken and the objectives achieved. A key element in assessing proportionality is the **effectiveness** of the intervention and effectiveness must be reviewed regularly. Powers to surveil should be granted for a defined purpose and for a defined period of time. **Alternatives** capable of achieving the same goal should be examined and documented and the least intrusive method should be selected. **Accountability** is a necessary pre-requisite for public surveillance thus, it should be clear that surveillance is being undertaken for appropriate reasons and in conformance with publicly available codes of practice. Security and surveillance technologies must be applied with as great a degree of **transparency** as possible, with legitimate exceptions explicitly determined in the legal system. Private and or commercial organisations involved in surveillance should also be bound by the aforementioned criteria.

In these regards, discrimination is an important area of concern. We need to be mindful of the possible unanticipated effects of ubiquitous surveillance. It corrals individuals towards conforming to forms of normality (as normativity), thus behaving differently and further strengthening that norm, and thus in turn giving rise to an impoverished – if not neutered – society (where diversity, creativity and even cohesiveness have been rooted out). Discrimination may concern the specific targeting and/or surveillance of minorities, and the EGE calls for action where and when this is the case in EU Member States. Furthermore, discrimination relates to issues of profiling as well as of stigmatization. Concerning profiling, it should be recognized that it takes many forms, from opt in/out programs (such as Global Entry) to 'face crime' and face recognition (and other biometrical systems), through to the profiling of all through advanced mass surveillance. Concerning stigmatization, while it is clear that it (and its correlate, humiliation) must be avoided, the role played by the increasingly pervasive use of algorithms as part of security and surveillance assemblages is particularly alarming in that regard. These algorithms can obfuscate or confiscate ethical reflexivity and justification of choices, resulting in in-built profiling or 'stigmatization by design'. In doing so they also risk perfecting the normality and compliance alerted to above, by black-boxing selection processes, removing them from human intervention and understanding. In this regard the EGE is fully aware of the risk of instrumentalisation of ethics councils and cognate bodies in these processes of normalisation pertaining to new technologies. Indeed the EGE is fully aware of the difficulties inherent to the embracing from an ethical perspective of the topic of security and surveillance technologies without this being understood as a form of overall condoning. It has chosen not to shy away from those difficulties but to confront them head-on in this Opinion.

Based on these considerations the EGE agrees on the following recommendations in the field of security and surveillance technologies:

**I.** Technologies with the potential to intrude into the privacy of individuals *and* to which they cannot consent (or cannot opt out), require specific justification. The EGE calls for a *case by case justification* for these measures.

#### 1. **Accountability**

Member States need to ensure that those granted with powers to surveil the private sphere of citizens are acting in the public interest and are accountable for their

actions. Where the State delegates security and/or surveillance tasks to private companies, they are bound by the same legal and ethical obligations and Member States should put in place mechanisms to monitor compliance with such obligations.

## **2. Judicial oversight**

Member States must have a system of judicial oversight for surveillance carried out by public authorities in order to investigate crime. The individual should be informed post-hoc that they have been the subject of surveillance provided that no investigation is prejudiced as a result. An individual should have the opportunity to seek redress from the Courts if they have been the subject of unlawful surveillance.

## **3. Towards a common understanding of national security**

*The shared European values enshrined in the Charter of Fundamental Human Rights represent the normative framework on which a common ethical understanding of national security could be built.*

**a)** While recognising that national security is legitimately placed at the heart of national interests and is a competence of Member States, the EGE recommends that EU institutions in conjunction with Member States should find ways to establish such a common understanding of national security.

**b)** The EGE also recommends that Member States should establish procedural means to keep other Member States appropriately informed of extra jurisdictional intelligence activities in order to preserve trust between partners.

**c)** Member States should not in the name of national security surveil other Member States for commercial advantage, because it conflicts with the EU objective of achieving a single European market.

## **4. Drones**

*The rapid development and increased deployment of drones by Member States in military, civilian and commercial contexts has not been accompanied by the necessary governance and oversight arrangements, which remain fragmented at best. For civilian and commercial uses, the EU lacks a comprehensive legal framework for the development, acquisition, use and export of drones. The EGE welcomes actions already taken by the European Commission in the area of Remotely Piloted Aircraft Systems (RPAS) integration in the EU aviation system (including wide ranging consultation and the publication of a roadmap). The inclusion from the outset, of a consideration of societal implications of drone deployment is to be commended.*

**a)** Given the recent EU commitment for improved coordination amongst Member States in the development and acquisition of drones, the EGE recommends that this cooperation be extended to the generation of common standards and a regulatory framework governing the civilian and commercial use of drones within the EU. Particular attention should be paid to an evaluation of existing EU data protection and privacy frameworks, in order to assess if the current regulatory regime is fit for

purpose in the context of Remotely Piloted Aircraft Systems integration in European airspace.

**b)** Member States must ensure that national policies regarding use of drones domestically (i.e. within national borders), in the public sphere, do not violate the human rights of those subject to drone operations. Domestic use of drones should be subject to an authorisation and proper oversight to ensure safety and prevent misuse. Further, those seeking authorisation for the use of surveillance drones must demonstrate that the proposed use is justified, necessary and proportionate. The EGE also recommends that policies and procedures governing the domestic use of drones for the purpose of surveillance should be publically available in the interests of transparency, a prerequisite of public trust.

**c)** The EGE draws attention to the grave ethical implications of the military use of drones as well as of automated warfare, and acknowledges the European Parliament resolution on the use of armed drones of 25 February 2014. The EGE calls for greater transparency and accountability on the part of Member States that operate drones for military purposes. To that end, Member States must disclose the legal basis, scope, and limits of any lethal drone strikes and there must be scrutiny that existing legal frameworks that apply to traditional armed conflicts are not being violated. Information on the number of civilians and non-civilians killed in drone strikes should also be publicly available. Further, the EGE strongly advocates research to address the ethical implications of lethal drone strikes and their compatibility or otherwise with just war theory. Moreover, research is required on the role of moral agency where drone operators are situated remotely as well as in relation to the development of autonomous drones.

**II.** Regarding surveillance technologies, the burden of proof should lie with states and/or companies, who have to demonstrate *publicly and transparently*, before introducing surveillance options,

- that they are **necessary**
- that they are **effective**
- that they respect **proportionality** (e.g. purpose limitation)
- that there are no better **alternatives** that could replace these surveillance technologies

These criteria must then also be subjected to **post factum assessment**, either on the level of normal political analyses, or through Member States policies to do so.

Furthermore:

**Accountability** means that individuals have the right to be informed about surveillance technologies - even though in some cases this information may only be provided ex post;

**Transparency** with respect to economic interests must be ensured at all times.

## 5. **Personal data**

The EGE affirms that the purpose limitation principle as regards personal data be the standard for both public and private organisations. Personal data should only be collected for a specific and legitimate purpose. As far as possible data should be anonymised and greater use should be made of encryption which can serve to enhance both privacy and security. Data sharing by default is to be avoided and users should be allowed to control (e.g. through access to privacy settings) and change information held by organisations about them. Profiling of individuals for commercial purposes should be subject to the individual's explicit consent. Information should be available by commercial organisations in relation to *what data* are going to be collected, *by whom*, for *what purpose*, for *how long* and if data collected will be linked with other data sources.

## 6. **Public awareness of data policies**

The EGE reaffirms its view that there needs to be greater clarity for the public in relation to how, why and for what purpose their personal information is managed, shared and protected. Public authorities as well as corporate actors must make their policies in that regard publicly available. The EU and Member States should seek to foster public knowledge, awareness and debate on the implications for individuals and wider society of the use of security and surveillance technologies. Education programs should start at school level and should provide information and tools for citizens to safeguard their data in the digital environment.

## 7. **Big data**

The EGE notes the shift towards collection and correlation of large datasets, so called "big data". While the EGE recognises the potential value of such datasets, we are concerned that without proper attention, the principle of purpose limitation at the core of data protection will be undermined. Thus, the EGE urges public authorities and private organisations to engage in purposeful ethical inquiry to inform and align their actions with shared European values of dignity, privacy and autonomy. The EGE recommends that the EU develop a code of conduct for big data analytics that would guide organisations with the process.

## 8. **Algorithms**

In the context of security and surveillance technologies, it is important to note that algorithms are necessarily selective in their design and are as subject to bias as the humans which program them. Underlying algorithms and their parameters are ethical assumptions and these should be made explicit as a mandatory requirement. Moreover, algorithms are not infallible and the data generated are contingent on the choice and quality of data input, which in the view of the EGE should be continually examined and validated. Furthermore, education on the ethical aspects in the design of algorithms should be included in the training of developers.

## 9. **e-Privacy**

The EGE recommends that the EC give consideration to revising the e-Privacy

Directive, the scope of which currently encompasses electronic communications. Given the explosion of digital interfaces since the introduction of the Directive, the EGE considers it appropriate that VoIP – Voice over Internet Protocol, indeed IP communications, broadband communications – products and also corporate private networks would be included in the remit of any revised Directive.

#### **10. Privacy Impact Assessment**

Privacy Impact Assessments procedures must form part of regulatory practice in Member States when new or modified information systems which process personal data are being introduced to the market. The assessment should address the potential implications of the proposed technology for personal data and if risks are identified, measures should be taken to identify processes to mitigate the risk or indeed alternatives to that which is proposed.

#### **11. Migration and border control**

Border control is one area where security and surveillance technologies are broadly applied. This raises several concerns as regards the impact on human rights and the solidarity principle, both globally and among EU Member States. The EGE recommends to evaluate the Border Control Systems in view of the criteria set up in this Opinion, namely dignity and human rights, justice, necessity, proportionality, effectiveness, alternatives, and accountability.

In line with the findings of the Article 29 working party, the EGE is concerned that the Entry/Exit System (EES) proposed under the Smart Borders Initiative involves a disproportionate intrusion into individual's privacy. The Stockholm programme notes that new systems should only be developed if it is established that existing systems are not sufficient; the EGE is not convinced that this criterion has been met in the case of the entry/exit program and recommends a moratorium on the introduction of the EES, while existing systems such as the Visa Information System are evaluated to see if the objectives of the EES can be met in a proportionate manner.

Acknowledging that large-scale EU databases such as Registered Travellers Program (RTP) and Entry/Exit System (EES) used for border control purposes can pose risks to the rights of EU and non-EU nationals, a proportion of whom are particularly vulnerable, the implementation of these databases should be subject to a rigorous evaluation with particular attention paid to their impact on fundamental rights and adherence to the principle of purpose limitation.

**III.** Ethical and legal assessment criteria go hand in hand. They can (re-)build **trust** only together, and therefore the EGE recommends several different measures intended more concretely to build up trust and represent citizens' interests in having/maintaining control over their personal affairs. These include issues of oversight, enforcement, whistleblowing, public information, education, training and research.



## **12. Trustworthy oversight**

The EGE recognises that in matters of national security it is not always possible to be transparent regarding surveillance activities. Nonetheless, public trust is crucial to the legitimacy of States actions in the pursuit of security. To that end, the EGE recommends that, without prejudice to judicial oversight, Member States establish or expand existing mechanisms in the form of a body or person vested with powers of oversight to act as a trusted third party on behalf of the public. The role of such an entity would include monitoring the effects of both public and private surveillance on the rights and duties of citizens. Aggregate information on the number of requests made for surveillance powers, by whom and for what purpose should be published by Member States thereby ensuring transparency and accountability. Member States should consult such a body or person in advance of introducing legislation pertaining to surveillance. The EGE envisages that the trusted third party would have a key role in raising public awareness and stimulating debate with regard to the risks and benefits of surveillance.

## **13. Data protection enforcement**

The EGE is of the view that the protection of data enshrined in EU law is robust but requires to be enforced at the national level. Member States should therefore ensure that data protection authorities have sufficient legal powers, technical expertise and resources to ensure effective levels of enforcement across the European Union.

## **14. Whistleblowing**

The European Commission and Member States should ensure that an effective and comprehensive whistle-blower protection mechanism is established in the public and private sectors. In line with the Transparency International principles as articulated in the 2013 *Whistleblowing in Europe* Report, in situations where national security is involved, whistleblower regulations and procedures should be present and clear; maintain confidentiality or anonymity; ensure thorough, timely and independent investigations of whistleblowers' disclosures; and have transparent, enforceable and timely mechanisms to follow up on a complaint of a whistleblower in relation to retaliation. Where a disclosure concerns matters of national security, official or military secrets, or classified information, special procedures and safeguards for reporting that take into account the sensitive nature of the subject matter should be adopted in order to promote successful internal follow-up and resolution and to prevent unnecessary external exposure. These procedures should permit internal disclosures, disclosure to an autonomous oversight body that is institutionally and operationally independent from the security sector, or disclosures to authorities with the appropriate security clearance. External disclosure (that is, to the media or civil society organisations) would be justified as a last resort.

### **15. Designing privacy**

Public and private organisations should adopt privacy-by and privacy-in design principles for development of security and surveillance technologies. The European values of dignity, freedom and justice must be taken into account before, during and after the process of design, development and delivery of such technologies. Privacy enhancing technologies should be integrated from the outset and not bolted on following implementation. In the view of the EGE, instilling a culture in organisations, where privacy is understood and reflected in practice, can be achieved through engineers, developers and experts in philosophical and ethical reflection working together in an interdisciplinary way. The introduction of ethical courses and training both on a theoretical and practical level in engineering and informatics for undergraduate and post-graduate students, but also during vocational education and training could improve the grasp of privacy by and in design approaches in the field of security and surveillance technologies.

### **16. Understanding and valuing privacy**

Privacy is not a static concept and a fuller understanding of how European citizens conceptualise and value privacy is required, if appropriate steps are to be taken to safeguard physical and informational privacy. To this end, the EU should make funds available for research to examine and analyse how citizens consider, and cultivate their involvement in, issues related to security and surveillance.

---

**Avis Nr. 28 du Groupe Européen d'Éthique des Sciences et des Nouvelles  
Technologies auprès de la Commission Européenne**

## **Éthique des Technologies de Sécurité et de Surveillance**

*Bruxelles, 20 Mai 2014*

*Référence:* avis requis par le **président Barroso**

*Rapporteurs:* **Inez de Beaufort, Linda Nielsen, Siobhán O'Sullivan**

*Seul le texte original en anglais est authentique.*



## Recommandations

Le GEE a été invité à émettre un avis sur les aspects éthiques des technologies de sécurité et de surveillance. Il s'agit là d'une tâche certes d'actualité, mais difficile, étant donné que ces technologies représentent des objectifs très divers, sont mises en œuvre par différents acteurs, entraînent différents degrés et formes d'atteintes aux droits de l'homme, et débouchent sur différentes utilisations.

La disponibilité croissante de volumes importants d'informations et l'expansion des réseaux de communication ont joué un rôle déterminant dans la mondialisation qui s'est produite au 20<sup>e</sup> siècle. Cette évolution s'est par ailleurs accompagnée d'un sentiment accru d'insécurité, d'un manque de confiance et d'un faible niveau de tolérance à l'égard du risque. Les tueries perpétrées dans les écoles, les cinémas et les centres commerciaux, les attentats aux explosifs commis dans le métro, les trains et les avions, les enlèvements d'enfants et les sévices et vols visant les personnes âgées ont contribué à renforcer le sentiment d'insécurité que nous éprouvons au sein même de nos communautés. Cette perception persiste, alors même que, objectivement, tout indique que le monde n'a jamais été aussi sûr qu'aujourd'hui. Il ne fait aucun doute que les stratégies de sécurisation adoptées en Europe et dans d'autres parties du monde résultent de la volonté des pouvoirs publics de répondre à ce sentiment d'insécurité éprouvé par les populations.

Selon une acception assez étroite, la sécurité désigne la protection des personnes contre les préjudices physiques ou la menace de tels préjudices, et constitue un élément essentiel du bien-être. En vertu du contrat social, les États se sont engagés à garantir la sécurité de leurs citoyens en échange du pouvoir de restreindre les libertés individuelles. Cela ne représente toutefois qu'un aspect de la problématique de la sécurité. En effet, si la protection de l'intégrité physique est nécessaire, elle n'est pas suffisante. La sécurité doit être envisagée dans un contexte plus large englobant à la fois la sécurité des individus et celle de la société dans son ensemble. Il nous faut dès lors élargir notre réflexion au-delà du seul rôle de l'État et nous pencher sur celui des individus, des communautés et des entités commerciales. L'Europe est une communauté de valeurs partagées au sein de laquelle nous nous efforçons de préserver la dignité, l'autonomie, la liberté et la justice en nous appuyant sur les droits de l'homme. L'environnement ainsi créé permet à l'individu de s'épanouir en laissant libre cours à sa créativité et à son esprit d'innovation, en nouant des relations personnelles solides et en participant à la vie de sa communauté. L'éducation, la santé, la démocratie, l'environnement et l'égalité sont autant d'éléments essentiels pour atteindre l'objectif d'une Europe sûre.

L'approche plutôt restrictive adoptée jusqu'ici en matière de sécurité, notamment dans le contexte de l'interprétation étroite de la sécurité de l'État, a consisté à se concentrer sur la théorie selon laquelle il faudrait nécessairement accepter des compromis, un exemple classique étant le compromis entre la liberté, souvent représentée sous l'angle de la vie privée, et la sécurité. S'il est certes nécessaire de trouver un bon équilibre entre des principes ou valeurs concurrents lorsqu'ils sont incompatibles, le respect de certains principes fondamentaux, comme celui de la dignité humaine, n'est tout simplement pas négociable. Aussi devons-nous dépasser la rhétorique des compromis pour nous engager dans une approche plus nuancée dans laquelle les technologies et les mesures de sécurité

sont évaluées à l'aune de leur proportionnalité et de leur efficacité et dans laquelle les droits, au lieu de faire l'objet de marchandage, sont considérés comme prioritaires.

Le GEE reconnaît que, dans une société démocratique, il est parfaitement légitime que le pouvoir de l'État se manifeste par la mise en place d'agences qui, sous réserve de restrictions légales strictes, sont autorisées à recourir à des technologies de surveillance pour préserver la sécurité des citoyens. Le GEE considère également que la **dignité** de la vie humaine suppose un certain degré de confidentialité et de discrétion. Lorsque les pouvoirs publics portent atteinte au droit à la vie privée d'un individu, ces atteintes doivent être **justifiées** et devraient faire l'objet d'un contrôle sous l'autorité d'un juge. La surveillance doit être **nécessaire et proportionnée** afin qu'il existe un lien approprié entre les mesures prises et les objectifs atteints. L'**efficacité** de l'intervention est un élément essentiel pour évaluer sa proportionnalité, et cette efficacité doit être réexaminée à intervalles réguliers. Les compétences en matière de surveillance devraient être accordées pour des buts spécifiques et une durée déterminée. Il convient d'examiner et de documenter les **solutions alternatives** permettant d'atteindre les mêmes objectifs, et d'opter pour la méthode la moins intrusive. L'**obligation de rendre compte** étant un préalable indispensable à la surveillance publique, il doit apparaître clairement que les activités de surveillance sont menées pour des motifs valables et dans le respect des codes de bonnes pratiques accessibles au public. La mise en œuvre des technologies de sécurité et de surveillance doit être aussi **transparente** que possible et les exceptions légitimes doivent être prévues expressément dans l'ordre juridique. Il convient que les organisations privées et/ou commerciales menant des activités de surveillance soient elles aussi tenues de respecter les critères susmentionnés.

La discrimination est un grave sujet de préoccupation à cet égard. Nous devons être conscients des effets imprévus que pourrait avoir une surveillance omniprésente. En effet, ce type de surveillance pousse les individus à se conformer à une certaine normalité (en tant que normativité), et donc à modifier leurs comportements et à renforcer davantage encore cette norme. Il en résulte une société appauvrie - voire totalement uniformisée - privée de toute diversité, créativité, et même cohésion. La discrimination peut consister à cibler et/ou surveiller plus spécifiquement certaines minorités: le GEE demande que des mesures soient prises lorsqu'une telle situation est constatée dans un État membre de l'Union. Elle concerne également la question du profilage et celle de la stigmatisation. Il faut reconnaître que, dans le cas du profilage, les formes sont multiples, allant des programmes de type «opt in/out» (comme le programme Global Entry) au profilage de populations entières au moyen de techniques sophistiquées de surveillance de masse, en passant par les «délits de faciès» et la reconnaissance des visages (ou d'autres systèmes biométriques). Pour ce qui est de la stigmatisation, si elle doit de toute évidence être évitée (de même que son corollaire, l'humiliation), le rôle joué par l'utilisation de plus en plus généralisée des algorithmes dans les dispositifs de sécurité et de surveillance est particulièrement préoccupant à cet égard. Ces algorithmes peuvent en effet brouiller ou confisquer la réflexivité éthique et la justification des choix, avec pour résultat le profilage intégré ou la «stigmatisation par conception». Ils sont également susceptibles de renforcer encore la normalité et la conformité mentionnées ci-dessus, en occultant les processus de sélection et en les dissociant de toute intervention et de tout raisonnement humains. Le GEE n'ignore en rien le risque d'instrumentalisation des conseils d'éthique et des organismes apparentés dans ces processus de normalisation liés aux nouvelles technologies. Il est en effet parfaitement conscient de la difficulté qu'il y a à se pencher sur les aspects éthiques des technologies de

sécurité et de surveillance sans que cela soit perçu comme une sorte de cautionnement global. Il a choisi de ne pas reculer devant cette difficulté, mais de l'attaquer de front dans cet avis.

Au vu des considérations qui précèdent, le GEE convient des recommandations suivantes dans le domaine des technologies de surveillance et de sécurité:

**I.** Le recours aux technologies qui sont susceptibles de porter atteinte à la vie privée des individus *et* que ces derniers n'ont pas la possibilité d'accepter ou de refuser, nécessite une justification particulière. Le GEE demande qu'une *justification au cas par cas* soit exigée pour ces mesures.

**1. Obligation de rendre compte**

Les États membres doivent veiller à ce que les organismes habilités à surveiller la sphère privée des individus agissent dans l'intérêt général et soient tenus de rendre compte de leurs actes. Lorsque l'État délègue des tâches de sécurité et/ou de surveillance à des entreprises privées, ces entreprises sont soumises aux mêmes obligations légales et éthiques; il convient, par ailleurs, que les États membres mettent en place des mécanismes permettant de vérifier que ces obligations sont respectées.

**2. Contrôle effectué par les juges**

Les États membres doivent disposer d'un système de contrôle sous l'autorité des juges pour les activités de surveillance menées par les pouvoirs publics dans le cadre d'enquêtes pénales. Il convient que les individus soient informés a posteriori de la surveillance dont ils ont fait l'objet, pour autant que cela ne compromette pas le déroulement d'une enquête. Tout individu ayant fait l'objet d'une surveillance illicite devrait avoir la possibilité d'exercer son droit de recours.

**3. Vers une conception commune de la sécurité nationale**

*Les valeurs européennes communes inscrites dans la Charte des droits fondamentaux de l'Union européenne constituent le cadre normatif qui pourrait servir de base à une conception éthique commune de la sécurité nationale.*

**a)** Tout en reconnaissant que la sécurité nationale figure, à juste titre, au cœur des intérêts nationaux et relève de la compétence des États membres, le GEE recommande que les institutions de l'Union, en concertation avec les États membres, trouvent les moyens de parvenir à une conception commune de la sécurité nationale.

**b)** Le GEE recommande également que les États membres mettent en place des procédures leur permettant de tenir les autres États membres dûment informés de leurs activités de renseignement extraterritoriales afin de préserver la confiance entre les différents partenaires.

**c)** Il convient que les États membres s'abstiennent de surveiller d'autres États membres sous couvert de sécurité nationale dans le but d'en retirer un avantage

commercial, cette activité étant contraire à l'objectif de l'Union de mettre en place un marché européen unique.

#### **4. Drones**

*Le développement rapide des drones et leur déploiement accru par les États membres dans des contextes militaires, civils et commerciaux n'ont pas été accompagnés par des mesures de gouvernance et de contrôle, de sorte que les dispositions en vigueur demeurent pour le moins fragmentaires. Pour les usages civils et commerciaux, l'Union doit se doter d'un cadre juridique détaillé régissant le développement, l'achat, l'utilisation et l'exportation des drones. Le GEE se félicite des mesures déjà adoptées par la Commission dans le domaine de l'intégration des systèmes d'aéronefs télépilotes (Remotely Piloted Aircraft Systems ou RPAS) dans le système aéronautique européen (incluant l'organisation d'une vaste consultation et la publication d'une feuille de route). Et le fait qu'il ait d'emblée été prévu de prendre en considération les conséquences du déploiement des drones sur la société dans son ensemble, doit être salué.*

**a)** Compte tenu de l'engagement pris récemment par l'Union d'améliorer la coordination entre les États membres dans le domaine du développement et de l'achat des drones, le GEE préconise d'étendre cette coopération à l'établissement de normes communes et d'un cadre réglementaire régissant les usages civils et commerciaux des drones dans l'Union. Il conviendra en particulier d'évaluer les cadres mis en place par l'Union en matière de protection des données et de la vie privée afin de déterminer si le régime réglementaire en vigueur est approprié dans le contexte de l'intégration des systèmes d'aéronefs télépilotes dans l'espace aérien européen.

**b)** Les États membres doivent veiller à ce que leurs politiques en matière d'usage des drones dans la sphère publique domestique (c'est-à-dire à l'intérieur des frontières nationales) ne portent pas atteinte aux droits humains des personnes visées par les opérations impliquant des drones. Cet usage des drones dans la sphère publique domestique doit être soumis à autorisation et faire l'objet d'un contrôle approprié afin de garantir la sécurité et de prévenir les abus. En outre, les personnes ou entités sollicitant l'autorisation d'utiliser des drones de surveillance doivent démontrer que l'usage envisagé est justifié, nécessaire et proportionné. Le GEE recommande également que les politiques et procédures régissant l'usage des drones dans la sphère publique domestique à des fins de surveillance soient mises à la disposition du public afin de garantir la transparence, sans laquelle il est impossible d'obtenir la confiance du public.

**c)** Le GEE attire l'attention sur les graves problèmes éthiques que soulèvent l'usage militaire des drones et la guerre robotisée, et prend note de la résolution du Parlement européen du 25 février 2014 sur l'utilisation des drones armés. Le GEE appelle les États membres qui utilisent des drones à des fins militaires à faire preuve d'une plus grande transparence et à veiller à respecter leur obligation d'en rendre compte. À cette fin, ils doivent divulguer la base juridique, la portée et les limites de toute frappe mortelle réalisée au moyen de drones et contrôler le respect des cadres juridiques existants applicables aux conflits armés traditionnels. Les informations



concernant le nombre de civils et d'autres personnes tués au cours de frappes de drones devraient également être mises à la disposition du public. Le GEE préconise par ailleurs vivement la réalisation de travaux de recherche portant sur les aspects éthiques des frappes mortelles par des drones armés et sur leur compatibilité avec la théorie de la guerre juste. Il importe en outre d'effectuer des recherches sur l'implication de l'agir moral lorsque les opérateurs de drones se trouvent à distance, et que se développent des drones autonomes.

II. En ce qui concerne les technologies de surveillance, la charge de la preuve devrait revenir aux États et/ou aux entreprises, lesquels, avant d'introduire des systèmes de surveillance, doivent démontrer *de manière publique et transparente*:

- que ces systèmes sont **nécessaires**,
- que ces systèmes sont **efficaces**,
- que ces systèmes respectent le principe de proportionnalité (limitation de la finalité, par exemple);
- qu'il n'existe aucune **solution de remplacement** meilleure pouvant se substituer à ces technologies de surveillance.

Ces critères doivent également être soumis par la suite à une évaluation **post factum**, soit dans le cadre des analyses politiques normales, soit dans le cadre des politiques des États membres.

En outre:

L'**obligation de rendre des comptes** implique que les individus sont en droit d'être informés des technologies de surveillance mises en œuvre - même si, dans certains cas, ces informations ne peuvent être communiquées qu'a posteriori;

La **transparence** en ce qui concerne les intérêts économiques doit être respectée à tout moment.

## 5. Données à caractère personnel

Le GEE estime que, dans le domaine des données à caractère personnel, les organisations publiques comme les organisations privées doivent se fonder sur le principe de limitation de la finalité. Autrement dit, les données à caractère personnel ne devraient être recueillies que dans un objectif spécifique et légitime. Les données ainsi recueillies devraient, si possible, être anonymisées et le cryptage devrait être plus largement utilisé, étant donné qu'il peut contribuer à améliorer à la fois la protection de la vie privée et la sécurité. Il convient d'éviter le partage des données par défaut, et de permettre aux utilisateurs de contrôler (par exemple au moyen de paramètres de confidentialité) et de modifier les informations les concernant et détenues par les organisations. Le profilage d'individus à des fins commerciales devrait être subordonné au consentement explicite des personnes concernées. Les organisations commerciales devraient indiquer la *nature des données* qu'il est prévu

de recueillir, *par qui* la collecte sera effectuée, dans *quel objectif*, pendant *combien de temps*, et s'il est prévu de relier les données recueillies à d'autres sources de données.

#### **6. Sensibilisation du public aux politiques en matière de données**

Le GEE réaffirme qu'il est, selon lui, nécessaire de mieux informer les membres du public sur les modalités, les raisons et les objectifs de la collecte, du partage et de la protection des données à caractère personnel les concernant. Les pouvoirs publics comme les entreprises doivent, à cet égard, rendre accessibles au public leurs politiques. Il convient que l'Union et les États membres s'efforcent de promouvoir la connaissance, la sensibilisation et le débat quant aux conséquences du recours aux technologies de sécurité et de surveillance sur les individus et la société dans son ensemble. Dès l'école primaire, des programmes d'éducation devraient fournir des informations et des instruments qui permettront aux individus de protéger leurs données personnelles dans l'environnement numérique.

#### **7. Données en masse (« Big data »)**

Le GEE constate une évolution vers la collecte et la corrélation d'ensembles volumineux de données, appelés «données en masse» («big data»). Bien que le GEE reconnaisse la valeur potentielle que revêtent ces ensembles de données, il craint que, si l'on n'y prend pas garde, le principe de limitation de la finalité, qui est au cœur de la protection des données, soit mis à mal. C'est pourquoi il exhorte les pouvoirs publics et les organisations privées à entreprendre une réflexion éthique poussée qui éclairera leurs actions et leur permettra de les aligner sur les valeurs européennes communes que sont la dignité, le respect de la vie privée et l'autonomie. Le GEE recommande que l'Union élabore un code de conduite pour l'analyse des données en masse qui guiderait les organisations dans ce processus.

#### **8. Algorithmes**

Dans le contexte des technologies de sécurité et de surveillance, il importe d'observer que les algorithmes sont par définition sélectifs et que leur impartialité est tout aussi sujette à caution que celle des personnes qui les programment. Les algorithmes sous-jacents et leurs paramètres sont des hypothèses éthiques qu'il devrait être obligatoire d'explicitier. En outre, les algorithmes ne sont pas infallibles et les données produites dépendent des données d'entrée utilisées et de la qualité de celles-ci, qu'il conviendrait, selon le GEE, d'examiner et de valider en permanence. Il convient par ailleurs de prévoir, dans le cadre de la formation des personnes chargées de l'établissement des algorithmes, d'aborder les aspects éthiques de cette activité.

#### **9. Protection de la vie privée dans les communications électroniques**

Le GEE recommande que la Commission européenne envisage de réviser la directive sur la vie privée et les communications électroniques, dont le champ d'application actuel couvre uniquement les communications électroniques. Compte tenu de l'explosion des interfaces numériques qui s'est produite depuis l'entrée en vigueur de la directive, le GEE juge opportun de réviser cette directive en élargissant

son champ d'application aux produits relevant de la téléphonie par internet (voice over Internet Protocole – VOIP - les communications sur IP et à haut débit), ainsi qu'aux réseaux privés d'entreprise.

#### **10. Évaluation de l'impact sur la vie privée**

Les procédures d'évaluation de l'impact sur la vie privée doivent faire partie intégrante de la pratique réglementaire des États membres lorsque des systèmes d'information nouveaux ou modifiés sont introduits sur le marché. L'évaluation devrait porter sur les conséquences potentielles de la technologie proposée sur les données à caractère personnel et, si des risques sont répertoriés, des mesures devraient être prises pour trouver des processus permettant de réduire ces risques, voire mettre au point des solutions de remplacement.

#### **11. Migrations et contrôle aux frontières**

Le contrôle aux frontières est un domaine dans lequel les technologies de sécurité et de surveillance sont largement utilisées. Cette utilisation soulève plusieurs préoccupations ayant trait aux incidences sur les droits de l'homme et au principe de solidarité, tant au niveau mondial qu'entre les États membres. Le GEE recommande d'évaluer les systèmes de contrôles aux frontières au regard des critères définis dans le présent avis, à savoir la dignité et les droits de l'homme, la justice, la nécessité, la proportionnalité, l'efficacité, les solutions de remplacement et l'obligation de rendre des comptes.

Conformément aux conclusions du groupe de travail «Article 29», le GEE craint que le régime d'enregistrement des entrées et des sorties (Entry/Exit System - EES) proposé dans le cadre de l'initiative «Frontières intelligentes» n'entraîne des atteintes disproportionnées à la vie privée des individus. Le programme de Stockholm préconise de limiter l'introduction de nouveaux systèmes aux situations dans lesquelles il est établi que les systèmes existants ne sont pas suffisants; le GEE n'est pas convaincu que ce critère soit rempli dans le cas du programme d'enregistrement des entrées et des sorties et recommande de décréter un moratoire sur l'introduction de l'EES, ce qui permettra, dans l'intervalle, d'évaluer les systèmes existants, comme le système d'information sur les visas, afin de déterminer si les objectifs de l'EES peuvent être atteints de manière proportionnée.

Dans la mesure où les bases de données UE à grande échelle comme le programme d'enregistrement des voyageurs (Registered Travellers Program - RTP) et le programme d'enregistrement des entrées et des sorties (EES) utilisées dans le cadre du contrôle aux frontières peuvent porter atteinte aux droits des ressortissants de l'Union et des pays tiers, dont une proportion non négligeable sont particulièrement vulnérables, il convient que leur mise en œuvre soit soumise à une évaluation rigoureuse sur le plan, notamment, de leur impact sur les droits fondamentaux et de leur conformité au principe de limitation de la finalité.

**III.** Les critères d'évaluation éthiques vont de pair avec les critères d'évaluation juridiques. Ce n'est que si ces deux catégories de critères sont remplies que la

**confiance** peut être (ré)instaurée. C'est pourquoi le GEE préconise l'adoption de diverses mesures destinées plus concrètement à renforcer la confiance des citoyens et à représenter l'intérêt qu'ils ont à retrouver/conservier le contrôle de leurs affaires personnelles. Ces mesures ont notamment trait au contrôle, à la répression, à la dénonciation des abus, à l'information du public, à l'éducation, à la formation et à la recherche.

#### **12. Un dispositif de contrôle digne de confiance**

Le GEE reconnaît que, pour les questions touchant à la sécurité nationale, il n'est pas toujours possible de garantir la transparence des activités de surveillance. La confiance du public n'en constitue pas moins un élément essentiel de la légitimité des actions menées par l'État pour garantir la sécurité. Le GEE préconise que, sans préjudice du contrôle sous l'autorité d'un juge, les États membres mettent en place des mécanismes à cet effet (ou étendent les mécanismes existants) en chargeant un organisme ou une personne disposant de compétences de contrôle, de remplir le rôle de tiers de confiance au nom du public. Ce rôle consisterait notamment à étudier les répercussions de la surveillance publique et privée sur les droits et obligations des citoyens. Dans un souci de transparence et de respect de l'obligation de rendre de comptes, les États membres devraient publier des données agrégées sur le nombre de demandes introduites en vue d'obtenir des compétences de contrôle, sur l'identité des demandeurs et sur les objectifs poursuivis. Les États membres devraient consulter la personne ou l'organisme concernés avant d'introduire des dispositions législatives ayant trait à la surveillance. D'après le GEE, le tiers de confiance jouerait un rôle décisif en sensibilisant le public et en favorisant le débat concernant les risques et les avantages de la surveillance.

#### **13. Contrôle du respect de la réglementation en matière de protection des données**

Le GEE estime que la protection des données prévue par la législation de l'Union est solide, mais qu'elle doit être mise en œuvre au niveau national. Aussi convient-il que les États membres veillent à ce que les autorités chargées de la protection des données jouissent de compétences juridiques suffisantes et disposent de l'expertise technique et des ressources requises pour assurer des niveaux d'application efficaces dans l'ensemble de l'Union.

#### **14. Dénonciation des abus**

Il convient que la Commission européenne et les États membres fassent en sorte qu'un mécanisme efficace et complet de protection des lanceurs d'alerte soit mis en place dans les secteurs public et privé. Conformément aux principes formulés par l'organisation Transparency International dans son rapport de 2013 intitulé «*Whistleblowing in Europe*», il importe que dans les situations touchant à la sécurité

nationale, des réglementations et des procédures concernant les lanceurs d'alerte existent et soient claires, qu'elles garantissent la confidentialité ou l'anonymat, qu'elles permettent la réalisation, en temps voulu, d'une enquête approfondie et indépendante sur les révélations des lanceurs d'alerte, et qu'elles prévoient des mécanismes transparents et contraignants permettant de donner suite en temps voulu aux plaintes des lanceurs d'alerte victimes de représailles. Lorsque les informations divulguées ont trait à des questions touchant à la sécurité nationale, à des secrets officiels ou militaires, ou à des informations classifiées, il convient d'adopter pour leur communication des procédures et des garanties spéciales tenant compte du caractère sensible de la question en cause, de manière à favoriser un suivi et une résolution au niveau interne et à éviter que des informations ne soient inutilement divulguées à l'extérieur. Ces procédures devraient permettre la divulgation interne, la divulgation à un organe de contrôle autonome et indépendant du point de vue institutionnel et opérationnel, du secteur de la sécurité, ou la divulgation à des autorités disposant d'une habilitation de sécurité appropriée. La divulgation externe (c'est-à-dire la divulgation aux médias ou à des organisations de la société civile) serait justifiée en dernier recours.

#### **15. Protection intégrée de la vie privée**

Les organisations publiques et privées devraient adopter, pour la mise au point des technologies de sécurité et de surveillance, des principes de protection de la vie privée par ou dans la conception (privacy by/in design). Les valeurs européennes que sont la dignité, la liberté et la justice doivent être prises en compte avant, pendant et après le processus de conception, de développement et de mise à disposition de ces technologies. Les technologies favorisant la protection de la vie privée devraient être intégrées dès le début du processus, et non rajoutées après la mise en œuvre. Le GEE estime qu'il serait possible, si les ingénieurs, les développeurs et les experts du domaine de la réflexion philosophique et éthique collaboraient dans un cadre interdisciplinaire, de diffuser au sein des organisations une culture dans laquelle le concept de respect de la vie privée serait compris et mis en pratique. L'introduction, dans le cursus des étudiants et des diplômés en ingénierie et en informatique, mais aussi au niveau de l'éducation et de la formation professionnelles, de cours et de formations aussi bien théoriques que pratiques sur les aspects éthiques, pourrait contribuer à une meilleure compréhension des approches fondées sur la protection de la vie privée par ou dans la conception dans le domaine des technologies de sécurité et de surveillance.

#### **16. Comprendre le concept de respect de la vie privée et en apprécier la valeur**

Le respect de la vie privée n'est pas un concept statique, et il faudra, pour adopter des mesures appropriées garantissant la protection de l'intimité physique des individus et des renseignements personnels les concernant, parvenir à mieux comprendre la signification et la valeur que les Européens attachent à ce concept. À cette fin, il convient que l'Union dégage des fonds en vue de la réalisation de travaux de recherche qui permettront d'examiner et d'analyser comment les Européens appréhendent les questions ayant trait à la sécurité et à la surveillance et quel rôle ils entendent jouer dans ce cadre.



**Stellungnahme Nr. 28 der Europäischen Gruppe für Ethik in Naturwissenschaften und  
Neuen Technologien bei der Europäischen Kommission**

## **Ethik der Sicherheits- und Überwachungstechnologien**

*Brüssel, 20 Mai 2014*

*Bezug:* Ersuchen von **Präsident Barroso**

*Berichterstatter:* **Inez de Beaufort, Linda Nielsen, Siobhán O'Sullivan**

*Nur der Originaltext auf Englisch ist authentisch.*





## Empfehlungen

Eine Stellungnahme zu ethischen Implikationen von Sicherheits- und Überwachungstechnologien zu formulieren, wie die EGE gebeten wurde zu verfassen, stellt eine dringliche, aber schwierige Aufgabe. Denn die genannten Technologien haben sehr unterschiedliche Zwecke, werden von unterschiedlichen Akteuren verwendet, bringen verschiedene Stufen und Formen von Gefährdungen der Menschenrechte mit sich und führen zu unterschiedlichen Nutzungsformen.

Die zunehmende Verfügbarkeit von großen Informationsmengen und die steigende Anzahl von Kommunikationsnetzen sind wichtige Faktoren, die die Globalisierung des 20. Jahrhunderts mit sich gebracht hat. Als weitere Merkmale einer globalisierten Welt lassen sich das Unsicherheitsgefühl, mangelndes Vertrauen und eine geringe Risikotoleranz benennen. Schießereien in Schulen, Kinos und Einkaufszentren, Sprengstoffanschläge in U-Bahnen, Zügen und im Luftverkehr, Kindesentführungen, Prügelattacken und Raubüberfälle auf ältere Menschen haben dazu beigetragen, dass unser Unsicherheitsgefühl auch in unserem eigenen Umfeld stärker geworden ist. Auch wenn alle objektiven Beurteilungen zeigen, dass es nie eine Zeit gab, in der das Leben sicherer war als heute, bleibt dieses Unsicherheitsgefühl bestehen. Der Wunsch der Regierungen, auf dieses von den Bürgern wahrgenommene Unsicherheitsgefühl zu reagieren, hat zweifellos zu einer Ausweitung sicherheitspolitischer Maßnahmen in Europa und anderswo geführt.

Sicherheit, im eher engen Wortsinn verwendet, beinhaltet den Schutz vor körperlichen Schäden oder der Androhung von Schaden und ist ein wesentlicher Bestandteil des Wohlbefindens. Im Sinne eines Gesellschaftsvertrages verstanden, haben sich Staaten verpflichtet, im Austausch für das Zugeständnis, die Freiheit des Einzelnen zu beschneiden, für die Sicherheit der Bürger zu sorgen. Dies ist jedoch nur ein Aspekt des Sicherheitsparadigmas. Der Schutz der körperlichen Unversehrtheit ist notwendig, aber nicht ausreichend. Sicherheit muss in einem breiteren Kontext betrachtet werden, der sowohl menschliche als auch gesellschaftliche Sicherheit umfasst. Dies erfordert, dass wir unsere Überlegungen zum Sicherheitsverständnis von der Bedeutung des Staates zu der von Einzelpersonen, Gesellschaftsgruppen und Wirtschaftsunternehmen erweitern. Europa ist eine Wertegemeinschaft, in der wir uns bemühen, Würde, Autonomie, Freiheit und Gerechtigkeit durch Menschenrechte zu schützen. Diese Werte und Güter schaffen ein Umfeld, in dem sich der Einzelne durch Kreativität, Innovation, Entwicklung von starken persönlichen Beziehungen zu anderen und durch den dadurch möglichen Beitrag zur Gesellschaft entfalten kann. Bildung, Gesundheit, Demokratie, Umwelt und Gleichheit sind wesentliche Bausteine eines sicheren Europas.

Ein eher begrenzter Ansatz zur Verwirklichung von Sicherheit, ganz besonders, wenn es um die enge Auslegung dieses Begriffs als Staatssicherheit geht, besteht darin, Kompromisse zu schließen. Das klassische Beispiel dafür ist der Kompromiss zwischen Freiheit, oft als Datenschutz bzw. Privatsphäre bezeichnet, und Sicherheit. Eine ausgewogene Balance zwischen konkurrierenden Prinzipien oder Werten muss hergestellt werden, wenn diese in Konflikt geraten. Es gibt aber einige Grundprinzipien wie die Menschenwürde, die in keinem

Fall geopfert werden dürfen. Dies erfordert, dass wir über die Rhetorik von Kompromissen hinausgehen und eine differenziertere Vorgehensweise anstreben, bei der Sicherheitstechnologien und Maßnahmen auf der Grundlage der Verhältnismäßigkeit und Wirksamkeit geprüft und Rechte priorisiert und nicht geopfert werden.

Die EGE erkennt an, dass die Staatsgewalt in einer demokratischen Gesellschaft in völlig legitimer Weise Behörden und Einrichtungen dazu einsetzt, nach strengen gesetzlichen Vorschriften die Überwachung als Mittel zur Wahrung der Sicherheit ihrer Bürger zu nutzen. Die EGE vertritt auch die Auffassung, dass Geheimhaltung und Diskretion ein wesentlicher Teil der **Würde** des menschlichen Lebens sind. Die Verletzung des Rechts einer Person auf Privatsphäre durch eine Behörde muss **begründet** werden und gerichtlicher Aufsicht unterliegen. Die Überwachung muss **notwendig** und **verhältnismäßig** sein, um eine entsprechende Relation zwischen den ergriffenen Maßnahmen und den erreichten Zielen zu gewährleisten. Ein entscheidendes Kriterium für die Beurteilung der Verhältnismäßigkeit ist die **Wirksamkeit** des jeweiligen Eingriffs. Diese Wirksamkeit muss regelmäßig überprüft werden. Die Befugnis zur Überwachung muss für einen bestimmten Zweck und für einen bestimmten Zeitraum gewährt werden. **Alternativen**, die das gleiche Ziel erreichen können, müssen geprüft und dokumentiert werden, um die am wenigsten eingriffstiefe Methode zu wählen. **Rechenschaftspflicht** ist eine notwendige Voraussetzung für die öffentliche Überwachung. Folglich muss die Überwachung evidenterweise aus angemessenen Gründen und in Übereinstimmung mit öffentlich zugänglichen Verfahrensregeln erfolgen. Sicherheits- und Überwachungstechnologien müssen so **transparent** wie möglich angewendet werden, wobei legitime Ausnahmen ausdrücklich im Rechtssystem bestimmt werden. An der Überwachung beteiligte private oder gewerbliche Organisationen sind ebenfalls an die oben genannten Kriterien gebunden.

Vor diesem Hintergrund gibt die drohende Diskriminierungsgefahr Grund zur Sorge. Denn wir müssen uns über die möglichen unerwarteten Auswirkungen der allgegenwärtigen Überwachung bewusst sein. Sie zwingt den Einzelnen dazu, sich mit entsprechenden Formen der Normalität (verstanden als implizite Normativität) abzufinden, sich folglich anders zu verhalten und diese Norm weiter zu verstärken, was wiederum zu einer verarmten - wenn nicht sogar steril gemachten - Gesellschaft führt (in der Vielfalt, Kreativität und sogar Zusammenhalt ausgemerzt wurden). Die Diskriminierung kann abzielen auf die Überwachung bestimmter Minderheiten, und die EGE fordert Abhilfemaßnahmen, wenn es in den EU-Mitgliedstaaten zu solchen Fällen kommt. Weiterhin kann Diskriminierung Profiling und Stigmatisierung betreffen. Es muss anerkannt werden, dass Profiling vielfältige Formen annehmen kann, von Programmen, bei denen man sich selbst für die Teilnahme entscheiden kann (wie das Global-Entry-Programm), bis hin zu „Facecrime“ und Gesichtserkennung (sowie anderen biometrischen Systemen) und zur Erstellung von Persönlichkeitsprofilen aller Bürger durch Massenüberwachung. Stigmatisierung (und ihre Entsprechung, die Demütigung) müssen selbstverständlich vermieden werden, doch die Rolle, die die zunehmend allgemeine Verwendung der Algorithmen als Teil der Ansammlung von Sicherheits- und Überwachungsdaten spielt, ist in dieser Hinsicht besonders alarmierend. Diese Algorithmen können die ethische Reflexion und Rechtfertigung von Entscheidungen verschleiern oder für sich einnehmen, was zu „In-built-Profiling“ oder „Stigmatisierung by Design“ führt. Dabei riskiert man auch die Perfektionierung der Normalität und Compliance, auf die oben hingewiesen wurde, durch unübersichtliche Auswahlprozesse, damit menschliches Eingreifen und Verstehen ferngehalten wird. Die EGE ist sich in dieser

Hinsicht der Gefahr der Instrumentalisierung von Ethikräten und verwandten Einrichtungen bei diesen Prozessen der Normalisierung in Bezug auf neue Technologien vollständig bewusst. Ebenfalls ist sich die EGE der Schwierigkeiten in Gänze bewusst, die darin liegen, die Sicherheits- und Überwachungstechnologien aus ethischer Sicht zu betrachten, ohne dass dies als eine Form des stillschweigenden Duldens verstanden wird. Die EGE ist entschlossen, diese Schwierigkeiten nicht zu scheuen, sondern sie in dieser Stellungnahme direkt anzugehen.

Basierend auf den skizzierten Überlegungen, ist die EGE in den folgenden Empfehlungen auf dem Gebiet der Sicherheits- und Überwachungstechnologien übereingekommen:

I. Technologien, die möglicherweise die Privatsphäre von Personen verletzen könnten, die ihrerseits nicht die Möglichkeit haben, ihr Einverständnis zu erklären (oder die ihre Ablehnung nicht kundtun können), erfordern eine spezifische Rechtfertigung. Die EGE fordert jeweils Begründungen für jeden Einzelfall dieser Maßnahmen.

**1. Rechenschaftspflicht**

Die Mitgliedstaaten müssen sicherstellen, dass Personen oder Einrichtungen, die berechtigt sind, die Privatsphäre der Bürger zu überwachen, im öffentlichen Interesse handeln und Rechenschaft über ihr Handeln ablegen. Wenn der Staat Sicherheits- und/oder Überwachungsaufgaben an private Unternehmen delegiert, sind diese an die gleichen rechtlichen und ethischen Verpflichtungsstandards gebunden. Die Mitgliedstaaten müssen gewährleisten, dass die Einhaltung dieser Verpflichtungen überwacht wird.

**2. Gerichtliche Kontrolle**

Die Mitgliedstaaten müssen über ein System der gerichtlichen Kontrolle von behördlichen Überwachungsmaßnahmen bei strafrechtlichen Ermittlungen verfügen. Der Einzelne muss nachträglich informiert werden, dass er überwacht wurde, vorausgesetzt, dass dadurch die Ermittlung nicht beeinträchtigt wird. Der Einzelne muss die Möglichkeit haben, auf dem Gerichtsweg Entschädigung zu beantragen, wenn er Objekt einer rechtswidrigen Überwachung wurde.

**3. Entwicklung eines gemeinsamen Verständnisses von nationaler Sicherheit**

*Die in der Charta der Grundrechte verankerten gemeinsamen europäischen Werte stellen den normativen Rahmen dar, auf dem ein gemeinsames ethisches Verständnis von nationaler Sicherheit aufgebaut werden kann.*

**a)** Es wird anerkannt, dass nationale Sicherheit legitim im Zentrum der jeweiligen nationalen Interessen steht und in die Zuständigkeit der Mitgliedstaaten fällt. Die EGE empfiehlt jedoch, dass die EU-Organe in Zusammenarbeit mit den Mitgliedstaaten auf ein gemeinsames Verständnis nationaler Sicherheit hinwirken.

**b)** Die EGE empfiehlt auch, dass die Mitgliedstaaten Verfahren etablieren, um andere Mitgliedstaaten entsprechend über nachrichtendienstliche Tätigkeiten außerhalb ihres

Hoheitsgebiets zu informieren, um das Vertrauen zwischen den Partnern zu bewahren.

c) Die Mitgliedstaaten dürfen nicht im Namen der nationalen Sicherheit andere Mitgliedstaaten überwachen, um kommerzielle Vorteile zu erzielen, weil ein solches Verhalten im Widerspruch zum Ziel der EU steht, einen einheitlichen europäischen Markt zu schaffen.

#### **4. Drohnen**

*Die rasante Entwicklung und der vermehrte Einsatz von Drohnen in militärischen, zivilen und wirtschaftlichen Zusammenhängen durch die Mitgliedstaaten wurden nicht von den notwendigen Entscheidungsstrukturen und Kontrollregelungen begleitet. Diese sind derzeit bestenfalls fragmentarisch. Der EU fehlt ein umfassender Rechtsrahmen für die Entwicklung, den Erwerb, den Einsatz und den Export von Drohnen für den zivilen und wirtschaftlichen Einsatz. Die EGE begrüßt die bereits von der Europäischen Kommission getroffenen Maßnahmen hinsichtlich der Integration ferngesteuerter Luftfahrzeuge (Remotely Piloted Aircraft Systems, RPAS) in das EU-Luftverkehrssystem (einschließlich umfassende Konsultation und Veröffentlichung eines Fahrplans). Es verdient Anerkennung, dass dabei von Anfang an die Betrachtung der gesellschaftlichen Auswirkungen des Drohneneinsatzes einbezogen wurden.*

a) Angesichts des jüngsten Engagements der EU für eine verbesserte Koordinierung zwischen den Mitgliedstaaten bei der Entwicklung und Beschaffung von Drohnen empfiehlt die EGE, dass diese Zusammenarbeit auf die Erarbeitung gemeinsamer Normen und rechtlicher Rahmenbedingungen für die zivile und kommerzielle Nutzung von Drohnen in der EU ausgedehnt wird. Besonderes Augenmerk muss auf eine Bewertung der bestehenden EU-Datenschutzregelungen gerichtet werden, um beurteilen zu können, ob die derzeitigen Rechtsvorschriften im Hinblick auf die Integration ferngesteuerter Luftfahrzeuge (Remotely Piloted Aircraft Systems, RPAS) in den europäischen Luftraum ihren Zweck erfüllen.

b) Die Mitgliedstaaten müssen dafür sorgen, dass die nationale Politik in Bezug auf den Einsatz von Drohnen im Inland (d.h. innerhalb der jeweiligen nationalen Grenzen), im öffentlichen Raum, nicht die Menschenrechte der Personen verletzen, die von den Drohneneinsätzen betroffen sind. Die Nutzung von Drohnen auf dem eigenen Staatsgebiet muss einer Zulassung und geeigneten Aufsicht unterliegen, um die Sicherheit zu gewährleisten und Missbrauch zu verhindern. Außerdem müssen Personen, die Genehmigungen für den Einsatz von Aufklärungsdrohnen beantragen, nachweisen, dass die beabsichtigte Nutzung gerechtfertigt, notwendig und verhältnismäßig ist. Die EGE empfiehlt auch, dass die Regelungen und Verfahren für den inländischen Einsatz von Drohnen zum Überwachungszwecke im Interesse der Transparenz, die wiederum eine Voraussetzung für das Vertrauen der Öffentlichkeit bildet, öffentlich zugänglich sein müssen.

c) Die EGE lenkt die Aufmerksamkeit auf die gravierenden ethischen Auswirkungen der militärischen Nutzung von Drohnen sowie der automatisierten Kriegsführung und

begrüßt die Entschlieung des Europischen Parlaments zum Einsatz von bewaffneten Drohnen vom 25. Februar 2014. Die EGE fordert mehr Transparenz und Rechenschaftspflicht auf Seiten derjenigen Mitgliedstaaten, die Drohnen fr militrische Zwecke einsetzen. Zu diesem Zweck mssen die Mitgliedstaaten die rechtliche Grundlage, den Umfang und Grenzen aller tdlichen Drohnenangriffe offenlegen und es muss eine Untersuchung stattfinden, dass die fr traditionelle bewaffnete Konflikte geltenden rechtlichen Rahmenregeln nicht verletzt werden. Informationen ber die Anzahl von Zivilisten und Nicht-Zivilisten, die bei Drohnenangriffen gettet werden, sollten ebenfalls ffentlich zugnglich gemacht werden. Ferner befrwortet die EGE ausdrcklich Untersuchungen, um die ethischen Implikationen der tdlichen Drohnenangriffe und deren Kompatibilitt oder anderweitige Aspekte mit der Theorie des gerechten Krieges zu prfen. Darber hinaus sind Studien zur Rolle des moralischen Handels erforderlich, wenn Drohnen ferngesteuert betrieben werden. Dasselbe gilt auch fr die Entwicklung von Drohnen mit Selbststeuerung.

II. In Bezug auf berwachungstechnologien muss die Beweislast bei den Staaten und/oder Unternehmen liegen, die *ffentlich und transparent* Nachweise erbringen mssen, bevor Sie berwachungsaktionen durchfhren,

- dass diese **notwendig** sind,
- dass diese **wirksam** sind,
- dass diese **verhltnismig** sind (z. B. durch Angabe der Zweckbindung),
- dass es keine besseren **Alternativen** gibt, die diese berwachungstechnologien ersetzen knnten.

Die Einhaltung dieser Kriterien ist einer **nachtrglichen Beurteilung** zu unterziehen. Dies muss entweder auf der Ebene der normalen politischen Analysen oder durch die diesbezglichen Regelungen der Mitgliedstaaten geschehen.

Auerdem ist zu beachten:

**Rechenschaftspflicht** bedeutet, dass alle Menschen das Recht haben, ber berwachungstechnologien informiert zu werden – auch wenn diese Information in einigen Fllen erst nachtrglich zur Verfgung gestellt wird.

**Transparenz** ber die wirtschaftlichen Interessen muss jederzeit gewhrleistet werden.

## 5. Personenbezogene Daten

Die EGE betont, dass Zweckbindung hinsichtlich der personenbezogenen Daten eine Standardnorm fr ffentliche wie private Organisationen zu sein hat. Personenbezogene Daten sollten nur fr einen spezifischen und rechtmigen Zweck gesammelt werden. So weit wie mglich sollten Daten anonymisiert und die Verschlsselung strker genutzt werden, um sowohl den Datenschutz als auch die Sicherheit zu erhhen. Standardmige Datenfreigabe ist zu vermeiden und Nutzer sollten die Mglichkeit haben (z. B. durch den Zugang zu Datenschutzeinstellungen),

Informationen, die Organisationen über sie besitzen, zu kontrollieren und zu berichtigen. Das Profiling von Personen für kommerzielle Zwecke soll der ausdrücklichen Zustimmung der Betroffenen unterliegen. Informationen von kommerziellen Unternehmen sollten im Hinblick darauf zur Verfügung stehen, wofür Daten gesammelt werden, von wem, zu welchem Zweck, wie lange und ob die Daten die gesammelt werden, mit anderen Datenquellen verknüpft werden.

#### **6. Das öffentliche Bewusstsein für Datenrichtlinien**

Die EGE bekräftigt ihre Auffassung, dass die Öffentlichkeit besser darüber aufgeklärt werden muss, wofür, wie, warum und zu welchem Zweck personenbezogene Daten verarbeitet, weitergegeben und geschützt werden. Behörden und Unternehmen müssen ihre Regelungen in diesem Zusammenhang öffentlich zugänglich machen. Die EU und die Mitgliedstaaten sollen sich bemühen, die Öffentlichkeit über die Folgen der Verwendung von Sicherheits- und Überwachungstechnologien für den Einzelnen und die Gesellschaft aufzuklären, das Bewusstsein für diese Problematik zu schärfen und die Debatte zu diesem Thema zu fördern. Aufklärungsprogramme müssen bereits in der Schule beginnen und Informationen und Instrumente für die Bürger bereitstellen, damit diese ihre Daten in der digitalen Umwelt schützen können.

#### **7. Big Data**

Die EGE hat festgestellt, dass mehr und mehr dazu übergegangen wird, große Datenmengen, sogenannte „Big Data“, zu sammeln und miteinander in Beziehung zu setzen. Während die EGE den potenziellen Wert solcher Datensätze anerkennt, sind wir besorgt, dass ohne angemessene Sorgfalt im Umgang mit diesen Daten der Grundsatz der Zweckbindung als Mittelpunkt des Datenschutzes untergraben wird. So fordert die EGE Behörden und private Organisationen dringend auf, aussagekräftige ethische Untersuchungen anzustellen, um ihr Handeln mit den gemeinsamen europäischen Werten der Würde, Privatsphäre und Autonomie zu durchdringen und in Einklang zu bringen. Die EGE empfiehlt, dass die EU einen Verhaltenskodex für die Big-Data-Analyse entwickelt, der Unternehmen bei diesem Prozess unterstützen würde.

#### **8. Algorithmen**

Im Kontext der Sicherheits- und Überwachungstechnik muss beachtet werden, dass Algorithmen in ihrer Konstruktion notwendigerweise selektiv sind und von den Menschen, die sie programmieren, beeinflusst werden können. Algorithmen und ihren Parametern liegen ethische Annahmen zugrunde, die obligatorisch explizit gemacht werden sollten. Außerdem sind Algorithmen nicht unfehlbar und die generierten Daten hängen von der Auswahl und Qualität der Dateneingabe ab, die nach Ansicht der EGE ständig geprüft und validiert werden sollte. Darüber hinaus sollte die Aufklärung über die ethischen Aspekte bei der Gestaltung von Algorithmen in die Ausbildung von Entwicklern aufgenommen werden.

#### **9. Datenschutz im Bereich der elektronischen Kommunikation (e-Privacy)**

Die EGE empfiehlt der Kommission, in Erwägung zu ziehen, die E-Privacy-Richtlinie zu überarbeiten, die derzeit den Rechtsrahmen für den Umgang mit elektronischer

Kommunikation darstellt. Angesichts des rapiden Anstiegens der Zahl der digitalen Schnittstellen seit der Einführung der Richtlinie hält es die EGE für angemessen, dass Produkte, die VoIP – Voice over Internet Protocol, IP-Kommunikation oder Breitbandkommunikation – verwenden, und auch private Unternehmensnetze in den Geltungsbereich einer überarbeiteten Richtlinie einbezogen werden.

#### **10. Datenschutz-Folgenabschätzung**

Die Mitgliedstaaten müssen in ihre Prüfungs- und Regulierungstätigkeit Verfahren zur Datenschutz-Folgenabschätzung einbeziehen, wenn neue oder geänderte Informationssysteme, die personenbezogene Daten verarbeiten, auf den Markt kommen. Die Bewertung muss die möglichen Auswirkungen der vorgeschlagenen Technologie für personenbezogene Daten berücksichtigen. Werden Risiken ermittelt, müssen Maßnahmen ergriffen werden, um Prozesse zur Senkung dieser Risiken zu identifizieren oder Alternativen zu dem zu finden, was vorgeschlagen wird.

#### **11. Migration und Grenzkontrolle**

Grenzkontrollen sind ein Bereich, in dem Sicherheits- und Überwachungstechnologien sehr verbreitet sind. Dies wirft sowohl global als auch in den EU-Mitgliedstaaten einige Bedenken hinsichtlich der Auswirkungen auf die Menschenrechte und das Solidaritätsprinzip auf. Die EGE empfiehlt, die Grenzkontrollsysteme im Hinblick auf die in dieser Stellungnahme aufgestellten Kriterien, nämlich Menschenwürde und Menschenrechte, Gerechtigkeit, Notwendigkeit, Verhältnismäßigkeit, Wirksamkeit, Alternativen und Rechenschaftspflicht zu beurteilen.

Im Einklang mit den Ergebnissen der Artikel-29-Arbeitsgruppe ist die EGE besorgt, dass das Einreise-/Ausreisensystem (Entry-Exit-System – EES), das im Rahmen der Grenzinitiative „Smart Borders“ vorgeschlagen wird, einen unverhältnismäßigen Eingriff in die individuelle Privatsphäre darstellt. Laut dem Stockholmer Programm sollten neue Systeme nur dann entwickelt werden, wenn festgestellt wird, dass die bestehenden Systeme nicht ausreichen. Die EGE ist nicht davon überzeugt, dass dieses Kriterium beim Einreise-/Ausreisensystem erfüllt ist, und empfiehlt ein Moratorium für die Einführung des EES, während bestehende Systeme wie das Visa-Informationssystem ausgewertet werden, um zu prüfen, ob die Ziele der EES in angemessener Weise erfüllt werden können.

Da EU-Großdatenbanken, wie das Registrierungsprogramm für Reisende (RTP) und das Einreise-/Ausreisensystem (EES), das für Grenzkontrollzwecke verwendet wird, die Rechte von EU- und Nicht-EU-Bürgern in Gefahr bringen, von denen ein Teil besonders gefährdet ist, muss die Einführung solcher Datenbanken einer strengen Bewertung unter besonderer Berücksichtigung ihrer Auswirkungen auf die Grundrechte und die Einhaltung des Grundsatzes der Zweckbindung unterzogen werden.

III. Ethische und rechtliche Bewertungskriterien gehen Hand in Hand. **Vertrauen** kann nur durch ein Zusammenwirken beider Typen von Kriterien (wieder) aufgebaut

werden. Daher empfiehlt die EGE verschiedene Maßnahmen, um konkreter Vertrauen aufzubauen und die Interessen der Bürger an der Kontrolle über ihre persönlichen Angelegenheiten zu wahren. Diese Maßnahmen fallen in die Bereiche Aufsicht, Durchsetzung, Whistleblowing, Information der Öffentlichkeit, Bildung, Ausbildung und Forschung.

#### **12. Vertrauenswürdige Aufsicht**

Die EGE erkennt an, dass es in Fragen der nationalen Sicherheit nicht immer möglich ist, mit Blick auf Überwachungsmaßnahmen transparent zu sein. Dennoch ist das Vertrauen der Öffentlichkeit von entscheidender Bedeutung für die Legitimität staatlicher Sicherheitsmaßnahmen. Zu diesem Zweck empfiehlt die EGE, dass unbeschadet jeglicher gerichtlicher Aufsicht die Mitgliedstaaten eine Stelle oder Person mit Aufsichtsbefugnis einrichten oder die Aufgaben bestehender Gremien erweitern, damit eine vertrauenswürdige dritte Partei zur Verfügung steht, die im Namen der Öffentlichkeit handeln kann. Eine solche Stelle würde auch die Auswirkungen der öffentlichen und privaten Überwachung auf die Rechte und Pflichten der Bürger beobachten. Aggregierte Informationen über die Anzahl der Anträge auf Überwachungsbefugnisse, unabhängig von wem und zu welchem Zweck diese eingereicht wurden, müssen von den Mitgliedstaaten veröffentlicht werden, damit Transparenz und Rechenschaftspflicht gewährleistet sind. Die Mitgliedstaaten sollten eine solche Stelle oder Person im Vorfeld der Einführung von Rechtsvorschriften auf dem Gebiet der Überwachung konsultieren. Die EGE rechnet damit, dass eine solche vertrauenswürdige dritte Partei eine wichtige Rolle bei der Sensibilisierung der Öffentlichkeit und der Anregung von Debatten über Risiken und Nutzen der Überwachung spielt.

#### **13. Durchsetzung des Datenschutzes**

Die EGE ist der Ansicht, dass der im EU-Recht verankerte Datenschutz robust ist, aber auf nationaler Ebene durchgesetzt werden muss. Die Mitgliedstaaten müssen daher sicherstellen, dass die Datenschutzbehörden über ausreichende rechtliche Befugnisse, technisches Know-how und Ressourcen, verfügen, um eine effektive Rechtsdurchsetzung in der gesamten Europäischen Union zu gewährleisten.

#### **14. Whistleblowing**

Die Europäische Kommission und die Mitgliedstaaten müssen sicherstellen, dass ein effektiver und umfassender Schutzmechanismus für Whistleblower (Hinweisgeber bzw. Informanten) im öffentlichen wie im privaten Sektor etabliert wird. Im Einklang mit den Grundsätzen von Transparency International, wie im Bericht von 2013 über „*Whistleblowing in Europa*“ angegeben ist, muss es Vorschriften und Verfahren für Fälle geben, in denen es um die nationale Sicherheit geht, und diese müssen klar



sein. Die Vertraulichkeit oder Anonymität muss gewährleistet sein und es muss für gründliche, zeitnahe und unabhängige Untersuchungen der Angaben von Informanten gesorgt werden. Außerdem muss es transparente, durchsetzbare und zeitnahe Mechanismen geben, um rechtzeitig eine Beschwerde eines Informanten wegen etwaiger Vergeltungsmaßnahmen zu verfolgen. Wenn eine Offenlegung Fragen der nationalen Sicherheit, Amts- oder Militärgeheimnisse oder Verschlussachen betrifft, sind spezielle Verfahren und Garantien für die Berichterstattung einzuführen, die die Sensibilität der Thematik berücksichtigen, um erfolgreich eine interne Verfolgung zu erreichen und eine unnötige externe Exposition zu verhindern. Diese Verfahren sollten eine interne Offenlegung, die Weitergabe an ein autonomes Aufsichtsgremium, das institutionell und operativ unabhängig vom Sicherheitssektor ist, oder die Weitergabe an Behörden mit der entsprechenden Sicherheitsüberprüfung vorsehen. Externe Weitergabe (das heißt, an die Medien und Organisationen der Zivilgesellschaft) würde als letztes Mittel gerechtfertigt werden.

#### **15. Planung von Datenschutz**

Behörden und private Unternehmen müssen Planungsprinzipien für den „Datenschutz durch die Entwicklung“ (privacy by design) und den „Datenschutz in der Entwicklung“ (privacy in design) von Sicherheits- und Überwachungstechnologien verabschieden. Die europäischen Werte Würde, Freiheit und Gerechtigkeit müssen vor, während und nach der Gestaltung, Entwicklung und Bereitstellung solcher Technologien berücksichtigt werden. Datenschutzfreundliche Technologien müssen von Anfang an integriert werden, es reicht nicht aus, auf eine spätere Implementierung zu verweisen. Nach Ansicht der EGE ist es möglich, durch die interdisziplinäre Zusammenarbeit von Ingenieuren, Entwicklern und philosophischen und ethischen Experten eine Organisationskultur zu schaffen, in der der Datenschutz verankert ist und in der die gängige Praxis reflektiert wird. Kurse und Schulungen zu ethischen Aspekten auf theoretischer und praktischer Ebene sowohl für Studenten und Hochschulabsolventen in den Fachbereichen Ingenieurwissenschaften und Informatik als auch in der beruflichen Bildung könnten die Berücksichtigung von Datenschutzaspekten bei der Entwicklung von Sicherheits- und Überwachungstechnologien verbessern.

#### **16. Das Verständnis für die Privatsphäre und ihre Wertschätzung**

Privatsphäre und Datenschutz sind kein statischen Konzepte, und ein vollständigeres Verständnis darüber, wie europäische Bürger diese Aspekte verstehen und bewerten, ist unbedingt erforderlich, wenn geeignete Maßnahmen ergriffen werden sollen, um die informationelle Selbstbestimmung und den Datenschutz sicherzustellen. Zu diesem Zweck muss die EU Mittel für die Forschung zur Verfügung stellen, um zu untersuchen und zu analysieren, wie Bürgerinnen und Bürger ihre Mitwirkung in Fragen der Sicherheit und Überwachung sehen und pflegen.



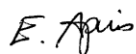
## The European Group on Ethics in Science and New Technologies



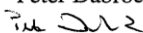
The Chairperson: Julian Kinderlerer

The members:

Emmanuel Agius



Peter Dabrock



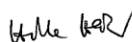
Inez de Beaufort



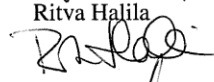
Andrzej Gorski



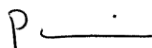
Hille Haker



Ritva Halila



Paula Martinho da Silva



Linda Nielsen



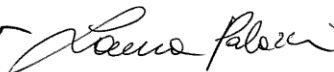
Herman Nys



Siobhán O'Sullivan



Laura Palazzani



Pere Puigdomenech



Marie-Jo Thiel



Günter Virt





## EGE Secretariat

### Address

European Commission

Berl 8/362 - B-1049 Brussels

Fax : (32-2) 299 45 65

Email: [BEPA-ETHICS-GROUP@ec.europa.eu](mailto:BEPA-ETHICS-GROUP@ec.europa.eu)



Jim DRATWA  
European Commission  
Member, Bureau of European Policy Advisers  
Secretary-General of the IDB  
Head of the EGE Secretariat  
Berl 8/358 B-1049 Brussels  
Tel : (32-2) 29 58253  
E-mail: [jim.dratwa@ec.europa.eu](mailto:jim.dratwa@ec.europa.eu)



Joanna PARKIN  
European Commission  
Policy Officer, Bureau of European Policy Advisers  
EGE Secretariat  
Berl 8/362 B-1049 Brussels  
Tel: (32-2) 29 54262  
E-mail: [joanna.parkin@ec.europa.eu](mailto:joanna.parkin@ec.europa.eu)



Kim Hoang LE  
European Commission  
EGE Secretariat  
Berl 8/362 B-1049 Brussels  
Tel: (32-2) 29 99228  
Email: [kim-hoang.le@ec.europa.eu](mailto:kim-hoang.le@ec.europa.eu)



Adriana Sorina OLTEAN  
European Commission  
EGE Secretariat  
Berl 8/362 B-1049 Brussels  
Tel: (32-2) 29 93016  
Email: [adriana-sorina.oltean@ec.europa.eu](mailto:adriana-sorina.oltean@ec.europa.eu)

### Website:

[http://ec.europa.eu/european\\_group\\_ethics/index\\_en.htm](http://ec.europa.eu/european_group_ethics/index_en.htm)