



European
Commission



Opinion No. 26

Ethics of Information and Communication Technologies

Brussels, 22 February 2012





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

Ethics of information and communication technologies

Brussels, 22 February 2012

Maurizio SALVI
Chief Editor
Head of the EGE Secretariat

26
Opinion No



***Europe Direct is a service to help you find answers
to your questions about the European Union.***

**Freephone number (*):
00 800 6 7 8 9 10 11**

(*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

More information on the European Union is available on the Internet (<http://europa.eu>).

Cataloguing data can be found at the end of this publication.

Luxembourg: Publications Office of the European Union, 2012

© European Union, 2012

Reproduction is authorised provided the source is acknowledged.

ISBN 978-92-79-22734-9

doi:10.2796/13541

Printed in Luxembourg

PRINTED ON ELEMENTAL CHLORINE-FREE BLEACHED PAPER (ECF)

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

Ethics of information and communication technologies

No 26

22/02/2012

Reference: Request from President Barroso

Rapporteurs: Julian Kinderlerer, Peter Dabrock, Hille Haker, Herman Nys

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 7 (Respect for private and family life), Article 8 (Protection of personal data), Article 14 (Right to education), Article 29 (Right of access to placement services), Article 34 (Social security and social assistance), Article 35 (Health care), Article 36 (Access to services of general economic interest), Article 41 (Right to good administration) and Article 42 (Right of access to documents) thereof,¹

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',

Having regard to the Council of Europe Convention on Human Rights and Biomedicine, signed on 4 April 1997 in Oviedo,²

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 services³ (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 facilities⁴ (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 services⁵ (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 services⁶ (Universal Service Directive),

¹ Official Journal C 364 of 18 November 2000, pp. 1 – 22.

² <http://conventions.coe.int/treaty/en/treaties/html/164.htm>.

³ OJ L 108, 24.4.2002.

⁴ OJ L 108, 24.4.2002.

⁵ OJ L 108, 24.4.2002.

⁶ OJ L 108, 24.4.2002.

Having regard to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector⁷ (Directive on privacy and electronic communications),

Having regard to Regulation (EC) No 717/2007 of the European Parliament and of the Council of 27 June 2007 on roaming on public mobile communications networks within the Community⁸,

Having regard to Commission Decision 2002/627/EC of 29 July 2002 establishing the European Regulators Group for Electronic Communications Networks and Services⁹ to advise and assist the Commission in the development of the internal market and, more generally, to provide an interface between national regulatory authorities (NRAs) and the Commission,

Having regard to the Radio Spectrum Policy Group established under Commission Decision 2002/622/EC of 26 July 2002¹⁰,

Having regard to the Contact Committee established under Directive 97/36/EC of the European Parliament and of the Council of 30 June 1997 amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities¹¹,

Having regard to Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC),

Having regard to Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws,

Having regard to Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services,

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 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, and in particular Article 41(2) thereof,

⁷ OJ L 201, 31.7.2002.

⁸ OJ L 171, 29.6.2007.

⁹ OJ L 200, 30.7.2002.

¹⁰ OJ L 198, 27.7.2002.

¹¹ OJ L 202, 30.7.1997.

Having regard to Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity¹²,

Having regard to Decision No 676/2002/EC of the European Parliament and of the Council of 7 March 2002 on a regulatory framework for radio spectrum policy in the European Community¹³ (Radio Spectrum Decision),

Having regard to the Internet of Things (IoT) strategic research roadmap¹⁴,

Having regard to Commission Decision 2002/622/EC of 26 July 2002 establishing a Radio Spectrum Policy Group¹⁵,

Having regard to Recommendation CM/Rec (2010) 13 of the Committee of Ministers to the member states of the Council of Europe on the protection of individuals with regard to automatic processing of personal data in the context of profiling,

Having regard to Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency¹⁶,

Having regard to the Commission Recommendation of 11 February 2003 on relevant product and service markets within the electronic communications sector susceptible to *ex-ante* regulation in accordance with Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services¹⁷,

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 in criminal matters,

Having regard to the 2009 EU telecoms reform package for stronger consumer rights, an open Internet, a single European telecoms market and a high-speed Internet connection for all citizens¹⁸,

Having regard to the Commission decisions on the adequacy of the protection of personal data in third countries based on Article 25(6) of Directive 95/46/EC to assess whether a third country ensures an adequate level of protection by reason of its domestic law or the international commitments it has entered into¹⁹,

Having regard to the Eurobarometer report 'Attitudes on Data Protection and Electronic Identity in the European Union' (June 2011)²⁰,

Having regard to the new strategy adopted by the European Commission on corporate social responsibility (CSR) from 25 October 2011²¹,

¹² OJ L 91, 7.4.1999.

¹³ OJ L 108, 24.4.2002.

¹⁴ http://www.internet-of-things-research.eu/pdf/loT_Cluster_Strategic_Research_Agenda_2011.pdf

¹⁵ OJ L 198, 27.7.2002.

¹⁶ OJ L 77, 13.3.2004.

¹⁷ OJ L 114, 8.5.2003.

¹⁸ <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/568>

¹⁹ http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

²⁰ http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

²¹ http://ec.europa.eu/enterprise/policies/sustainable-business/files/csr/new-csr/act_en.pdf

Having regard to a number of thematic reports²² on data protection governance including: the Report on the Economic Evaluation of Data Protection Directive 95/46/EC (Final Report prepared by Rambøll Management for the European Commission); the IPTS (Institute for Prospective Technological Studies) Report - Issue 67 of September 2002 on Identity and Privacy; the results of the two Eurobarometer surveys on data protection awareness in the European Union carried out in autumn 2003; the first report on the implementation of the data protection directive (95/46/EC); the Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE) on Security and Privacy for the Citizen in the Post-September 11 Digital Age - A Prospective Overview; the implementation of Directive 95/46/EC to the Processing of Sound and Image Data, British Institute of International and Comparative Law; the IPTS Report to the European Parliament Committee on Industry, External Trade, Research and Energy (ITRE) on Future Bottlenecks in the Information Society; and the Commission study entitled: ' "Junk" e-mail costs Internet users EUR10 billion a year worldwide',

Having regard to the Resolutions of the European Parliament of 1 December 2005 and 4 April 2006 concerning the Doha Round and the WTO Ministerial Conferences, where the Parliament calls for basic public services, such as audio-visual services, to be excluded from liberalisation under the GATT negotiations.

Having regard to the Resolution of the European Parliament of 27 April 2006 on the proposal of a Council decision on the conclusion of the UNESCO Convention on the Protection and Promotion of the Diversity of Cultural Expressions, which states in particular that 'cultural activities, goods and services have both an economic and a cultural nature, because they convey identities, values and meanings, and must therefore not be treated as solely having commercial value',

Having regard to the Council Decision²³ of 18 May 2006 on the conclusion of the Convention on the Protection and Promotion of the Diversity of Cultural Expressions approved by the UNESCO Convention on behalf of the Community, the Convention entering into force on 18 March 2007,

Having regard to the Commission Communication on the future of European regulatory audio-visual policy²⁴,

Having regard to Decision 2004/68/JHA of the Council of the European Union of 22 December 2003 on combating the sexual exploitation of children and child pornography²⁵,

Having regard to the Commission communication 'i2010: European Information Society'²⁶,

Having regard to the Madrid Resolution on international standards for the protection of personal data and privacy adopted by the International Conference of Data Protection and Privacy Commissioners on 5 November 2011,

Having regard to the Granada Ministerial Declaration on the European Digital Agenda, agreed on 19 April 2010²⁷,

Having regard to the Commission communication 'Digital Agenda for Europe'²⁸ (26/08/2010),

²² http://ec.europa.eu/justice/data-protection/document/studies/index_en.htm.

²³ OJ L 201 of 25.7.2006.

²⁴ The future of European regulatory audio-visual policy — COM(2003) 784, 15.12.2003.

²⁵ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004F0068:EN:HTML>

²⁶ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005DC0229:EN:NOT>.

²⁷ http://www.eu2010.es/export/sites/presidencia/comun/descargas/Ministerios/en_declaracion_granada.pdf.

²⁸ [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245R\(01\):EN:NOT](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245R(01):EN:NOT).

Having regard to Europe's Digital Competitiveness report, 2010 drafted by the European Commission²⁹ 17/05/2010,

Having regard to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data³⁰ (ETS No 108), which was opened for signature on 28 January 1981 (allowing the European Communities to accede) and adopted by the Committee of Ministers of the Council of Europe on 15 June 1999,

Having regard to the revision of the EU data protection law (which will be adopted in co-decision by the European Parliament and Council from 25 January 2012³¹),

Having regard to the Communication entitled 'A comprehensive approach to personal data protection in the European Union'³²,

Having regard to the Council of Europe 'Additional protocol to Convention 108 regarding supervisory authorities and transborder data flows'³³ (ETS No 181),

Having regard to the Universal Declaration on the Human Genome and Human Rights adopted by UNESCO on 11 November 1997,³⁴ the Declaration on Human Genetic Data adopted by UNESCO on 16 October 2003 and the Universal Declaration on Bioethics and Human Rights adopted by UNESCO on 19 October 2005,

Having regard to the hearings of experts and Commission departments by the EGE during their meetings in March 2011, April 2011, May 2011, June 2011, September 2011, October 2011, November 2011 and December 2011³⁵,

Having regard to the EGE General report of Activities 2005-2010³⁶,

Having regard to EGE Opinion No 20 – 16/03/2005 — on Ethical aspects of ICT Implants in the Human Body³⁷,

Having regard to EGE Opinion No 13 – 30/07/1999 — on Ethical issues of healthcare in the information society³⁸,

Having regard to the roundtable organised by the EGE on 15 November 2011 in Brussels,

Having regard to the contributions from the EGE open consultation on ethics and ICT,

Having heard the EGE Rapporteurs, Julian Kinderlerer, Peter Dabrock, Hille Haker and Herman Nys,

Hereby adopts the following Opinion:

²⁹ http://ec.europa.eu/information_society/digital-agenda/documents/edcr.pdf.

³⁰ http://www.coe.int/t/dghl/standardsetting/DataProtection/convention_en.asp.

³¹ http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

³² Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 'A comprehensive approach on personal data protection in the European Union', 4 November 2010, COM (2010) 609 final, 2

³³ http://www.coe.int/t/dghl/standardsetting/DataProtection/convention_en.asp.

³⁴ http://portal.unesco.org/shs/en/ev.php-URL_ID=2228&URL_DO=DO_TOPIC&URL_SECTION=201.html.

³⁵ See agendas on the EGE website: http://europa.eu.int/comm/european_group_ethics/index_en.htm.

³⁶ http://ec.europa.eu/bepa/european-group-ethics/docs/gar_ege_2005-2010_web.pdf.

³⁷ http://ec.europa.eu/bepa/european-group-ethics/docs/avis20_en.pdf.

³⁸ http://ec.europa.eu/bepa/european-group-ethics/docs/avis13_en.pdf.

TABLE OF CONTENTS

14	Scope of the Opinion
15	1. Scientific Aspects
15	1.1 Introduction
15	1.1.1 Age of Hardware
16	1.1.2 Initial Use of Computers
17	1.1.3 The Personal Computer Revolution
18	1.1.4 Internet
19	1.1.5 Age of Software
19	1.2 The Current Use of the Internet
20	1.2.1 Data mining
20	1.2.2 Cloud Computing
21	1.2.3 Internet of Things
22	1.2.4 Social Networks
23	1.3 The Future Internet
24	1.4 Mobile Devices
25	2. Regulatory Frameworks and Policy Frameworks
25	2.1 Internet Governance: International Bodies
25	2.1.1 The United Nations Internet Governance Forum
26	2.1.2 UNESCO: Code of Conduct for the Information Society
26	2.1.3 Organisation for Economic Cooperation and Development
26	2.1.4 Council of Europe
26	2.1.5 Internet Corporation for Assigned Names and Numbers (ICANN)
27	2.2 European Union Policy Regarding ICT
27	2.2.1 The Digital Agenda for Europe (DAE).
27	2.2.2 E-Government
28	2.2.3 E-Commerce
30	2.2.4 Corporate Social Responsibility
30	2.2.5 Interoperability and Standards
30	2.2.6 Very Fast Internet
31	2.2.7 E-Skills
31	2.2.8 E-Advertising

31	2.2.9	Cybercrime
32	2.2.10	Digital Divide
32	2.2.11	Net Neutrality
33	2.2.12	Internet of Things
33	2.2.13	E-Health
34	2.3	Current EU Regulatory Frameworks for Personal Data Protection
36	2.4	Gaps or Deficits in Regulations and Policies
37	3.	Ethical Aspects
37	3.1	Challenges to the Concept of Identity
37	3.1.1	Introduction
38	3.1.2	The Digital Identity
38	3.1.3	The Concept of Personal Identity in the Digital Era
42	3.1.4	Individual Identity and Social Identity in ICT.
42	3.1.5	The Concept of Moral Identity in ICT Domains
44	3.2	Privacy as a Fundamental Right
45	3.2.1	Concerns Regarding the Current EU Legal Protection of Personal Data
45	3.2.2	Safety of Personal Data
46	3.2.3	Profiling and Data Mining
46	3.2.4	Sensitive Data
46	3.2.5	Giving and Withdrawing Consent
47	3.2.6	Transparency
47	3.2.6.1	Mandatory Breach Notification
47	3.2.6.2	Managing One's own Data
48	3.2.7	Right to Data Deletion
48	3.2.8	Special Protection for Minors
49	4.	Sphere of Social Implications, Culture, Education and Environmental Protection
49	4.1	Social Inclusion in the Age of ICT
51	4.2	E-Government
51	4.3	Education
51	4.3.1	Culture
52	4.4	E-Health
52	4.5	E-environment

55	4.6	Political Dimension
56	4.7	E-Commerce
57	4.7.1	Data Mining
57	4.7.2	Internet of Things (IoT)
58	4.7.3	E-advertising
58	4.8	Conclusions
59	5.	Recommendations
59	5.1	The Ethical Framework of the Opinion
60	5.2	Right of Access to ICT
60	5.3	Recommendations Concerning Individual Identity
61	5.4	The Right to Privacy and Protection of Data
62	5.5	Social Aspects: Digital divide
62	5.5.1	Digital Divide
63	5.5.2	Work-Life Balance
63	5.6	Political participation
63	5.7	Recommendations Concerning the Sphere of Commerce
63	5.7.1	Commercial Transactions
64	5.7.2	Corporate Social Responsibility
64	5.8	Cross-Correlative Data Mining
64	5.9	Environment and Raw Materials
65	5.10	Concluding Recommendation
69	6.	ANNEX 1
79	7.	ANNEX 2



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

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

Ethics of information and communication technologies

Reference: Request from **President Barroso**

Rapporteurs: **Julian Kinderlerer, Peter Dabrock,
Hille Haker, Herman Nys;**

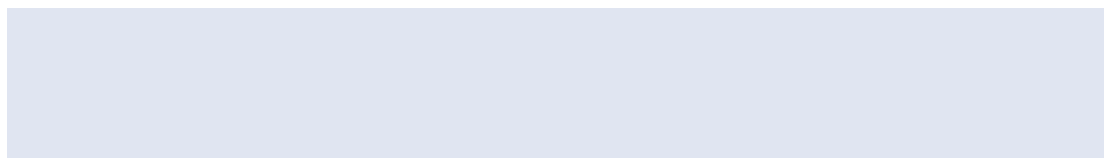
Maurizio SALVI

Chief Editor

Head of the EGE Secretariat

26

Opinion No



Scope of the Opinion

Every day more than 250 million Europeans connect to the Internet, to work, learn, communicate, play and socialise. But the digital economy, which has grown rapidly around all those activities, poses new challenges to governments and regulators. Business models are likely to change significantly as Internet access allows consumers to compare goods and prices and to shop across borders. Work and play will also change dramatically, as personal interactions continue to change from word of mouth and personal meetings to include interactions unlimited by place or time. Communication and mechanisms for interacting with others have already changed beyond recognition, and this will almost certainly continue at an accelerating pace. The digital revolution has and will impact on everything people do, from their life choices to their health, their shopping, their education and the way they communicate. Most importantly, national and regional boundaries are becoming, and will continue to become, blurred as a result of the speed and accessibility of new technologies.

According to the Digital Agenda,³⁹ fragmented markets currently hinder European digital commerce. The lack of interoperability between national systems also acts as a brake on the development of commerce. Rising levels of crime create significant problems in providing European citizens with a reliable and safe digital environment that engenders trust. Ideas for mechanisms to improve the use of technology across the European Union are addressed. The Agenda also recognises that '[T]oday, under EU law, citizens in the EU enjoy a series of rights that are relevant to the digital environment, such as freedom of expression and information, protection of personal data and privacy, requirements for transparency and universal telephone and functional Internet services and a minimum quality of service'. In addition to the impact on commerce, there is a very considerable impact on the manner in which we live our lives. Technology is likely to impinge on us in both positive and negative ways. The Digital Agenda for Europe (DAE) emphasises that this should be built into the various technologies as they become available.

The impact of the new technologies is so far-reaching that it is impossible to address the vast range of issues that are encompassed within the scope of information and communication technologies. In accepting the request the EGE decided to focus on Internet technologies. As the EGE will be examining security issues arising from ICT in a subsequent opinion, it will not address them in this document. There will be similarities in the ethical issues arising from the use of ICT in health, government, education, agriculture and commerce as they impact on society and individuals. The EGE will therefore deal with the ethical problems in general, using examples to highlight issues within particular domains. ICT in the home and in the interaction of individuals is as important as the Internet, and the implications are just as far-reaching. This Opinion should provide suggestions for an ethically sound use of ICT.

The EGE has decided not to address issues related to IPR and ICT even though it is aware of the controversy related to the ongoing and future negotiations of the Anti-Counterfeiting Trade Agreement.

On 21 March 2011 President José Manuel Barroso asked the EGE to draft an Opinion on the ethical issues arising from the rapid expansion of information and communication technologies (ICT). President Barroso indicated that the Opinion could 'offer a reference point to the Commission to promote a responsible use of the Digital Agenda for Europe and facilitate the societal acceptance of such an important policy item.

The EGE is aware of the changes that have come about in the lives of most citizens of the European Union, and further afield, as a result of the pervasiveness of new electronic media. The challenge is to ensure that the availability of electronic information and the use of ICT are handled in an ethical manner.

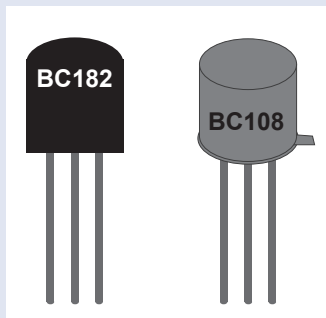
³⁹ [http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245R\(01\):EN:NOT](http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245R(01):EN:NOT).

PART A: STATE OF THE ART: SCIENCE, REGULATION AND POLICIES

1. Scientific Aspects

1.1 Introduction

The science of information and communication technologies has changed very drastically over the last 70 years. The invention of the transistor in 1947 was to herald a revolution in consumer electronics that was unimaginable in previous times. For most of the first half of the 20th century thermionic valves enabled radio and radar communication. The development of computing equipment relied on a very large number of transistors. It was miniaturisation that led to the massive change in availability of electronic devices, and hence in people's expectations.



As a solid-state device, the transistor was small, used relatively little power (and hence heat) and was the basis for the microprocessor, integrated circuit and memory storage devices. Whereas the

valves used in the original computing systems measured several tens of cubic centimetres, even the original transistors were orders of magnitude smaller. Current microprocessors contain millions of transistors on a tiny area of silicon.⁴⁰ Heat is a problem only because of the number of individual structures on the die used for creating integrated circuits. Today the most advanced circuits contain several hundred millions components on an area no larger than a fingernail. The transistors on these chips measure about 90 nm, you could fit hundreds of these transistors inside a red blood cell.

1.1.1 Age of Hardware

Although computers were initially developed during the First World War, the personal computer did not become available until the 1980s. In less than 30 years, computers have changed from number-crunching, data-analysing machines to being primarily communication tools

which are essential to our lives. The first computers were impossible to imagine as personal devices. The Harvard Mark I, designed by Aiken and Hopper in 1944, was approximately 15 metres long and 3 metres tall, weighing some 5 tonnes. It contained 7600.00 separate pieces and was in use until 1959!⁴¹ It was capable of addition, subtraction and multiplication and it could store some results. Data was stored and counted mechanically using 3000 decimal storage wheels, 1400 rotary dial switches and 500 miles of wire. Its electromagnetic relays classified the machine as a relay computer. All output was displayed on an electric typewriter. By today's standards, the Mark I was slow, requiring 3-5 seconds for a multiplication operation.

The computer on the Apollo missions that placed men on the moon had 2000 bytes of memory. It ran at 1 MHz and had a total of 32 Kilobits of storage. Today, a mobile



telephone carried in a pocket may have more than 32 gigabytes of memory and run at over 1 GHz. Programming has become complex and depends on an operating system (IOS, Windows 7 or Android, for example) Programming today involves the interaction of code produced by many individuals and teams. There is no longer a linear sequence of instructions and programs are unlikely to be understood in full by any individual. Originally, programmers wrote very basic (or low-level) calls to a micro-coded 'hard-wired' system. Today, operation is dependent on very sophisticated software routines that run the computer — the operating system. In the early 1970s computer languages were developed that provided an interface between the ordinary user and the computer. UNIX, for example, was developed

⁴⁰ http://upload.wikimedia.org/wikipedia/commons/thumb/0/00/Transistor_Count_and_Moore%27s_Law_-_2011.svg/2000px-Transistor_Count_and_Moore%27s_Law_-_2011.svg.png.

⁴¹ <http://inventors.about.com/library/weekly/aa052198.htm>.

as a toolbox of routines that could be strung together to provide required functionality.⁴²

Computing started off with the storage and analysis of information. Nothing was inter-connected. Mechanisms were required for providing the computers with two input types. Firstly, the programmes that defined what were to be done with the data. Initially, this was a series of sequential instructions with a mechanism for jumping to a different sequence of instructions based on tests performed on the data. [This has become more sophisticated, relying on sequences of instructions based on actions (e.g. the position of a mouse, or a mouse click, or input coming from somewhere else)]. The second source of information was the data to be analysed using these instructions. The two sorts of information were kept separate. Mechanisms for the output of results were also required. Punched cards (Hollerith cards initially) and punched tape were the first to be used and were read at a relatively high speed by the computers.

Magnetic tape and magnetic discs followed rapidly during the latter part of the 20th century. In the 1960s teletypewriters were used which provided a coded form of information (for either control or data) directly to the memory of the computer, there was no contact with other machines or other users.

Primary data storage, often referred to as memory, is the system that makes data directly available to the computer itself. Computers had some memory dedicated to the system as well as some memory dedicated to the user(s). The system memory consisted of both the memory in which programs and data were held and the registers used by the computer in which to perform the basic operations specified by a program, or linear sequences of instructions. User memory was often separated into (at least) two segments — one that contained the program and one that contained the data to be addressed and modified by the program. From the early 1950's this was some form of magnetic memory that could be accessed randomly, as required. Initially these were magnetic cores whose magnetic states were altered by the passage of an electric charge. They were replaced by semi-conductor memory in about 1975. The earliest personal computers (circa 1975-1980) had as little as 16 kilobytes of semi-conductor memory. Today's home computers have up to 64 gigabytes (4 million times as large) and even mobile phones are likely

to have 16 gigabytes or more built in. In 1980 a computer memory board with about 32 kilobytes cost about \$ 3000, which was a significant sum. Memory was very expensive, if relatively fast.

Slower bulk memory was needed for storing large amounts of data. If necessary, programs could be paged in and out of the faster memory. Initially, magnetic drums were used, followed by floppy disks that could hold up to 360 Kbytes of data, and then by floppy disks capable of storing 1.4 megabytes of data. Storage media in the form of USB sticks and solid-state memory are relatively recent. The main memory for long-term storage remains hard disk drives. They tend to be relatively slow but can store large amounts of data in an easily accessible manner. All these are organised into file systems that allow for logical storage of the data and the metadata that provides information such as ownership, amount of data, date and time of creation and of last use, etc.

It is both the size of such memory systems and the speed of access that have turned computers into information and communication devices. The real advances that have made computers ubiquitous are, on the one hand, the software to search through data and allow rapid and effective access in real time and, on the other, mechanisms to access the data and provide it in a readable form for the user.

1.1.2 Initial Use of Computers

Initially, computers were used on their own to analyse scientific data. In the office, word-processors, less powerful than those found today, but with similarities to the typewriters they replaced, except that editing was possible slowly became ubiquitous. Initially the data was stored on removable diskettes and did not even include spell-checkers. As the first word processors did not provide a WYSIWYG interface (what you see is what you get), the final output depended on the available printers and they were, in some ways, more difficult to use than typewriters, for codes had to be included in the 'copy' to indicate formatting (bold, italic, justification etc). Spreadsheets quickly replaced numeric calculators, making the job of those working with figures significantly easier than it had been. The days of laboriously adding up long columns of figures were numbered once personal calculators, and then computers, appeared on the scene. While the concept of spreadsheets had been used for centuries, and similar calculation programs existed before, the computerised spreadsheet was probably invented in about 1978 by Dan Bricklin and Bob Frankston.

⁴² <http://www.bell-labs.com/history/unix/>.

It was called VisiCalc and was designed for use on an Apple personal computer.

The first computer users were primarily scientists, who had to do a great deal of their own programming. Computer languages (either interpreted or compiled) were invented to make this possible. Interpreted languages were translated at the time of use into code that could be implemented by the computer. This had to be done each time the programme was used. Compilers took the code produced by the programmer and translated it into code that could then be used by the computer.

Languages like BASIC were interpreted; Fortran, Algol, Lisp, C, C++ and Java were compiled. Operating systems, which provide routines that can be accessed by user programmes for particular purposes were 'invented'.

With the advent of systems like UNIX, an Application Programme Interface (API) was developed that allowed programmes to talk to systems which sat between the basic machine and the program produced for a particular task. The API is the definition of that which is implemented in a library of machine-specific routines that can then be used by those programming without needing to take account of the machine on which the program is running.

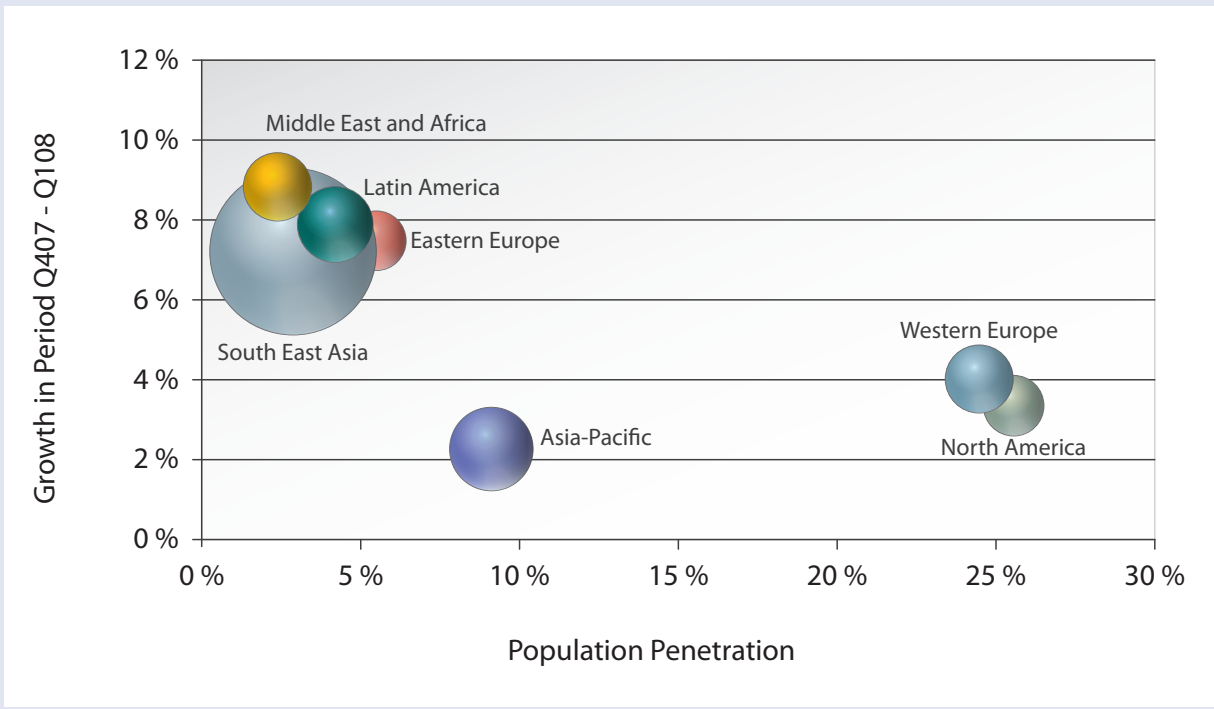
The availability of memory is a major factor in the ubiquity of computer devices. As has been indicated,

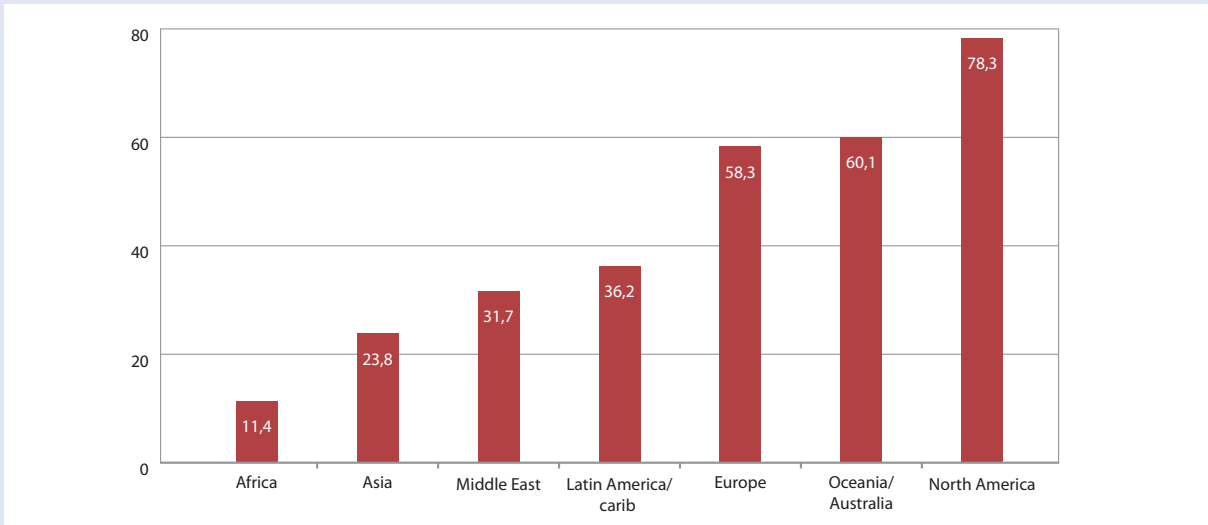
in the early years of computing memory devices were extremely limited. This has clearly changed, to the extent that random access memory costs about € 4 per gigabyte. This is the 'fast' memory used within the computer which enables a range of activities to be undertaken. Random-access memory (RAM) is made up of integrated circuits that allow stored data to be accessed in any order. As RAM is usually volatile, stored information is lost if the power is removed. Slower memory, either in the form of semi-conductors or some kind of magnetic disk, is used to retain data over a long period.

1.1.3 The Personal Computer Revolution

In 1980 it was estimated that less than 5 million computers were in use worldwide. Today it is estimated that by 2015 there will be more than 2 billion. In 2010 there were over 5 billion mobile phones, which are themselves computers, in use (for a world population of approximately 7 billion). The penetration (% of population using computers) and quarterly growth of computers in 2008 is indicated below.

By 2011, the picture had changed very significantly, with major penetration growth in emerging and even developing countries. The runaway lead in computer technology enjoyed by the United States and Europe is no longer as great as it was. The graph below indicates penetration — that is, the percentage of the population in each of the regions that has access to ICT.





The situation had also changed markedly in character. Whereas initially personal computers had been stand-alone devices, having little contact with the outside world, they had become machines with a great deal of ‘intelligence’ but, more significantly, they were now connected to the outside world and to each other. The major parameters were no longer the speed and memory size associated with the machine, but rather its connectivity and ability to interact.

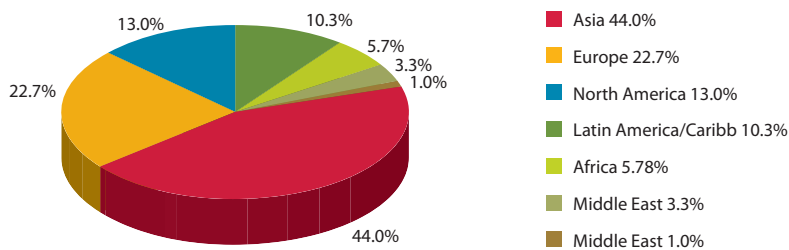
1.1.4 Internet

Towards the end of the last century mechanisms (protocols) were developed for machine-to-machine interaction. In 1982 the Internet Protocol Suite (TCP/IP) was standardised and the concept of a world-wide network of fully interconnected TCP/IP networks called the Internet was introduced. The Internet was commercialised in 1995.

One of the most important issues that had to be addressed before this whole system could take off was speed. If the speed of transmission of information had remained at the speed at which typing is possible, none of the changes to our lives that we have witnessed could have happened. Computers which contained the critical elements of conditional response — ‘do x if y’ — and larger memory, could carry out numerical calculation and, in general, many symbol-manipulation tasks. Computer technology has undergone profound changes in every decade since the 1940s, in terms of both the hardware and the programs which make the system usable (and ‘user- friendly’).

Computers deal with at least three streams: the set of instructions that identify what must be done with any data presented to the system; the data that is presented; and the instructions that identify how to interact with other computers or humans.

Internet Users in the World
Distribution by World Regions - 2011



Source: Internet world stats - www.internetworldstats.com/stats.htm
Basis: 2,095,006,005 Internet users on March 31, 2011
Copyright© 2011, Miniwatts Marketing Group

1.1.5 Age of Software

The mid 1990s saw a large increase in the use of the Internet and its impact on our lives. The development of computer operating systems that provided an easy-to-use interface, such as MSDOS (developed by Microsoft) followed by graphical user interfaces enabled the general public to use computers in ways that initially had not been available. Word-processing packages have had an enormous impact on communication, making simple cross-cultural communication possible, for example. Once WYSIWYG⁴³ interfaces became available, word-processing software was in use everywhere. Companies like Microsoft provided the means to kick-start a revolution in the way people communicate. E-mail had begun in the early 1980s and may have led to the development of the Internet.

The World Wide Web is now part of our culture. It was developed by Tim Berners Lee in 1989 at CERN as a 'Hypertext project' called 'WorldWideWeb' as a 'web' of 'hypertext documents'. It involved a simple system for hypertext documents written in English, where angular brackets (< and >) separated the text itself from the instructions to the computer as to the manner in which the text was to be displayed. Initially the web related to the text that was to be sent from one computer to another. 'Content is king' was a popular slogan. The simplicity of the hypertext mark-up language meant that the system was accessible even over slow Internet lines. The system has changed slightly. The latest versions of the language (HTML5 for example) allow for much more in the way of web applications than those which were initially developed.

Web pages used to be simple, with a single page defining both the information and instructions to the browser (displaying the information in a single file). When Amazon's Chief Executive Officer, Bezos, introduced their new e-book readers in December 2011, he noted that most modern web pages, such as Amazon's own or that of CNN, are sophisticated creations, with multiple photos, animations, and complex scripts and mark-up code. The CNN home page, for instance, is built by the browser from about 53 static images, 39 dynamic images, three Flash files, 30 JavaScript files from seven different domains, 29 HTML files and seven CSS (Cascading Style Sheet) files.' (28 September 2011).

⁴³ What you see is what you get.

It is estimated that in 1993 the Internet carried only 1 % of the information flowing through two-way telecommunication. By 2000 this figure had grown to 51 %, and by 2007 more than 97 % of all telecommunicated information was carried over the Internet.

The graphical user interface had a major influence on the accessibility of the computer by the general public. It is generally understood that it provides some form of graphical display of what there is to do, along with a pointing device enabling the user to point to and choose a particular operation to be performed.

The availability of large amounts of memory and the development of algorithms that enable effective searching and cross-correlating large amounts of data have changed our world completely. It is estimated that there are 2 billion people using the Internet today, which is approximately one third of the population.⁴⁴ The use of portable mobile devices has further increased the magnitude of this phenomenon.⁴⁵ Over 2 billion people worldwide will own at least one smartphone by 2015⁴⁶ and in the EU the number of mobile phone subscribers was around 650 million in 2010.

1.2 The Current Use of the Internet

The way the Internet is used today is very different from what was originally designed. The first form of the Internet was called Web 1.0 and consisted of static pages. The consumer was merely a receiver and user of content dictated and created by someone else, the producer. The producer normally had the technical know-how as a programmer and software developer. The second and current state (dating from 2010) is referred to as Web 2.0.

The distinction between the producer and consumer of content has now disappeared. Thanks to new applications, any user can create content on the Internet

⁴⁴ Figure quoted by William Echikson, Google, during the round table organised for this Opinion.

⁴⁵ A mobile device is a small, hand-held computing device, typically having a display screen with touch input and/or a miniature keyboard and weighing less than 0.91 kg. Early pocket sized ones were joined in the late 2000s by larger but otherwise similar tablet computers. As in a personal digital assistant (PDA), the input and output are often combined into a touch-screen interface. In telecommunications, 4G is the fourth generation of cellular wireless standards. It is a successor to the 3G and 2G families of standards.

⁴⁶ <http://www.parksassociates.com/blog/article/parks-pr2011-smartphones>.

without needing to know any programming languages. 'The Internet provides people with the ability to leap borders, to disregard convention and to engage in unprecedented debate on everything from movies to monarchy. Blogs, social networks and online video platforms are now widely available for everyone with access to the Internet'.⁴⁷ Nonetheless, there are marked differences in the speed of access, depending on the part of the world where it is being used. This may prevent people living in developing countries from accessing information or using computer systems as effectively as people living in North America or Western Europe. Netcraft's May 2011 survey reported that there were approximately 325 million websites online compared to 623 websites on New Year's Day 1994.⁴⁸ Researchers at the University of California Berkeley have estimated that around 5 exabytes of data were created during 2002 across all storage forms (print, film, magnetic, optical). Now, in 2011 — less than a decade later — International Data Cooperation (IDC) estimates that more than 5 exabytes⁴⁹ are recorded online every day.

1.2.1 Data mining

Data mining is the process of discovering new patterns from multiple, large data sets involving methods at the intersection of artificial intelligence, machine learning, statistics and database systems. The goal of data mining is to extract knowledge from a data set in a structure which humans can understand. It involves database and data management, data pre-processing, model and inference considerations, 'interestingness metrics', complexity considerations, post-processing of found structure, visualisation and online updating. The dramatic growth of powerful computing and communication technologies enables vast amounts of personal information to be collected, stored and used more easily and effectively than ever before. Such information is generated, knowingly or unknowingly, by individuals going about their daily activities: withdrawing money from a cash machine, website browsing and online purchasing, using loyalty cards or even making a mobile telephone call.⁵⁰ Techniques such as data mining enable

large amounts of personal data from disparate sources to be organised and analysed, thereby facilitating the discovery of previously unknown relationships among the data. A variety of methods, such as probability, information and graph theory as well as artificial intelligence, database techniques and classification algorithms, are employed to discover interesting patterns in the data.⁵¹

Data mining may be of real significance when databases collected from many sources are analysed together to provide information that is not contained in the individual databases. Linking shopping data collected through store cards with bank data and/or health data, for example, provides insights into an individual's habits which may not have been immediately obvious.

1.2.2 Cloud Computing

Cloud computing provides computation, software, data access, and storage services that do not require the end-user to know the physical location and configuration of the system that delivers the services. Cloud computing providers deliver applications via the Internet that are accessed from web browsers and from desktop and mobile apps, while the business software and data are stored on servers at a remote location.⁵² Cloud computing is founded on the broad concept of infrastructure convergence and shared services. Most cloud-computing infrastructure consists of services delivered through shared data-centres and appearing as a single point of access for consumers' computing needs.



⁴⁷ *ibid.*

⁴⁸ *ibid.*

⁴⁹ an exabyte is 218 bytes or, 152 921 504 606 846 976 bytes.

⁵⁰ Information and Privacy Commissioner, Ontario. Data Mining: Staking a Claim on your Privacy 1998 <http://www.ipc.on.ca/images/resources/datamine.pdf>, accessed 10 January 2012.

⁵¹ Fayyad UM. *IEEE Expert* 1996;11(5):20-25.

⁵² In some cases, applications are stored locally and delivered via screen-sharing technology, while the computing resources are consolidated at a remote data centre location; in other cases, entire business applications have been coded using web-based technologies such as AJAX where the program and data are stored remotely.

Cloud computing has developed since the 1960s and since the availability of a significant bandwidth permitting rapid transfer of data between computers in the 1990s. From a user point of view, cloud computing means that users can access their files, data, programs and other services via the Internet that are hosted by other service providers. Control and responsibility for what is stored in the cloud may, however, rest either with the cloud provider or the user, and the physical location of the data may result in problems relating to jurisdiction.

1.2.3 Internet of Things

The Internet of things (IoT) is an integral part of Future Internet, encompassing existing and evolving Internet and network developments. It could be defined as a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities, use intelligent interfaces, and are seamlessly integrated into the information network. In the IoT, 'smart things/objects' are expected to become active participants in business, information and social processes. There they are enabled to interact and communicate among themselves and with the environment by exchanging data and information 'sensed' about the environment, while reacting autonomously to events in the 'real/physical world' and influencing it by running processes that trigger actions and create services with or without direct human intervention. Services will be able to interact with these 'smart things/objects' using standard interfaces that will provide the necessary link via the Internet, to query and change their state and to retrieve any information associated with them, taking security and privacy issues into account.

According to the European Commission, the Internet of things means: 'Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts.'⁵³ One important aspect of future Internet is that the Internet will extend outside traditional computer devices so that any objects in the environment can be connected to it.⁵⁴ The

network becomes more powerful when intelligence can be embedded in things and processing power can be distributed more widely in the network.

The Internet of things (IoT) is usually identified as having started in 1999 when the Auto-ID Centre was established at the Massachusetts Institute of Technology (MIT).

Interacting with other machines has become at least as important as interacting with people or other computers. 'The Internet of things is about interacting with the objects around us, including static non-intelligent objects, and augmenting such interactions with context as provided by geo-location, time etc. Even non-powered devices can be brought into the Internet of things via a handset or a smartphone serving as a gateway to the Internet. In the case of machine-to-machine communication (M2M), this involves communicating with machines such as energy-meters or sensors or even your refrigerator via IP over wireless or wire.'⁵⁵ The devices do not even have to be intelligent or powered. Near-field communication (NFC) is based on very short-range radio communication technology and NFC-enabled handsets are being introduced into the market.

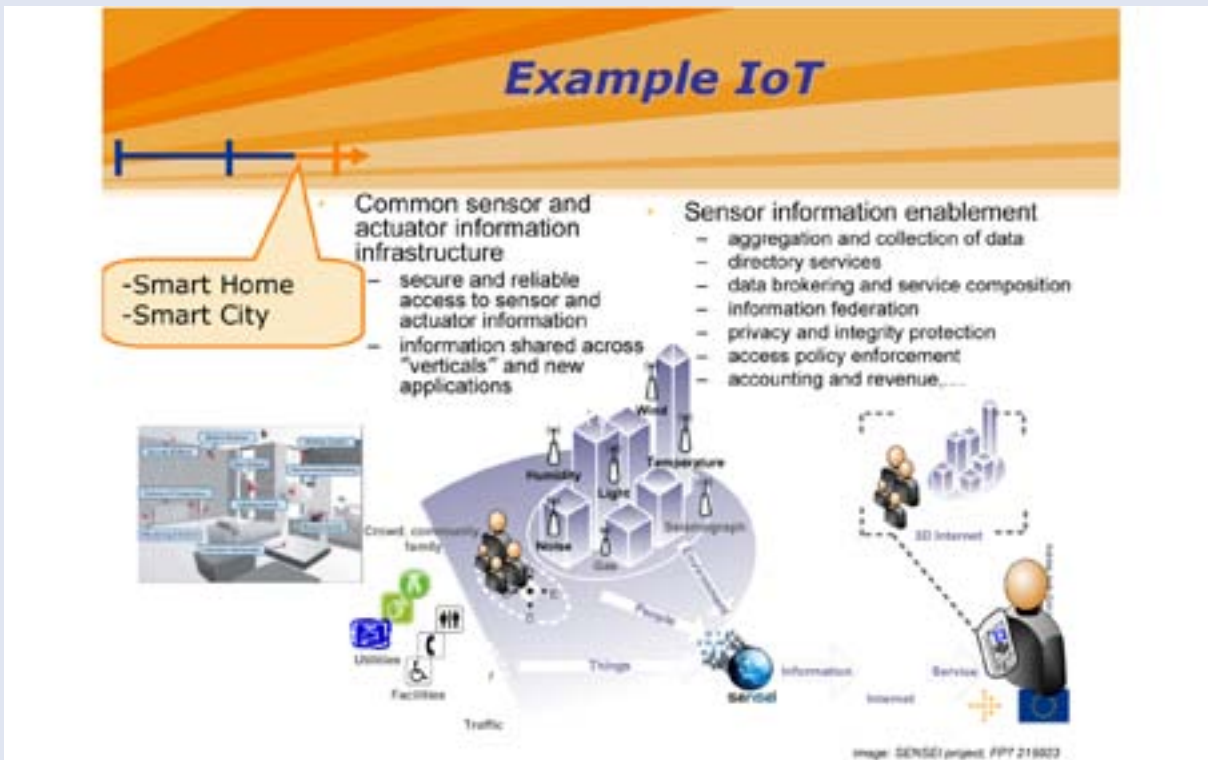
RFID (radio-frequency identification systems) tags are simple. They are able to cause a response in the form of a unique number from a (possibly) non-powered tag which, via computers, can then be associated with an individual or an individual object to which the tag is attached. The reader can be several metres away from the tag and not necessarily in line of sight. Tags are now being used everywhere, from the identification and sorting of luggage at airports to charging for toll roads or for biometric surveillance for security purpose. RFID data can be read through the human body, clothing and non-metallic materials. RFID tags used with entry systems allow access to specific buildings and allow data concerning the tagged persons or objects to be recorded when passing a reader device. The Internet of things is considered to be an innovative ICT sector. It may be used in the home environment, or even in smart health monitoring devices, but there are implications in that it can (and is) used to track individuals' movements.

⁵³ http://ec.europa.eu/information_society/policy/rfid/documents/iotprague2009.pdf.

⁵⁴ Data about things is collected and processed with very small computers (mostly Radio Frequency Identifier Devices – RFID- tags) that are connected to more powerful computers

through networks. Sensor technologies are used to detect changes in the physical environment of things, which further benefits data collection.

⁵⁵ <http://weblog.cenriqueortiz.com/Internetofthings/2010/08/02/m2m-vs-Internet-of-things/>.



1.2.4 Social Networks

A social networking service is an online service, platform, or site that focuses on building social networks or social relations among people with shared interests or activities. Most social network services are web based and provide means for users to interact over the Internet, such as through e-mail and instant messaging. Online community services are sometimes considered as a social network, albeit in a broader sense. A social network service usually means an individual-centred service, whereas online community services are group-centred. In the late 1990s, user profiles became a central feature of social networking sites, allowing users to compile lists of 'friends' and search for other users with similar interests. By the end of the 1990s new social networking methods had been developed and many sites began to develop more advanced features for users to find and manage friends.⁵⁶ This newer generation of social

networking sites began to flourish with the emergence of SixDegrees.com in 1997, followed by Makeoutclub in 2000 and Friendster in 2002, soon becoming part of the Internet mainstream. Friendster was followed by MySpace and LinkedIn a year later, as well as Bebo.

The main social networking services are those which contain category places (such as former school year or classmates), means to connect with friends (usually with self-description pages) and a recommendation system linked to trust. Popular methods now combine many of these features: Facebook and Twitter are used extensively worldwide; Nexopia (mostly in Canada); Bebo, VKontakte, Hi5, Hyves (mostly in The Netherlands), Draugiem. lv (mostly in Latvia), StudiVZ (mostly in Germany), iWiW (mostly in Hungary), Tuenti (mostly in Spain), Nasza-Klasa (mostly in Poland), Decayenne, Tagged, XING, Badoo and Skyrock in parts of Europe; Orkut and Hi5 in South America and Central America; and Mixi, MultiPLY, Orkut, Wretch, renren and Cyworld in Asia and the Pacific Islands. LinkedIn and Orkut are very popular in India.

⁵⁶ Efforts to support social networks via computer-mediated communication were made in many early online services, including Usenet, ARPANET, LISTSERV and bulletin board services (BBS). Many prototypical features of social networking sites were also present in online services such as America Online, Prodigy, and CompuServe. Early social networking on the World Wide Web began in the form of generalised online communities such as Theglobe.com (1995), Geocities (1994) and Tripod.com (1995).

The use of social networks is massive; the magnitude of this phenomenon is clearly illustrated by the 2011 data relating to Facebook. With over 500 million users, Facebook is now used by 1 in every 13 people on earth. Over 250 million of them (over 50 %) log in every day. Over 700 billion minutes a month are spent on Facebook, 20 million applications are installed per day and

over 250 million people interact with Facebook from outside the official website on a monthly basis, across 2 million websites. Over 200 million people access Facebook via their mobile phone; 48 % of young people say they now get their news through Facebook. In the space of just 20 minutes, over 1 million links are shared on Facebook, 2 million friend requests are accepted and almost 3 million messages are sent.⁵⁷

1.3 The Future Internet

The Future Internet (sometimes referred to as Web 3.0) is a term describing all the research and development activities concerning the Internet. A concept that distinguishes FI from the current Internet is Semantic Web. The World Wide Web Consortium (W3C) defines Semantic Web as a Web of data. The original Internet was designed as a web of documents but the amount of information in the networks has grown so much that better ways of retrieving and combining it are needed. The information can be integrated from various different sources and types of data and the type of the relationships between the pieces of data are defined to enable

better and automatic interchange. In many respects, information has never been so free. There are more ways to spread more ideas to more people than at any moment in history. And even in authoritarian countries, information networks are helping people discover new facts and making governments more accountable.⁵⁸

Perhaps the most important change is that information on the Internet is readily searchable. 'In fact, the potential of search and retrieval of information has long been a driving factor in digital publishing, as, indeed, it has been a major rationale for the Internet itself. We have come to take search and retrieval of information for granted, and publishers may overlook this very important aspect of digital titles. While it may be merely an occasional convenience to see when last a particular character had appeared in the course of reading, say, a murder mystery, for many types of publishing, the significant improvement in the speed and accuracy of finding particular information is a big deal.'⁵⁹

Cognitive networks will also contribute to making a more 'intelligent' Internet. They perceive current

Parameters of evolution	1. Smooth trip	2. Going Green	3. Commercial Big Brother	4. Power to the people
Internet infrastructure	Based on current architectural principles	Real-time, data driven, mesh, cloud services	Vertically integrated	Ad hoc/mesh, data/user driven
Technological developments	Mobility based No change in archit. Principles Interoperability	Sensors Distributed network control	Streaming requires NGN or 'clean slate Walled gardens, specialized nets	Distributed control Online Reputation, Viral adoption Generalized wiki
Security, Privacy and Control	Security from competing private efforts Tradeoffs with anonymity	Sensitive to privacy, data protection	Strong Security, either real or apparent Power to data collectors	Privacy and identity more important than security
Economic models	As varied as possible. Work process evolution. Government and business support.	Natural resources consumption. May need incentives.	Entertainment Driven by profits from industry, content and network providers	Distributed, user generated Innovation from the bottom
Social aspects	Social inequality	Globalization key	No social drive	Main social drive
Policy	Data protection	Moderate IPR Transparency Energy, Ecvironment	Strong IPR protection	No IPR protection Open standards Interconnection
Standards	Some tension between open and industrial standards Filter/search technologies key Need global standards	Competing closed standards may prevail Open standards acceptable	Open or Open source standards	Multi-cultural support
Network Neutrality	Important but not strongly enforced	Important but not key	Ignored, just a burden	Key element to enforce

⁵⁷ <http://www.digitalbuzzblog.com/facebook-statistics-stats-facts-2011/>.

⁵⁸ Hilary Clinton, 2010

⁵⁹ Gilbane Group (October 2010) 'A Blueprint for Book Publishing Transformation: Seven Essential Processes to Re-Invent Publishing'

network conditions, and based on that they are able to plan, decide and act. Cognitive processes belong to 'machine learning'. They use different mechanisms to remember previous interactions with the network and adapt future decisions according to that knowledge. The preceding figure shows future uses of Internet.

1.4 Mobile Devices

A mobile device is a small, hand-held computing device, typically having a display screen with touch input and/or a miniature keyboard and less than 0.91 kg. Early pocket sized ones were joined in the late 2000s by larger but otherwise similar tablet computers. As in a personal digital assistant (PDA), the input and output are often combined into a touch-screen interface⁶⁰. Enterprise digital assistants can further extend the available functionality for the business user by offering integrated data capture devices like barcode, RFID and smart card readers. 38% of Internet users worldwide had a smartphone in the second quarter of 2011, according to the results of Insites Consulting 'Social Media around the World 2011' global study about the usage of social media around the globe, with 9,000 respondents in 35 countries. Internet usage via mobile is quickly becoming as important as Internet usage via PC among those who own smartphones, according to research from Google and the Mobile Marketing Association (MMA)⁶¹ conducted during the first half of 2011 in several countries around the world.

Over 2 billion people worldwide will own at least one smartphone by 2015, with unit sales growing over 175% from 2010, according to Parks Associates' forecasts⁶². Parks Associates indicates that smartphone shipments jumped 70% in 2010, with approximately 500 million users. (Parks Associates, May 2011). Smartphone adoption grew considerably in the US and EU markets⁶³ during 2010.

⁶⁰ In telecommunications, 4G is the fourth generation of cellular wireless standards. It is a successor to the 3G and 2G families of standards. The 4G system was originally envisioned by the Defence Advanced Research Projects Agency (DARPA). In 4G systems mobility is provided by the mobile IP protocol, part of IP version 6, while in earlier cellular generations it was only provided by physical layer and datalink layer protocols.

⁶¹ <http://mmaglobal.com/Mobile%20web%20and%20app%20FINAL%2030June2011.pdf>

⁶² <http://www.parksassociates.com/blog/article/parks-pr2011-smartphones>

⁶³ Spain has the highest rate of smartphone adoption of all six markets, 37.6%, up about 38% from 27.3% in December 2009. Spain surpassed 2009 leader Italy in November 2010.

Smartphone use accounts for 65% of all mobile cellular traffic worldwide⁶⁴, despite smartphone penetration running at just 13%, according to Informa Telecoms & Media⁶⁵. The number of mobile phone world subscribers has doubled in the past five years⁶⁶. This figure is expected to rise by 10% to 5.6 billion in 2011. The growth in developing and emerging countries is especially strong. According to the most recent data from the UN agency International Telecommunication Union (ITU)⁶⁷, more than half the homes in these countries, even in rural areas, have a mobile phone connection. Landlines are rarely found or not at all.

In the EU the number of mobile phone subscribers is expected to rise to around 650 million by the end of 2010. This is a growth of almost 3 per cent compared to the previous year. Nearly a third of these now use UMTS. Germany has the most mobile phone contracts in the EU: around 111 million by the end of 2010.

The UK had the fastest year-over-year growth of the six markets, increasing about 63% from 21% to 34.3% and taking third place. The US came in fourth with a 27% adoption rate, up about 61% from 16.8% the prior year and in fourth place ahead of Germany and France.

⁶⁴ The US has higher percentages of smartphone users in the 18-to-24 bracket (16.7% compared to 14.5%) and 25-to-34 bracket (27.2% compared to 23.6% percent). Meanwhile, in EU5, those 55 and older represent 18.1% of the smartphone market, compared to 12.6% in the US. In December 2010, nearly 47% of mobile subscribers in the US were mobile media users (browsed the mobile web, accessed applications, downloaded content or accessed the mobile Internet via SMS), up about 17% from the previous year, according to other report data. comScore says the growth in mobile media usage is largely attributable to the growth in smartphone adoption, 3G/4G device ownership and the increasing ubiquity of unlimited data plans, all of which facilitate the consumption of mobile media. (Marketing Charts, February 2011)

⁶⁵ <http://blogs.informatandm.com/1397/press-release-smartphones-account-for-almost-65-of-mobile-traffic-worldwide/>

⁶⁶ The use of mobile communications is increasing far more in Asia and South America than in Europe and North America. In China, the number of mobile phone subscribers has risen by almost 13 percent this year to around 844 million. This figure is expected to grow by one-tenth within the next year to 930 million. In India, the number of subscriptions will go up by 30 per cent to 680 million. In Brazil, there will be 193 million connections by the end of the year; a growth of 11 percent. Japan is technically very advanced: 96 percent of all mobile communications users already use UMTS. (eito.com, August 2010).

⁶⁷ http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/CellularSubscriberPublic&ReportFormat=HTML4.0&RP_intYear=2010&RP_intLanguageID=1&RP_bitLiveData=False

Germany is followed by Italy (87 million), Great Britain (81 million), France (62 million) and Spain (57 million). By comparison: There are an anticipated 220 million in Russia and 287 million in the USA.

The threshold of 5 billion mobile phone subscribers will be exceeded this year for the first time. By the end of the year, the 4.5 billion figure will have increased by 12 per cent to 5.1 billion⁶⁸.

2. Regulatory Frameworks and Policy Frameworks

2.1 Internet Governance: International Bodies

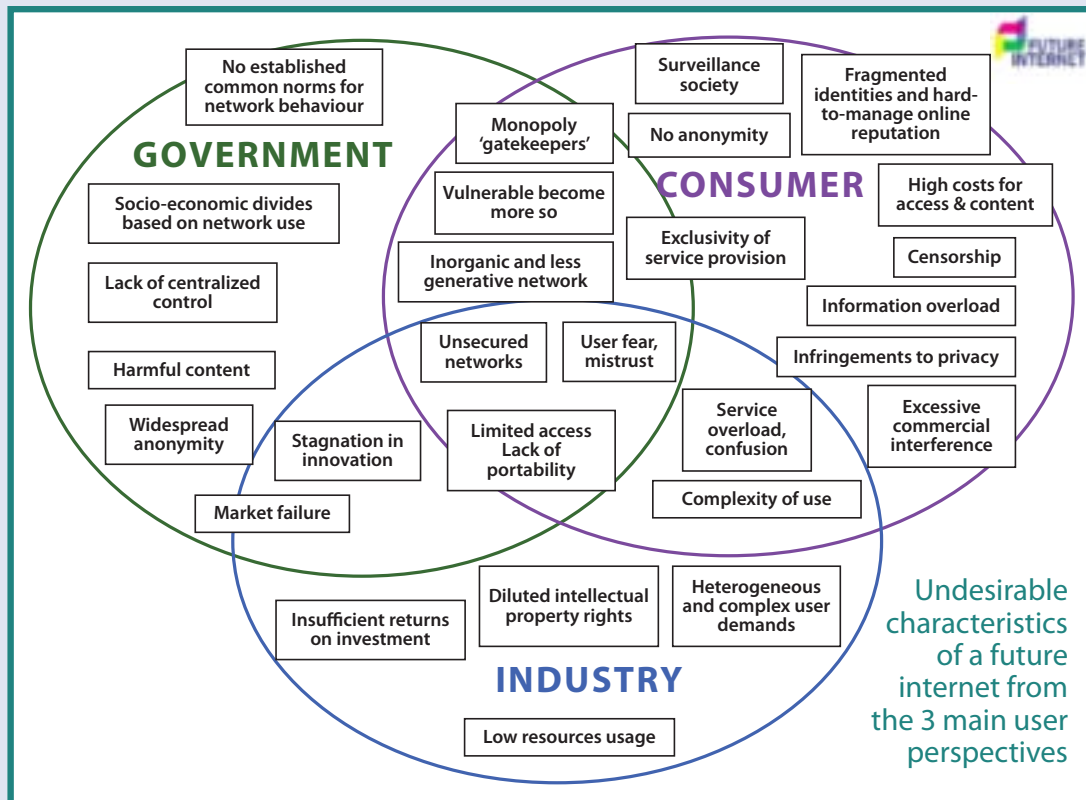
'Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.' This working definition was taken up in the Tunis Agenda for the Information Society, at the United Nations World Summit on the Information Society (WSIS) in 2005. In the last decades the number of initiatives taken by

international bodies to promote Internet governance provisions has grown. This chapter aims to provide some factual information on the main initiatives promoted internationally.

2.1.1 The United Nations Internet Governance Forum

The Internet Governance Forum (IGF) was established by the United Nations World Summit on the Information Society⁶⁹ (WSIS) as a non-binding multi-stakeholder platform. Since then, it has become the leading global multi-stakeholder forum on public policy issues related to Internet governance.

It is convened by the United Nations Secretary-General and has no executive powers. It brings together all the stakeholders (NGOs, Industry and Government) to discuss issues around ICT. Its UN mandate gives it convening power and the authority to serve as a neutral space for all actors on an equal footing. As a space for dialogue it can identify issues to be addressed by the international community and shape decisions that will be taken in other fora. The IGF is useful in shaping the



⁶⁸ <http://www.parksassociates.com/bento/shop/samples/parks-Smartphones.pdf>

⁶⁹ <http://www.intgovforum.org/cms/>

international agenda and in preparing the ground for negotiations and decision-making in other institutions.

2.1.2 *UNESCO: Code of Conduct for the Information Society*

In 2000 the United Nations Education, Scientific and Cultural Organisation (UNESCO) initiated a global debate on ethics in ICT aimed at stimulating reflection and debate on ethical, legal and societal aspects of the Information Society. It brings together participants from the largest possible number of countries representing the widest range of educational, scientific, cultural and social environments. The objectives of this initiative were to facilitate broader and fairer access to information, by elaborating common principles that could guide the Member States in the formulation of rules governing the application of 'fair use' within the framework of their national legislation while, protecting human dignity in the digital age.⁷⁰ European regional meetings on the ethical dimensions of the information society have been organised by the French Commission for UNESCO⁷¹ in cooperation with UNESCO and the Council of Europe. In October 2011 a code of conduct for the information society (non legally binding) was discussed at the UNESCO General Assembly⁷².

2.1.3 *Organisation for Economic Cooperation and Development*

The mission of the Organisation for Economic Cooperation and Development (OECD) is to promote policies that will improve the economic and social well-being of people around the world. The OECD's work on Internet governance spans several themes, including the information economy, information security and privacy, broadband and telecom, and e-government.⁷³ At a High Level Meeting⁷⁴ entitled 'The Internet Economy: Generating Innovation and Growth' in June 2011, the OECD developed an *Issues Paper (June 2011)* outlining

⁷⁰ <http://webworld.unesco.org/infoethics2000/objectives.html>.

⁷¹ Commission nationale française pour l'UNESCO

⁷² <http://unesdoc.unesco.org/images/0021/002126/212696f.pdf>.

⁷³ The OECD has developed a privacy statement generator, building on the OECD guidelines for the protection of privacy. They regularly publish policy guidelines on Internet economy issues and reviews of good governance in information society. Additionally, the OECD releases regular statistical updates on the future of the Internet economy (June 2011).

⁷⁴ See http://www.oecd.org/site/0,3407,en_21571361_47081080_1_1_1_1_1,00.html

some background to the issues discussed at the sessions of the High-Level Meeting, including broadband access, the role of broadband in developing the Internet economy, the balance of policy goals to strengthen growth and policy-making principles for an open Internet. In December 2011 the OECD published a report on data protection and trans-border data flow.⁷⁵

2.1.4 *Council of Europe*

The Council of Europe's expert group on critical Internet resources and cross-border traffic presented its proposal for '12 principles of Internet governance' at the 2010 summit of the Internet Governance Forum in Lithuania. A draft Treaty enshrining the principles of net neutrality and protecting the Internet from political interference was discussed by the Internet Governance Forum but not adopted. According to the draft Treaty 'Net neutrality' means that the commercial interests of telecommunications companies and Internet service providers should not affect consumers' access to the Web. For example, any action taken for competitive gain, such as blocking access to Skype with a view to selling another Internet telephony service, runs counter to the principles of net neutrality.

The proposal was drawn up by the Council of Europe, which has 47 member states and aims to promote human rights, the rule of law and democracy in Europe. This draft Internet treaty has been likened to the Space Treaty⁷⁶, agreed in 1967, according to which space exploration should be carried out for the benefit of all nations and guarantee 'free access to all areas of celestial bodies'. 'The fundamental functions and the core principles of the Internet must be preserved in all layers of the Internet architecture with a view to guaranteeing the interoperability of networks in terms of infrastructure, services and contents'.

2.1.5 *Internet Corporation for Assigned Names and Numbers (ICANN)*

'ICANN⁷⁷ was formed in 1998. It is a not-for-profit public-benefit corporation with participants from all over the world dedicated to keeping the Internet secure,

⁷⁵ http://www.oecd-ilibrary.org/science-and-technology/regulation-of-transborder-data-flows-under-data-protection-and-privacy-law_5kg0s2fk315f-en.

⁷⁶ Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies.

⁷⁷ See <http://www.icann.org/en/about/>

stable and interoperable. It promotes competition and develops policy on the Internet's unique identifiers.' It holds periodic public meetings for the purpose of encouraging global participation in its processes. The United States has been the supervisor of the organisation's policy decisions since its formation including dispute resolution over domain-name ownership or the introduction of top-level domains. In November 2005, an agreement was struck between the EU and the US to leave the supervision of domain names and other technical resources unchanged. On 2 October 2009, the United States announced it would end its unilateral supervision powers over ICANN,⁷⁸ which remains the body responsible for managing Internet addresses worldwide.

2.2 European Union Policy Regarding ICT

2.2.1 The Digital Agenda for Europe (DAE).

According to data prepared by the Global Institute and McKinsey's Technology, Media and Telecommunications Practices⁷⁹ as part of a knowledge partnership with the e-G8 Forum organised by the G20 French Presidency⁸⁰ in 2011, Internet-related consumption and expenditure is now bigger than agriculture or energy. On average, the Internet contributes 3.4 per cent to GDP in the 13 countries covered by the research.⁸¹ Most of the economic value created by the Internet falls outside the technology sector, with 75 % of the benefits captured by companies in more traditional industries. The Internet is also a catalyst for job creation. Among 4 800 small and medium-sized enterprises surveyed, the Internet created 2.6 jobs for each job lost to technology-related efficiencies.

⁷⁸ <http://www.euractiv.com/fr/node/188352>.

⁷⁹ http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Internet_matters.

⁸⁰ http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Internet_matters.

⁸¹ The United States is the largest player in the global Internet supply ecosystem, capturing more than 30 per cent of global Internet revenues and more than 40 per cent of net income. It is also the country with the most balanced structure within the global ecosystem among the 13 countries studied, garnering relatively equal contributions from hardware, software and services, and telecommunications. India and China are rapidly strengthening their position in the global Internet ecosystem with growth rates of more than 20 per cent. France, Canada, and Germany have an opportunity to leverage their strong Internet usage to increase their presence in the supply ecosystem. Other Asian countries are rapidly accelerating their influence on the Internet economy at faster rates than Japan. Brazil, Russia and Italy are in the early stages of Internet supply (ibid).

In 2011, Europe faced many challenges to its economic and social progress including an ageing population and growing global competition. With a view to addressing those challenges, in March 2010 the European Commission launched the Europe 2020 strategy, which sets out a vision for achieving high levels of employment, a low carbon economy, productivity and social cohesion. Seven flagship initiatives were foreseen to implement the strategy. The first, which was adopted by the Commission in May 2010, was the 'Digital Agenda for Europe'⁸² (DAE). It defines the key role that ICT must play if Europe is to succeed in its ambitions for 2020. Below is a summary of the key policies of the five-year plan:

- create a new **single market** to remove barriers to cross-border trade and licensing, simplify copyright clearance, complete the Single European Payment Area and boost the allocation of spectrum to new services such as mobile applications;
- improve **ICT standard-setting** and interoperability by reviewing the European Interoperability Framework;
- improve **trust and security** by tackling cybercrime and sexual exploitation and reviewing the data protection framework to protect consumer rights;
- increase **access to fast Internet** and aid the roll-out of fixed and wireless networks;
- raise the level of **digital literacy** by promoting e-skills initiatives and *inclusive* digital services.
- smart use of technology and exploitation of information to address **major societal challenges** such as climate change and the ageing population.

This strategy addresses the plethora of ICT applications so far identified in the EU, including:

2.2.2 E-Government

Europe's E-Government has developed significantly in recent years and is now seen by millions of citizens as a tangible reality. The impact of e-Government is being felt by citizens and companies well beyond government services, with tools such as electronic identity

⁸² http://ec.europa.eu/information_society/digital-agenda/index_en.htm.

helping citizens and businesses in everyday activities across society. ICT systems have become central to government processes for delivering services.

The roadmap focuses on a number of priorities, such as: 1) making e-Government inclusive, so that ‘no citizen is left behind’; 2) genuine efficiency and effectiveness in e-Government (to improve the transparency and accountability of government services, increase user satisfaction, and lighten the administrative burden on businesses and citizens); 3) making high-impact services for citizens and businesses more widely available, together with electronic procurement services for businesses, services for mobile citizens, including better job searching across Europe, or social security services (for example pension records and electronic benefit applications). E-Government will be critical in enabling service providers to take advantage of market opportunities outside their home country, under the EU’s Services Directive; 4) putting in place key enablers to lay the foundations for e-Government systems to work together, and building the connections between ICT systems in different public organisations and countries.

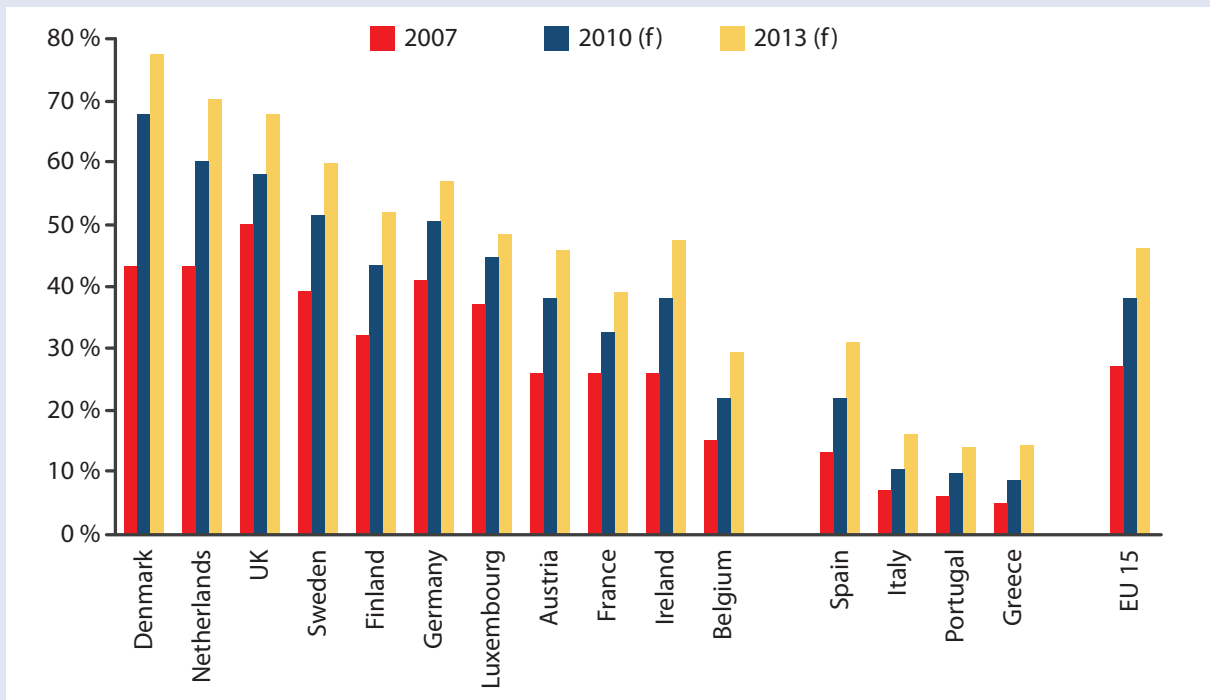
2.2.3 E-Commerce

E-commerce (electronic commerce) means the buying and selling of any goods or services on the Internet, ranging from flight tickets to garden furniture, newspaper subscriptions, ‘apps’ (smart phone applications) or music.

The Internet in general and e-commerce in particular, have enormous potential for boosting growth and creating jobs. In some G8 countries the Internet has accounted for 20 % of economic growth and 25 % of job growth in the last five years.⁸³ The Internet only accounts for less than 3 % of the EU economy (gross domestic product) and only 3.4 % of all products and services are sold over the Internet at the present time.

It has been suggested that the development of high-speed networks today is having the same impact as the development of electricity and transportation networks had a century ago. Services are converging and moving from the physical into the digital world, universally accessible on any device, be it a smart-phone, tablet, personal computer, digital radio or

Percentage of adults in selected EU countries who have made purchases on the Internet in the last 3 months, by country⁸⁵



⁸³ http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Internet_matters.

high-definition television. In parallel, the use of ICT is opening up an Internet-based commerce which covers many business sectors.⁸⁴ Key factors involved in this phenomenon are: e-commerce, e-invoicing and e-signatures. According to Eurostat, on average, 57 % of EU citizens ordered goods for parcel delivery using the Internet in 2010.

The e-commerce Directive,⁸⁶ which regulates a broad range of Internet activities in the EU, is to be reviewed to provide businesses and consumers with greater legal certainty in a borderless online marketplace. Towards the end of 2010 the Commission concluded a public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on electronic commerce.⁸⁷

On 11 January 2012 the European Commission adopted a communication on e-commerce to address a number of issues related to the optimisation of the EU single market for growth and jobs⁸⁸. The plans propose a number of measures including: better access to different kinds of online services for consumers across the EU;⁸⁹ greater transparency with respect to companies

and prices on the Internet and improved consumer protection;⁹⁰ and a more extensive availability of high-speed Internet and improved communication infrastructure for more citizens⁹¹.

The Commission is focusing on broad aspects of e-commerce which are inevitably linked to the application of the e-commerce directive, such as online payment systems and the efficiency of cross-border delivery services. The Commission agrees with online service providers that the current framework of the e-commerce directive and the principle of the limited liability of Internet intermediaries in particular, have proven to be of value.

‘Electronic communication and commerce necessitate “electronic signatures” and related services allowing data authentication; divergent rules with respect to legal recognition of electronic signatures and the accreditation of certification-service providers in the Member States may create a significant barrier to the use of electronic communications and electronic commerce; on the other hand, a clear Community framework regarding the conditions applying to electronic signatures will strengthen confidence in, and general acceptance of, the new technologies.’⁹²

⁸⁴ Only one of the nine ICT applications companies on the Financial Times Global 500 list is European; only four of the top 54 websites visited across Europe are of European origin.

⁸⁵ E-commerce across Europe Progress and prospects October 2008 http://www.eaca.be/_upload/documents/publications/E-commerce%20across%20Europe.pdf.

⁸⁶ http://ec.europa.eu/internal_market/e-commerce/docs/study/ecd/%20final%20report_070907.pdf.

⁸⁷ The e-commerce Directive (2000/31/EC) contains rules that facilitate the offer of online services in the EU and ensure, in the interests of consumer protection, that these services meet certain standards. The e-commerce Directive, for instance, determines that online service providers need only comply with rules from the country in which they are established. The Directive also obliges service providers to place their contact details on their websites, and ensures that advertisements can easily be identified as such. It also sets out a ‘safe harbour’ in the form of a liability exemption for online intermediary companies if they comply with certain conditions. In the second half of 2010, the Commission consulted stakeholders on the functioning of the Directive. Despite the numerous technological and business developments over the 10 years since its adoption, stakeholders consider that the Directive still offers a sound and balanced framework for the development of e-commerce. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:NOT>.

⁸⁸ http://ec.europa.eu/europe2020/index_en.htm.

⁸⁹ The Commission will: 1) extend the Internal Market Information System (IMI) and the Consumer Protection Cooperation

network (CPC) in order to ensure the correct application of the e-commerce Directive and of the Directives protecting consumers online; 2) quickly implement the European strategy for intellectual property rights, in particular by presenting a legislative initiative on private copying (2013) and a review of the Directive on copyright in the information society (2012); 3) report on the outcome of the consultation on the online distribution of audiovisual works (mid-2012); and (4) ensure that the new rules on selective distribution are rigorously applied.

⁹⁰ The Commission will also: 1) boost the capacity of the Consumer Protection Cooperation (CPC) Network, which consists of national authorities enforcing consumer legislation and equipping it with instruments able to ensure the implementation of relevant legislation at European level; 2) adopt a ‘European Consumer Agenda’ in 2012, including digital issues, which proposes measures to guarantee an appropriate level of information and customer care online; and 3) ensure the adequate protection of patients purchasing medicines online through the application of the directive on falsified medicines. This will include contributing to the creation of ‘trust marks’ to allow the identification of legal distance-selling websites, monitoring the development of falsified medicines and examining the potential specific risks linked to the online sale of medicines.

⁹¹ The Commission will, inter alia, adopt an overall strategy on cloud computing (2012).

⁹² Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures; recital 4.

2.2.4 Corporate Social Responsibility

In October 2011, the European Commission adopted a new strategy on corporate social responsibility (CSR)⁹³. It describes how enterprises can benefit from CSR while contributing to society as a whole by making every effort to meet their social responsibilities. In the Commission's view, enterprises should have in place a process to integrate social, environmental, ethical and human rights concerns into their business operations and core strategy in close cooperation with their stakeholders. Important features of the CSR definition⁹⁴ are: 1) recognition of the importance of core business strategy; 2) development of the concept of 'creating shared value'; 3) explicit recognition of human rights and ethical considerations in addition to social, environmental and consumer considerations.

The action agenda put forward for the new CSR policy for the period 2011-2014 covers 8 areas: 1) enhancing the visibility of CSR and disseminating good practices; 2) improving and tracking levels of trust in business; 3) improving self- and co-regulation processes; 4) enhancing market reward for CSR; 5) improving company disclosure of social and environmental information; 6) further integrating CSR into education, training and research; 7) emphasising the importance of national and sub-national CSR policies and (8) better aligning European and global approaches to CSR.⁹⁵

⁹³ http://ec.europa.eu/enterprise/policies/sustainable-business/corporate-social-responsibility/index_en.htm.

⁹⁴ This is the first time in 10 years that the Commission has changed its definition of CSR. Its previous definition was: 'a concept whereby companies integrate social and environmental concerns in their business operations and in their interaction with their stakeholders on a voluntary basis.' The new definition is consistent with internationally recognised CSR principles and guidelines, such as the OECD Guidelines for Multinational Enterprises, the ISO 26000 Guidance Standard on Social Responsibility and the United Nations Guiding Principles on Business and Human Rights. It should provide greater clarity for enterprises, and contribute to greater global consistency in expectations for business, regardless of where they operate.

⁹⁵ The Commission highlights the OECD Guidelines for Multinational Enterprises, the 10 principles of the UN Global Compact, the UN Guiding Principles on Business and Human Rights, the ILO Tri-partite Declaration of Principles on Multinational Enterprises and Social Policy, and the ISO 26000 Guidance Standard on Social Responsibility. The Commission aims to monitor the commitments of large European enterprises to take account of internationally recognised guidelines and principles. It will also present a report on EU priorities for the implementation of the UN Guiding Principles on Business and Human Rights,

The Commission has noted that while progress is continuing to be made in embedding CSR in the ICT domain, only 15 of the 27 EU Member States have national policy frameworks to promote CSR. A report on the implementation of this action agenda will be published in time for a review meeting scheduled for mid 2014. All CSR measures previously described also apply to the ICT sector.

2.2.5 Interoperability and Standards

Interoperability is the ability of computers or digital systems to exchange and use information with one another.⁹⁶ If, for example, rival telephone networks used completely different protocols it would not necessarily be possible to connect to others on a different network. 'Interoperability means working together - collaboration of systems, services and people. When people work together, they need to communicate and make agreements. They need to agree on the tasks they will perform and how they will exchange results. If their nationality is different, they also need to agree on the language in which they will communicate. Moreover, they need to overcome cultural and legal differences.'⁹⁷ The European Commission recently announced the adoption of the European Interoperability Framework, which has been closely monitored by big ICT firms and public administrations to find out what kind of software licences they should have.⁹⁸

2.2.6 Very Fast Internet

The Internet is facing problems as a result of the enormous growth in content and traffic on the network. Moreover, phenomena such as e-commerce and Internet banking are struggling with security issues, because

and develop human rights guidance for a limited number of industrial sectors and for small businesses.

⁹⁶ Lack of interoperability of Microsoft software and servers, for instance, was at the centre of an antitrust case brought by former EU Commissioner Mario Monti in 2004 when he was head of the Commission's competition department. Last June the European Commission launched an antitrust investigation into IBM's mainframe business after two smaller companies complained that they could not use the company's operating system without buying costly IBM hardware.

⁹⁷ <http://ec.europa.eu/idabc/en/document/2319/5938.html>

⁹⁸ — Fair Reasonable and Non-Discriminatory (FRAND) or royalty-free. Commission initiatives in the area stem from a 2009 White Paper 'Modernising ICT Standardisation in the EU — The Way Forward'. The European Parliament has also published a non-legislative report on the future of European standardisation.

they were not considered in the design of the original network architecture. Although, the European Union has seen connection speeds double in recent years, it still has a steep hill to climb before it hits the targets set out in its Digital Agenda. The Commission is working on a number of initiatives to reach the Digital Agenda targets.⁹⁹

2.2.7 E-Skills

The EU's 'New Skills for New Jobs' initiative was launched in December 2008.¹⁰⁰ Its premise is that in order to provide job opportunities for all and create a more competitive and sustainable economy, Europe needs a highly-skilled workforce able to meet current and future challenges. In November 2010, the commissioner published a set of proposals known as the 'Agenda for New Skills and Jobs'.¹⁰¹

2.2.8 E-Advertising

The EU consumer policy strategy 2007-2013 states that 'the technological revolution brought about by the Internet is paving the way for innovative ways to advertise goods and services'. However, it concedes that the same revolution also presents challenges to the self-regulation of advertising. Advertisers have preferred a self-regulatory approach to their work. A report from the European Advertising Standards Alliance (EASA)¹⁰² outlines how advertisers regulate themselves.¹⁰³ In

April 2009, the Commission launched the European Consumer Summit, inviting leading industry players to participate in a consultation on consumer protection and privacy in relation to online advertising in Europe.¹⁰⁴

On 1 December 2011, The European Commission joined forces with major technology firms including Apple, Facebook and Google and agreed to improve the protection of children online.¹⁰⁵ The coalition, which includes 28 companies,¹⁰⁶ will develop an age-based online ratings system and aims to strengthen privacy settings. It also plans by the end of next year to make it easier to report inappropriate content. Other measures include improving parental control and enhancing cooperation among law enforcement and hotline authorities to remove online material showing sexual abuse. The EU produced specific guidelines on child pornography in December 2003 (Decision 2004/68/JHA)¹⁰⁷.

2.2.9 Cybercrime

In the Council of Europe's *Cybercrime Treaty* (EST no. 185),¹⁰⁸ cybercrime is used as an umbrella term to refer to an array of criminal activity including offences against computer data and systems, computer-related offences, content offences, and copyright offences. Other commentators have suggested that the definition is broader and includes activities such as child pornography and cyber-bullying.¹⁰⁹ Common cyber criminal activity involves stealing sensitive information such as credit card details, online login credentials, browsing history and email addresses. This information can then be sold in a vibrant underground economy where credit card details can be bought from \$0.07 to \$ 100, with

⁹⁹ See the Broadband Package published in September 2010. The package also includes a five-year programme to promote efficient radio spectrum use, encourages public and private investment in networks and proposes the inclusion of broadband in the EU's Universal Service requirements to increase its take-up. The Commission's Radio Spectrum Policy Programme (RSPP) is currently under scrutiny at the European Parliament and in the Member States.

¹⁰⁰ <http://www.euractiv.com/innovation/eu-launches-new-skills-new-jobs-initiative/article-178158>.

¹⁰¹ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0682:EN:NOT>.

¹⁰² The EASA represents Europe's advertising industry by bringing together national self-regulatory organisations, or SROs, at European level. National SROs, which exist in 22 of the 27 Member States, differ slightly from country to country, mainly as a result of legal and cultural differences between EU Member States, but all have the same goal of making sure that advertising standards remain within an acceptable boundary.

¹⁰³ As advertisers migrate to the Web, advertising standards have attracted attention. In 2008 negotiations between advertising agencies, associations and national self-regulatory organisations produced a Digital Marketing Communications Best Practice guidebook which is intended to define

what kind of online content falls under the agreed advertising codes. Nevertheless, EU lawmakers and consumer groups continue to question whether these rules are robust and transparent enough to address consumer protection issues that arise in the online sphere. .

¹⁰⁴ http://ec.europa.eu/consumers/events/euro_cons_summit/index_en.htm.

¹⁰⁵ <http://www.euractiv.com/infosociety/eu-tech-firms-join-forces-protect-children-Internet-news-509381>.

¹⁰⁶ Other companies in the coalition include Apple, BSKyB, BT, Deutsche Telekom AG, Nintendo, Nokia and Orange.

¹⁰⁷ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004F0068:EN:HTML>.

¹⁰⁸ *Convention on Cybercrime Budapest, 23.XI.2001* <http://conventions.coe.int/Treaty/en/Treaties/html/185.htm>.

¹⁰⁹ Gabriole Zeviar-Geese, *The State of Law on Cyberjurisdiction and Cybercrime on the Internet*, 1 Gonz. J. Int'l L. (1997-98).

discounts offered for buying in bulk. It has been estimated that 69 % of adults with an online presence have been a victim of cybercrime during their lifetime, which equates to one million victims every day. The cost of global cybercrime has been estimated at \$ 114 billion annually; rising to \$ 388 billion when financial losses and time lost are included.¹¹⁰ In the UK alone, cybercrime costs the economy £ 27 billion a year with nearly half of the £ 21 billion cost to business being made up of intellectual property theft.¹¹¹ Worryingly, the trends for cybercrime are moving in the wrong direction; the average daily volume of web-based attacks increased by 93 % between 2009 and 2010.¹¹² It is unsurprising then that the EU Internal Security Strategy lists cybercrime as one of the main security challenges facing Member States.¹¹³

Europol has pointed to the Internet as a facilitator for organised crime.¹¹⁴ The EU's first significant response to cybercrime has been the establishment of computer emergency response teams (CERSTS) in every country.¹¹⁵ The EU initiative on Critical Information Infrastructure Protection (CIIP) aims to strengthen the security and resilience of vital ICT infrastructure by stimulating and supporting the development of a high level of preparedness, security and resilience capabilities at both national and European levels. The Commission set out a CIIP action plan in its Communication on Critical information Infrastructure Protection (COM (2009) 149). The EU adopted the CIIP action plan on 31 March 2011. The plan also aims to forge international agreements on cyber-security. The EU-US Working Group on Cyber-security and Cyber-crime, established during the EU-US Summit of November 2010,¹¹⁶ is an important step in this direction. This Working Group, is tasked

with developing collaborative approaches to a wide range of cyber-security and cyber-crime issues.

In 2010, the European Commission also presented a proposal for a Directive *on attacks against information systems* and repealing Council Framework Decision 2005/222/JHA.¹¹⁷ The Directive seeks to strengthen and modernise the already existing rules of the Framework Decision adopted in 2005, by including provisions to deal with the emergence of large-scale simultaneous attacks against information systems and the increased frequency of botnets. The Directive also provides for criminal prosecution and more severe criminal sanctions for perpetrators of cyber attacks.

The EGE will be addressing all these topics in its forthcoming Opinion on ethics and surveillance and security technologies to be adopted in 2013.

2.2.10 Digital Divide

Under Pillar 6 of the Digital Agenda (Enhancing digital literacy, skills and inclusion), the Commission proposes a series of measures to promote the take-up of digital technologies by potentially disadvantaged groups, such as the elderly, the less-literate and those on a low-income. Improving access for people with a disability is another of the policy measures set by the Digital Agenda. An additional part of the e-inclusion agenda is tackling the issues of an ageing population, with the help of ICT: a better quality of life for the elderly, reduced cost of care, and business opportunities in the 'silver economy'. Under Pillar 7 (ICT-enabled benefits for EU society) the Commission will reinforce the Ambient Assisted Living (AAL) Joint Programme to allow older people and persons with disabilities to live independently.

2.2.11 Net Neutrality

As part of the 2009 EU telecoms reform package,¹¹⁸ the Commission committed itself to scrutinising closely the open and neutral nature of the Internet and to reporting on the state of play to the European Parliament and the Council of Ministers.

¹¹⁰ Symantec Internet Security Threat Report, Volume 16 April 2011.

¹¹¹ http://www.baesystemsdetica.com/uploads/resources/THE_COST_OF_CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf.

¹¹² op cit 2.

¹¹³ The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, Brussels, 22.11.2010 COM(2010) 673 final http://ec.europa.eu/commission_20102014/malmstrom/archive/internal_security_strategy_in_action_en.pdf.

¹¹⁴ <http://www.scribd.com/doc/55886813/Europol-Organised-crime-threat-assessment-2011>.

¹¹⁵ The President of the European Commission has asked the EGE to issue an Opinion on the ethics of security and surveillance technologies. It is expected to be completed in 2013.

¹¹⁶ <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/246>.

¹¹⁷ Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, Brussels, 30.9.2010 COM(2010) 517 final 2005/222/JHA http://www.coe.int/t/dghl/standardsetting/t-cy/Proposal%20directive_com2010_517.pdf.

¹¹⁸ <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/568>.

The consultation covers a number of issues such as: whether Internet providers should be allowed to adopt certain traffic management practices, prioritising one kind of Internet traffic over another; whether such traffic management practices may create problems and have unfair effects on users; whether the level of competition between different Internet service providers and the transparency requirements of the new telecom framework may be sufficient to avoid potential problems by allowing consumer choice; and whether the EU needs to act further to ensure fairness in the Internet market, or whether industry should take the lead.

2.2.12 Internet of Things

The Internet of things (IoT) is an integrated part of the Future Internet. The Commission has published a strategic research roadmap¹¹⁹ which states that the vision of Future Internet based on standard communication protocols considers the merging of computer networks, the Internet of things (IoT), Internet of people (IoP), Internet of energy (IoE), Internet of media (IoM), and Internet of services (IoS), into a common global IT platform of seamless networks and networked 'smart things/objects'.

2.2.13 E-Health

European healthcare establishments are facing substantial challenges over the next decade, such as significant demographic changes and reduced human resources. E-Health offers the rich potential of supplementing traditional delivery of services and channels of communication to provide enhanced access to information, streamlined organisational processes and improved quality, value and patient satisfaction. e-Health is popularly defined as 'health services and information delivered through the Internet and related technologies'.¹²⁰ The concept of e-Health is part of the wider umbrella term 'connected health'. Connected health relates to a model of healthcare delivery based on the use of technology to provide health care remotely. The areas of e-Health and connected health, therefore, encompass a diverse range of information and communication technologies (ICT) employed in the health field.¹²¹ The development, adoption and

implementation of a broad range of e-Health applications, such as electronic health records, health information websites, e-prescribing, home health monitoring and tele-health, has the potential to enhance quality of care and empower patients to make informed healthcare decisions. On a daily basis, healthcare professionals strive to reduce risks and improve outcomes for their patients. Health information has a key role to play in healthcare planning decisions — where to locate a new service, whether or not to introduce a new national screening programme and decisions on best value for money in health and social care provision. Reductions in health budgets and competition for limited resources require enhanced efficacy and efficiency of health services.¹²² For meeting all of these challenges, adequate information and knowledge are required and e-Health applications offer the prospect of acquiring information which is accurate, reliable and timely.

The European Commission has supported EU research in the field of e-Health for over two decades and during that time it has provided € 1 billion in funding to over 450 projects.¹²³ Since 2004, the Commission has been developing targeted policy initiatives aimed at encouraging the widespread adoption of e-Health technologies throughout Europe. These targeted e-Health initiatives began with the publication of *Communication COM(2004) 356*, i.e. the e-Health Action Plan 2004-2010 (eHAP).¹²⁴ The aim of the eHAP was to facilitate the EU in achieving the full potential of e-Health systems and services within a European e-Health Area. An Action Plan for e-Health was published by the Commission in 2007, which overlapped and coincided with many aspects of the eHAP, with a view to assisting in progressing the eHAP.¹²⁵ A public consultation on a new

docs/policy/interoperability_report_final092006-cover.pdf, accessed January 11th 2012.

¹²² Ashly D. Black AD, Car J, Pagliari C et al. *PLoS Med* 2011; 8(1):e1000387.

¹²³ European Commission (2011). Digital Agenda: Kroes and Dalli welcome Council Presidency e-Health Declaration on delivering better health care. Available at: <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/287&ty pe=HTML>, accessed January 11th 2012.

¹²⁴ European Commission (2004). *Communication COM(2004) 356 e-Health – making healthcare better for European citizens: An action plan for a European e-Health Area*. Available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0356:FIN:EN:PDF>, accessed on 11 January 2012.

¹²⁵ European Commission (2007). *Action Plan for e-Health, Commission Staff Working Document, SEC(2007) 1729*. Available at: <http://eur-lex.europa.eu/LexUriServ/>

¹¹⁹ http://www.Internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2011.pdf.

¹²⁰ Eysenbach G. What is Health?. *Journal of Medical Internet Research* 2001;3(2):e20.

¹²¹ Connected Health and Quality for European Citizens 2006 http://ec.europa.eu/information_society/activities/health/

e-Health Action Plan for 2012-2020 ran from March to May 2011 and it is envisaged that the new e-Health Action Plan will be adopted in the fourth quarter of 2012.¹²⁶ In 2006 the Commission launched 'ICT for Health and i2010' as part of the i2010 policy framework, which was a new strategy aimed at transforming the European healthcare landscape by moving towards preventative and patient-centred health systems.¹²⁷ This would provide greater continuity of care through the deployment of interoperable e-Health services throughout Europe. e-Health also represents an important aspect of the Digital Agenda for Europe and is incorporated into a number of actions under Pillar 7 ICT for Social Challenges, where the potential of ICT is used to revolutionise health services and deliver better public services, i.e. through its strategy for 'sustainable healthcare and ICT-based support for dignified and independent living'.¹²⁸

2.3 Current EU Regulatory Frameworks for Personal Data Protection

The Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data of 1981 (Convention 108) can be considered as the first European legal framework for the fundamental right to protection of personal data. The principles of Convention 108 were refined in Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,¹²⁹ which forms the cornerstone of data protection law within the EU. Social networking sites (SNS) and 'cloud computing' could also pose challenges to data protection, as they may involve a loss of individuals' control over their potentially sensitive information when they store their data with programs

hosted on someone else's hardware. A recent study confirmed that there seems to be a convergence of views — among data protection authorities, business associations and consumer organisations — that risks to privacy and the protection of personal data associated with online activity are on the increase.¹³⁰

At the same time, ways of collecting personal data have become increasingly elaborate and less easy to detect. For example, the use of sophisticated tools allows economic operators to target individuals better, thanks to the monitoring of their behaviour. Moreover, the growing use of procedures allowing automatic data collection, such as electronic transport ticketing, road-toll collecting or the use of geo-location devices, makes it easier to determine the location of individuals simply because a mobile device is used. Public authorities also use an increasing amount of personal data for various purposes, such as tracing individuals in the event of an outbreak of a communicable disease, preventing and fighting terrorism and crime more effectively, administering social security schemes, for taxation purposes, or as part of their e-government applications.¹³¹

All this inevitably raises the question whether the existing personal data protection legislation can still cope with these challenges fully and effectively. To address this question, the European Commission launched a review of the current legal framework with a high level conference in May 2009 followed by a public consultation until the end of 2009. The findings confirmed that the core principles of the Directive are still valid and that its technologically neutral character should be preserved.

On 4 November 2010, the Commission adopted a communication entitled 'A comprehensive approach to personal data protection in the European Union'.¹³² This communication was sent to the European Data Protection Supervisor (EDPS) for consultation. The EDPS identified the four main drivers which determine

LexUriServ.do?uri=CELEX:52007SC1729:EN:HTML, accessed on 11 January 2012.

¹²⁶ For more information see: http://ec.europa.eu/information_society/activities/health/ehealth_ap_consultation/index_en.htm, accessed on 11 January 2012.

¹²⁷ European Commission (2006). *ICT for Health and i2010. Transforming the European healthcare landscape*. Available at: http://ec.europa.eu/information_society/activities/health/docs/publications/ictforhealth-and-i2010-final.pdf, accessed January 11th 2012.

¹²⁸ Digital Agenda For Europe 2010-2020 http://ec.europa.eu/information_society/digital-agenda/index_en.htm, accessed on 11 January 2012.

¹²⁹ OJ L 281, 23.11.1995, p. 31.

¹³⁰ Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 'A comprehensive approach on personal data protection in the European Union', 4 November 2010, Com (2010) 609 final, 2.

¹³¹ Com (2010) 609 final, 2-3.

¹³² Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 'A comprehensive approach on personal data protection in the European Union', 4 November 2010, COM (2010) 609 final, 2.

the environment in which the review process of the Directive should take place. The first driver is technological development;¹³³ the second is globalisation¹³⁴ and the third is the Lisbon Treaty. In fact under the Lisbon Treaty, data protection has gained significant importance. The Charter of Fundamental Rights of the European Union has become binding and Article 8 of the Charter recognises an autonomous right to the protection of personal data.¹³⁵ The same right is laid down in Article 16 of the Treaty on the Functioning of the European Union (TFEU),¹³⁶ which introduced a new legal basis for data protection applicable to all personal data processing in the private and in the public sector, including processing in the areas of police and judicial cooperation and common foreign and security policy. The fourth and final driver identified by EDPS is represented by parallel developments taking place in the context of international organisations. There are currently various debates focusing on the modernisation of the current legal instruments for data protection.¹³⁷

Data Protection in the EU has a strong internal market dimension. As a result, the Directive's harmonisation of national data protection laws is not limited to minimal harmonisation but amounts to harmonisation that is generally complete.¹³⁸ At the same time, the Directive gives the Member States room for manoeuvre in certain areas, authorising them to maintain or introduce specific rules for specific situations. This, together with the fact that the Directive 'has sometimes been incorrectly implemented by Member States',¹³⁹ has led to divergences among the national laws implementing the Directive, which run counter to one of its main objectives, that of ensuring the free flow of personal data within the internal market. This applies to a large number of sectors and contexts, for instance when processing personal data in the employment context or for public health purposes. Moreover, the divergence in the way the Directive is implemented by the Member States creates legal uncertainty, not only for data controllers but also for data subjects, with the risk of distorting the equivalent level of protection that the Directive is supposed to achieve and ensure. The Commission's reports on the implementation of the Data Protection Directive 95/46/EC¹⁴⁰ concluded in 2003¹⁴¹ and in 2007¹⁴² that the Directive did not succeed in achieving its internal market policy objective fully, or in removing differences in the level of data protection actually afforded in the Member States. Enforcement was also identified as an area where improvement was needed. To address the question whether existing EU data protection legislation can still cope fully and effectively with the challenges, the Commission

¹³³ Today's technology is not the same as when the Directive was conceived and adopted. Technological phenomena such as cloud computing, behavioural advertising, social networks, road toll collecting and geo-location devices profoundly changed the way in which data are processed and pose enormous challenges for data protection. A review of European data protection rules will have to address these challenges effectively.

¹³⁴ The progressive abolition of trade barriers has given businesses an increasingly worldwide dimension. Cross-border data processing and international transfers have increased tremendously in recent years. Furthermore, data processing is now ubiquitous due to information and communication technologies: Internet and cloud computing have allowed delocalised processing of large quantities of data on a worldwide scale.

¹³⁵ Article 8.1 Charter: 'Everyone has the right to the protection of personal data concerning him or her'. As the protection of the individual with regard to the processing of personal data is in no way restricted to data concerning the private sphere of the individual, the right to personal data protection and the right to privacy do not coincide. See on this, Colette Cuijpers, 'A private law approach to privacy: mandatory law obliged?', *Scripted*, volume 4, Issue 4, September 2007, 312.

¹³⁶ Article 16 TFEU: 'Everyone has the right to the protection of personal data concerning them'.

¹³⁷ It is important to mention in this respect the current reflections in relation to the future revision of Convention 108 of the Council of Europe and of the OECD Privacy Guidelines. Another important development concerns the adoption of international standards on the protection of personal data and privacy, which might possibly lead to the adoption of a binding global instrument on data protection.

¹³⁸ Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 'A comprehensive approach on personal data protection in the European Union', 4 November 2010, COM (2010) 609 final, 10.

¹³⁹ Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 'A comprehensive approach on personal data protection in the European Union', 4 November 2010, COM (2010) 609 final, 10.

¹⁴⁰ Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

¹⁴¹ Report from the Commission — First Report on the implementation of the Data Protection Directive (95/46/EC), 15.5.2003, COM(2003) 265final.

¹⁴² Communication on the follow-up of the work programme for a better implementation of the Data Protection Directive, 7.3.2007, COM(2007) 87final.

has launched a review of the current legal framework on data protection. An assessment of the current regulatory framework (implementation of Directive 95/46, including the analysis of Member States' legislation transposing the Directive into national law, on the basis of studies,¹⁴³ opinions of the Article 29 Working Party,¹⁴⁴ and a survey launched by the Commission in relation to certain aspects of the Directive, to which 22 Member States responded) is also expected to be published in 2012. In its resolution of 6 July 2011 the European Parliament approved a report that was in favour of the Commission's approach to reforming the data protection framework.¹⁴⁵ The Council of the European Union adopted conclusions on 24 February 2011 in which it broadly supported the Commission's intention to reform the data protection framework and agreed to many elements of the Commission's approach. Likewise, the European Economic and Social Committee supported an appropriate revision of the Data Protection Directive and the Commission's general intention of ensuring a more consistent application of EU data protection rules across all Member States.¹⁴⁶

¹⁴³ Comparative study on different approaches to new privacy challenges, (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf); European Agency on Fundamental Rights, Data Protection in the European Union: the role of National Data Protection Authorities — Strengthening the fundamental rights architecture in the EU II, 2010, available at http://fra.europa.eu/fraWebsite/attachments/Data-protection_en.pdf; Study on the economic benefits of privacy enhancing technologies, London Economics, July 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf); Study for an impact assessment for the future legal framework for personal data protection by GHK Consulting Ltd., February 2011, launched by the Commission to support the IA process; case law on the circumstances in which IP addresses are considered personal data, by time.lex CVBA, October 2010; Allocation and Use of IP Addresses, by Vigilio Consult, 2010; Privacy and Trust in the Ubiquitous Information Society, by Fraunhofer ISI et al., March 2009; Legal Analysis of a Single Market for the Information Society: New rules for a new age?, by DLA piper, 2009.

¹⁴⁴ Working Party on the Protection of Individuals with regard to the Processing of Personal Data, established by Article 29 of the Directive; the opinions of the Working Party are accessible under: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2011_en.htm.

¹⁴⁵ EP resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union (2011/2025(INI)), <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2011-0323&language=EN&ring=A7-2011-0244> (rapporteur: MEP Axel Voss (EPP/DE)).

¹⁴⁶ CESE 999/2011.

On January 25, 2012, the Commission has adopted a revision of the data protection EU law¹⁴⁷ to be now adopted in co-decision by the European Parliament and the Council. Changes introduced in the adopted Commission proposal include:

- A reinforced 'right to be forgotten': people will be able to delete their data if there are no legitimate reasons for retaining it.
- Wherever consent is required for data to be processed, it will have to be given explicitly, rather than assumed, as is sometimes the case now.
- There will be increased responsibility and accountability for those processing personal data.
- People will be able to refer cases where their data has been breached or rules on data protection violated to the data protection authority in their country, even when their data is processed by an organisation based outside the EU.
- EU rules will apply even if personal data is processed abroad by companies that are active in the EU market.

2.4 Gaps or Deficits in Regulations and Policies

The previous sections describing the history, current state of the art and foreseeable future regarding ICT on the one hand, and governance and regulatory frameworks on the other hand, have shown that there are a number of ICT areas, both well-known and new, that involve challenges for individuals and societies. In the next part of the Opinion a number of ethical concerns will be described both in general terms and with respect to a number of different topics where ICT is especially relevant. The debate on ethics and governance of ICT is complex and needs to address a wide range of considerations, values and principles, such as: *autonomy; identity; privacy and trust; responsibility; justice and solidarity.*

Part B of this Opinion elaborates on these ethical considerations. Gaps will be identified where the group has identified a need for further action in the form of public communication, research, education, technological solutions or regulatory measures.

¹⁴⁷ http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

PART B: EGE OPINION

3. Ethical Aspects

Information and Communication Technologies have not only dramatically changed personal behaviour, life styles and interpersonal relationships, but also the perception and the notion of society itself and the information that may be collected about individuals with or without their consent. Technological changes also affects routine aspects of modern societies such e-administration, e-commerce, e-health, e-education, telework and e-voting, telephone communication, political activities, consumers' rights, private (intellectual) property, democracy etc..

In order to provide an analysis of the ethical concerns, the EGE has drawn on the ethical framework of the European Union, as stated in the Lisbon Treaty and the European Charter of Fundamental Rights.¹⁴⁸ The EGE has grouped the 'ethical concerns' regarding ICT under the four headings of:

1. a person's identification using ICT, and the development and/or continuous re-interpretation of one's personal identity, in the media made available by ICT;
2. the changes of the social sphere, particularly concerning social relations, culture, education, environment, and e-governance;
3. the new possibilities of political participation and practices of citizenship using ICT;
4. the sphere of e-commerce.

The following chapters will address the specific implications of different uses of ICT. They will also refer to some EU legislation and policy actions while not pretending to address all the possible legal or policy issues.

3.1 Challenges to the Concept of Identity

3.1.1 Introduction

Since the introduction of digital communication, 'the' Internet has been associated with the dream of limitless communication, creativity, new forms and formats

of social relationships bridging time, place and space. The metaphor of the 'global village' romanticized the new 'space' as a 'space without borders', and even more so, as a *common* sphere where individuals share their private lives, build up new networks, and create a new understanding of the social sphere in transcending the conceptual separation of the public and the private. But, there are nice dreams nonetheless. The digital era and the digital ways of self-expression and communication raise new questions and a reconsideration of many 'traditional' ways of protecting individual rights while maintaining the freedom and security of societies and individuals.

Online games, social networks, blogs and new marketplaces have become crucial factors in determining an individual's identity or identities (and avatars) They change the way everyone, including children and adolescents develop their identity and maintain relationships, and often the younger generation educates the older generation about the ways use of the Internet may combine very different skills to 'design' one's identity rather than just 'to have' it.

'Wrzuciła zdjęcia na Facebooka i wyleciała z pracy'

A female student – Joanna - worked at a day care center for handicapped children as an assistant to a teacher. Somebody has discovered her photographs on Facebook (one of them showed her with bare shoulders, other in bathing suits) and reported to a director, who gave Joanna an order to remove the photos. Joanna insisted that there is nothing wrong with the photos but promised to block access to them. She consulted with a lecturer in professional ethics who was of the opinion that the photos did not pose any problem. She blocked access leaving the note: 'best regards to a whistleblower who forced me to block my photos'. Eventually, she got fired from her job. A director for public media from a company dealing with the presentation of institutions on the web warned against leaving the texts on social portals. The employers check whether the portals do not contain materials adversely influencing a company's image which can result in a termination of employment.

¹⁴⁸ The principles are quoted at the beginning of the Recommendation Part.

3.1.2 The Digital Identity

Scholars from the fields of developmental biology, psychology, sociology and philosophy have begun to look into the ways that identities are shaped and changed in the era of digital self-expression and communication.¹⁴⁹ The changes, these scholars claim, will be radical, modifying many 'traditional' concepts that have structured our way of giving the world we live in, and our own lives, meaning. One concept that has attracted attention is the so-called digital identity.¹⁵⁰ Mostly, the digital identity approach addresses questions of authentic identification, i.e. the identification of a person in the Internet, and the challenge of trust: For example, in digital interactions the partners need to ensure that their signatures are valid and belong to those who use them; not only must credit card or bank account uses be secured but the whole process of online shopping, for example, has to rely upon the trust that we provide what is ours, and that the recipient handles our 'identity' and any information provided with care.

In addition to commercial transactions, social networks demand an 'authentic' name of their users. Hence, the digital traces left during one's actions require trust, care, and respect for the other's privacy, property or even dignity on both sides. These requirements adhere implicitly or explicitly to *moral values and norms* that up to the present have not been spelled out sufficiently. While the digital identity with respect to commerce is now being regulated, the broader question of identity-as-identification, as is the case with 'faked identities' in networks, games etc., needs to be further addressed — and not necessarily only from a legal point of view.

3.1.3 The Concept of Personal Identity in the Digital Era

While literature on the 'digital identity' is growing, newer research has shown that it is not enough to analyse identity questions in terms of those matters that mostly concern the *identification of a person* rather than his or

her *identity as a person* (philosophy distinguishes between identity of the same — idem — and identity of the self — ipse).¹⁵¹

Individuals welcome ICT because they expect or experience new ways to realise their freedom, and they share their social identity with others. The informal social forms of communication – over time and over space: certainly enhance traditional ways of expression and communication.

'Writing simultaneously online gives me an added sense of interactivity and a feeling of proximity. I go as far as sacrificing my early morning sleep to get up and go online with friends in Greece who are seven hours ahead. My mornings are dedicated to writing online and sending emails while drinking my coffee. Early mornings have become the favourite part of my day and early classes seem to disrupt my daily interactive ritual.'
(Stacey)

'I think I actually need to use the Internet on a daily basis in order to maintain all of my relationships with people that are currently established. If I don't "instant message" or e-mail my girlfriend on a daily basis, she will get worried about me because that is our main method of communication.'
(Matt)

Furthermore, many people use ICT to explore new ways of creative imagination, using different kinds of expression, such as visual tools and graphics, films, or social games. If the human being is to be conceived as 'homo ludens', the 'playing animal', exploring himself or herself in creativity, ICT offer many opportunities in that respect.¹⁵² However, individuals, especially children and adolescents, are exposed to so many options that they need to be educated in a 'reflective' and responsible use of ICT including the use of text messaging and 'twitter'. One new problem created by

¹⁴⁹ Cf. for an overview K. Rannenberg, Royer, D., Deuker, A., ed. The future of identity in the information society. Challenges and opportunities (Berlin: Springer, 2009).

¹⁵⁰ This term embraces the different ways a person manages himself or herself in the world wide web, i.e. with respect to digital signatures, accounts, traces, etc. Cf. among others Phillip J. Windley Digital identity, 2005. .

¹⁵¹ For an overview, cf. Paul Ricoeur, *Oneself as another* (Chicago: University of Chicago Press, 1992).

¹⁵² More and more companies are creating new virtual games in order to train their employees on specific points, in putting them in professional situations.

ICT from a psychological perspective is, for example, cyber-addiction.¹⁵³

This first area of ethical concern that needs to be addressed in further research is what we call the change in the personal and social identity. Being shaped and shaping one's identity in the digital era means, for example, that a person's self-perception is likely to change when identity markers such as age, gender, ethnicity, language and culture do not constrain individuals in creating their social identity. When engaging in social relationships on the web, individuals can choose and actually create new identities, from the use of pseudonyms to the invention of whole characters in online communities. Offline and online identities may vary radically, although both aspects are integrated in one self-concept. While the new narrative construction of identity may well be experienced as liberation from social ascription, it changes the very nature of our personal identities, and as such it needs to be addressed.

'We should not forget that interactive media are based on a computer, which is not a human being. We can write e-mails to friends, buy online without entering a store, chat with unknown people, maybe fall in love with unknown people all without moving from our chair. We can even forget about the outer world, the real one. All this, though, is very different from a real chat with a friend, a day of shopping, and a first date. This is, as far as I am concerned, the biggest risk about the spread of interactive media: losing contact with the world around us. We must not forget that a computer will never be able to replace personal relationships. After all, we all need to interact with real people and places. The emotion that derives from facing such masterpieces as La Gioconda could never be replaced by the most detailed virtual tour of the Louvre. In the same way, a real hug or smile will always transmit emotions that are impossible to feel through an apathetic computer screen.' (*Sophia*)

¹⁵³ A recent study analyzes the fine line between adolescents' self-assurance and self-exploration via ICT, and addiction. It defines Internet-addiction in the following way: 'In terms of time, an Internet addiction is commonly defined (Beard & Wolf, 2001; Young, 1998) as use of the Internet for at least 38 h each week. In the current study, based on participants' self reports about their daily use of the Internet, it seems that 6% of these adolescents meet that criterion. This rate fits evaluations made among other samples of adolescents world-wide (Cao, Su, Liu, & Gad, 2007). Cf. Israelashvili, M., et al., Adolescents' over-use of the cyber world – Internet addiction or identity exploration?, *Journal of Adolescence* (2011), doi:10.1016/j.adolescence.2011.07.015

The fluid self: The effect on the concept of personal identity has been described in the context of social studies that examine the de-centred self, together with a certain tendency of the 'fluidity' of modern social relations.¹⁵⁴ The digital self, too, can be described in this line of thought. Its relevance for ethical reflection lies in its impact on the traditional concepts of 'authenticity' and 'autonomy': fluid or hybrid identities may threaten the consistency and continuity that has been considered to be crucial for the concept of a practical identity, which ultimately relies upon a self that may not only identify with his or her actions but is also identified by others. Hence, the new possibilities for shaping one's own identity, constrained only by the features and rules of the programs one uses, make social relationships potentially insecure; ethical concepts such as trust, truthfulness or reliability may lose their function to create spheres of belonging — while at the same time enforcing short-term relationships that can easily be replaced.

In face-to-face relations, the 'creative' construction of identity is constrained by social perceptions that enable the persons involved to compare actions and statements with what they see and hear, or the knowledge they all share. The cyber-identity may be completely disconnected from such 'embodied' interactions, and even in cases where people engage 'authentically' in social networks, the lack of a shared location or space outside the web changes the way in which this new form of authenticity is spelled out. This not only raises the question of how the web-identity can be integrated in one's overall identity concept, but the 'fluidity' may also threaten the traditional understanding of autonomy as sovereignty. One consequence of the erosion of 'fixed identities' is that accountability for one's actions has to be newly spelled out.

Identity and ICT devices: On a different level, ICT blur the distinction between the concept of an embodied self — a self that has a body and at the same time is embodied — when several body parts are replaced by computer-controlled devices, and the concept of inter-personal interaction, when, for example, robots are designed to care for human beings, as, for example, with care for persons suffering from dementia, or persons with disabilities. Though there are many good reasons to introduce these devices as complementary ways to attend to people's needs, the emotional responses create new interactions and new forms of attachment that need to be scrutinised.

¹⁵⁴ Cf. for the concept of identity as 'fluid' or 'liquid': Zygmunt Baumann: *Liquid Life*. Cambridge: Polity Press 2005.

Ambient Assisted Living and the Elderly

Europe is facing a significant social and economic challenge, brought about by an unprecedented demographic change. Projections by EUROSTAT estimate that by 2060, 30% of all EU citizens will be over 65 and the number of people over 80 will more than double from 5% to 12% over the same period. While gains in life expectancy are to be generally welcomed, such gains have important implications for health and long-term care systems in Europe. As a result of our ageing population, it has been projected that healthcare spending will rise by between 1% to 2% of the GDP in most Member States in the period 2008-2060; an increase of approximately 25% of current spending levels. In addition to the increased costs of caring for our older family members, there is the added complication of fewer carers available. By 2060, there will be two persons aged 15 to 64 for every person aged 65 or more, compared with four persons to one in 2010. Thus, many Governments have become active in supporting innovative ICT solutions to assist in the delivery of high-quality cost effective health and social care provisions. For example, the European Union has an action plan on ICT and Ageing, which aims to support active ageing. The emergence of new types of mobile and embedded computing devices, developments in wireless technologies and smart sensors, provide the tools to develop innovative applications to assist older people to maintain or improve their quality of life and to facilitate their desire to live independently in their own homes. Smart homes address the promotion of independent living by using assistive technologies for higher quality of daily life, which aims to maintain a high degree of autonomy and dignity of the older person. Smart homes are typically equipped with a large amount of networked sensors which collect lifestyle pattern data, which are analysed regularly and the patterns recorded thereby building up a picture of the user's everyday activities. If a deviation from the normal pattern is detected e.g. not getting out of bed, an alert is issued to the user and in the case of no response, the alarm is raised via an automatic telephone message. Sensors can also be linked through an intelligent network to cut-off devices which can enhance safety of the occupant(s) e.g. if excessive heat is detected in the kitchen, the stove is automatically switched off.

Wireless technology can be extended to wearable devices to monitor people 24h a day both inside and outside the house. Items of jewellery such as bracelets and watches worn by Alzheimer patients can be GPS-enabled and can identify the location of the individual if they get disoriented and wander off. The bracelet/watch automatically detects any departure from a security zone, which is pre-determined by the patient's family or caregiver. More recently, wireless technologies are allowing doctors and carers to continuously monitor the health status of the elderly person. For example the smart shirt is a wearable T-shirt which consists of integrated wireless sensor nodes designed to collect physiological data such as heart rate, electrocardiogram results, respiration and temperature. This information can then be transmitted wireless to a base station along with the geo-location of the wearer which can be accessed by health care providers.

Alerts can be generated in response to signs of clinical deterioration thereby allowing for early intervention. Robotics has been recognised as a technology of potentially key importance in helping the growing elderly population with day-to-day tasks as well as communications with family members. Robots which can aid in feeding, dressing, bathing and reminding older people to take their medication are already in use. Beyond the service robot, new developments in the field of human-robot interaction are aimed at alleviating loneliness, and assisting in cognitive function. The National Institute of Advanced Industrial Science and Technology in Japan have developed 'Paro', a robotic baby seal which stimulates behaviour of a real pet and is used to provide companionship for those with dementia. Interaction with a robotic dog resulted in cognitive gains, specifically increased communication in older subjects with dementia. Information and communication technologies are also being utilised to encourage social interaction in older populations who may have reduced mobility and fewer opportunities for social contact. In 2007, 41.2% of women and 19.5% of men aged over 65 were recorded as living alone in the EU, thus videoconferencing and 3D calls using hologram technology will become increasing important in supporting older people in maintaining their social links with family and friends, thereby reducing a sense of isolation and exclusion.

The potential gains in autonomy and independence for older people, which can be harnessed through ICT is not without its' challenges. Despite significant decreases in the cost of computing over the last 20 years, introductory costs of technologies described above are relatively high. This raises the issue of e-inclusion and whether it is possible to ensure accessibility to all user groups. In addition, research has shown that older people are reluctant to adopt technical solutions facilitating independent living. This is related to a number of issues, including the complexity of using the technology, the cost, the lack of perceived usefulness and the stigmatisation of not being considered capable of caring for oneself. Heretofore, work in the ambient assisted living area has been largely concerned with technical feasibility; there is however a growing recognition that a more user-centred model is now required.

Ethical questions relating to privacy and dignity also need to be addressed. While continuous monitoring of homes and human activity can offer a safer environment for older people, many are wary of constant surveillance and the lack of control over data collected. Solutions proved to overcome these concerns include collecting and processing data on a local level, with the data being shared only if an emergency situation is detected, at which point the information could be released to health-care workers and/or carers. The situation is more complex in the care of older people with cognitive impairments who may not be in a position to participate in the decision making process around privacy settings.

Technical solutions should not violate an older person's dignity and it is critical that ICT serves to augment, rather than replace, human interaction. Concerns have been expressed that dependence on assisted living technologies could further serve to isolate older people, eroding their social connectedness. In the field of robotics there have been warnings that the presence of robots in the home could risk leaving the elderly in the care of machines without sufficient human contact. These essential questions will be considered in the context of the EU Ambient Assisted Living Joint Programme which runs from 2008-2013.

Identity and time: Traditionally, identity is not only

considered 'embodied' in the way described above, but also as identity over time. In the 'digital identity' concept, this concerns questions of identification. But in the broader perspective, the whole concept of identity-over-time may change considerably: On the one hand, time becomes an unreliable source of identification: statements, images or entries in social networks may well be taken as quasi-present representations of a person's self-image, while they may in fact be only a fragment of the past that a person would not consider important for his or her contemporary way of thinking or living. The distinction between synchronic communication and diachronic narrative is, therefore, easily blurred when entries or profiles are stored for a potentially very long time, and can be used by others outside of their original context.

Facebook now allows its members to store a life story and hence structure their entries in a diachronic manner. Memory and forgetting are complementary concepts for personal identity: without some forgetting and the necessary selection process in giving meaning to one's identity, the creation of an identity of the self (ipse) becomes more and more dependent on the socially ascribed 'markers' of identification (idem). As has been stated with respect to the legal initiative of the 'right to be forgotten', however, the web seems to 'never forget'.¹⁵⁵ The ethical question with respect to identity concepts, then, is how it affects one's self-relation and social relations alike over time — there are signs that the impossibility of 'deleting' a part of one's life story from the collective memory of the web may create an unforgiving culture, either with respect to employment or social forms of shaming, or with respect to surveillance policies.¹⁵⁶

¹⁵⁵ Cf. Viktor Mayer-Schönberger, *Delete: the virtue of forgetting in the digital age* (Princeton: Princeton University Press, 2009). The group acknowledges that the term the 'right to be forgotten' is used to call attention to this difficulty of the traces a person leaves without being able to delete them. Nevertheless, the term as such seems unfortunate as it easily alludes to the forgetting of a person, which is contra to its intention.

¹⁵⁶ As an example, Mayer-Schönberger tells the story of a woman who was denied immigration to the US because it could be proved that she had taken drugs in her adolescent years. Adults by now regularly warn their adolescent children about the images they post on facebook, because future employers scan the Internet for purposes of informal profiling. The unforgetting memory of the Internet thus can easily be 'unforgiving'.

Identity theft is one of the most prominent forms of cybercrime. Techniques such as phishing and pharming are used, luring users to fake websites which look legitimate, and where users are asked to enter their personal information. This could include e-mail addresses, username, passwords, credit card details and other information criminals can use to 'steal' another person's identity. This information can then be used online to open bank accounts, apply for loans and buy goods. Due to the insidious nature of the crime, victims may not become aware of the fact they have been targeted until the impact becomes severe. In 2010, Albert Gonzales, the ringleader of a group of hackers, was sentenced to 20 years in a US court for the theft of 130 million credit and debit card details from US retailers, used for fraudulent transactions resulting in \$200 million in losses.

As public awareness about the dangers of identity theft increases, so too does the sophistication of the phishing techniques employed. There have been reports of cyber criminals exploiting the goodwill of people in response to natural disasters. Following the earthquake in Haiti in 2010, emails purporting to be from charities directed donors to fake websites where donations made using credit cards were deposited in accounts controlled by criminal entities.

3.1.4 Individual Identity and Social Identity in ICT.

The second area the EGE considers as requiring further examination is the impact of ICT on the relation between individual identities and social communities and group identities. While scholars easily agree that individuals develop values and convictions in relation to others, Internet platforms and social networks may also reinforce group identities. When people can — and will — choose between different sources of information, and when companies profile their consumer habits, the two practices combined easily enforce a selective perception of the 'world' as it is presented in the Internet. As a result, the individual's social horizon is actually narrowed.

Another example of an ethically important change in the relation between the individual and the social sphere is the way in which social networks shape the concept of friendship and community — when one can easily have hundreds of 'friends' in a social network with whom one barely shares more than a loose sense of belonging to the same Internet community, one of the most important moral institutions, the personal

relation and interaction between individuals who know each other, share interests and shape personal responsibilities, is radically re-interpreted.¹⁵⁷

The British Medical Association alerts to the ethical-professional problems coming from the use to TWITTER.

And FACEBOOK advising medical doctors on the risks of having patients and "friends" in Facebook and Twitter mainly informal commentaries, exchange of patient's photos, discussion regarding their professional work especially with sensitive data.

Furthermore, ICT may easily 'mainstream' social patterns, beginning with the languages used to communicate, through to cultural patterns such as gender roles (even though these may be actualised by persons of another sex), and social norms of various kinds. Ethically speaking, the Internet creates the space not only for creative social relations but also for new collective identities that are gained or maintained by re-introducing forms of inclusion and exclusion. Disrespect and discrimination of 'other' groups would then be an extreme and blameworthy form of 'identity politics' that potentially threatens any collective identity.¹⁵⁸ Here criminal practices like explicit discrimination or 'hate speech' must certainly be addressed by international cooperative legal regulations but regulation will not prevent practices of social stigmatisation.

3.1.5 The Concept of Moral Identity in ICT Domains

The third area the EGE wishes to highlight with respect to individual identity concepts is the concept of moral identity. Moral identity entails the interpretation of accountability for a person's actions on the one hand, and the integration of moral values in one's identity. For the European Union, this means that the European values need to be communicated to the citizens, and interpreted in view of ICT, as in a first step suggested in this EGE Opinion. For example, what should count as a *responsible use of personal data* from the perspective of the individual is not easily determined on the one hand, when

¹⁵⁷ Aristotle addressed friendship as mutual care between equals; as such it has been conceptualised frequently throughout the history of moral philosophy and moral theology.

¹⁵⁸ This is not specific to ICT communities and group identities; however, ICT evoke new forms of such identities.

on the other hand, companies continuously expand the means to profile citizens and use multiple initially unlinked databases for this purpose (cf. Part One of this Opinion, Data mining), and countries are not transparent about their surveillance practices.¹⁵⁹ Many people make data available for what is thought to be one purpose ignoring or not realizing that they have implicitly or even explicitly agreed to specific marketing strategies that are used for completely different purposes.

Moral identity, however, involves more than protecting one's own rights with respect to others or the state; it also concerns the responsibility for a 'decent' civil cyberspace. Bullying of individuals in social networks will not disappear through legal regulation; individuals need to step forward and protect others against bullying, but they also need to know how to act in such cases. Since in principle everyone is vulnerable to disrespect, the EGE emphasizes that the Internet is not an ethically neutral sphere but a sphere of social interaction that necessarily creates values and norms, so that much effort must be put in communicating the European values and normative principles of action, from the respect of dignity and rights, to non-discrimination and particular protection of vulnerability.

Cyberbullying

The ease of access to powerful communication tools such as social networking sites, email and internet enabled smart phones are allowing young people to connect with each other and engage with society in ways previously unimaginable. Parents report that 75% of 6-17 year olds in the 27 EU member states use the internet, and 63% of children own a mobile phone. This increases to 94% in the 15-17 year old group. Sixty percent of 9-16 year old internet users in Europe go online on a daily basis, spending an average of 88 minutes online that increases to 118 minutes on 15-16 year olds. Thus, engaging in social media constitutes a routine activity for our children and research has shown that there are many positive benefits including enhanced communication and technical skills. At the same time, we are witnessing how the anonymous, instant and far-reaching communication capabilities have afforded young people

an opportunity to harass and intimidate each other. While bullying is not a new phenomenon, the ways in which it happens are changing. Several definitions of cyberbullying can be found in the literature, Patchin and Hinduja define cyberbullying as 'wilful and repeated harm inflicted through the use of computers, cell phones and other electronic devices'. Essentially, cyberbullying involves sending threatening messages (by text or e-mail), posting derogatory comments, or circulating false rumours on social networking sites. Cyberbullies can use a variety of online settings to physically threaten or intimidate their peers. Cyberbullying differs from traditional bullying in that it can take place outside of school and on a 24hour, seven day a week basis due to the accessibility of the internet and mobile phones. This kind of bullying can reach a wider audience and has a permanence not normally associated with traditional bullying (posts on social media site can be difficult if not impossible to remove). Cyberbullying also offers the perpetrator anonymity which engenders a confidence to commit hurtful acts. Easily maintaining anonymity in cyberspace has been found to be one of the triggers of cyberbullying. Without any direct contact with victims or any feedback, cyberbullies may have difficulty appreciating the magnitude of harm their actions are causing, and have fewer opportunities for empathy or to express remorse.

Recent research has attempted to establish the prevalence of cyberbullying amongst children and teenagers and findings suggest that approximately 10-35% of students have been victims of cyberbullying. In a recent UK study, 18.4% of young people between 10 and 19 reported that they have been bullied by perpetrators using the internet or mobile phone. The EU kids online study which interviewed 25.000 European children across 25 countries documented that 6% of 9-16 year olds have been bullied online. While there is disagreement about whether one or other sex is more likely to be involved in cyberbullying, and the age of cyberbullying, there is a significant overlap between being a victim and being perpetrator. A common finding in studies is that the majority of victims do not tell and adult about the difficulties they are experiencing. This has been attributed to the fact that many parents are not as digitally savvy as their children and there is a fear amongst young people that in response to such reports, parents will withdraw their internet/phone privileges. Cyberbullying is an issue of which many parents are aware

¹⁵⁹ As the group has stated in the beginning of this Opinion, the EGE does not address questions of security but will turn to this in a later Opinion.

and concerned about. According to the 2008 Flash Eurobarometer survey, 54% of European parents are worried that their children could be bullied online, with 61% reporting that they stay close by in order to monitor their child's usage of the internet.

Victims of cyberbullying exhibit signs of emotional distress, low self esteem, depression and anxiety. These children complain of headaches and stomach aches more frequently than children who are not cyberbullied.

Victims report being frightened to attend school, leading to concerns that school absences will inevitably lead to a detrimental effect on academic performance, which could have life-long consequences. In extreme situations, cyberbullying can contribute to cyberbulicide, a recently coined term to refer to suicides influenced directly or indirectly by this form of bullying. There have been several high profile cases reported in the media of young people taking their own lives, in part because of harassment and mistreatment mediated through the internet. Cyberbullies themselves have also been shown to have low self-esteem, are anxious, have difficulty in making friends; all risk factors for suicide.

Efforts aimed at counteracting cyberbullying range from legislation to awareness campaigns. Twenty-five states in the US have enacted specific cyberbullying legislation, with seven states classifying cyberbullying as a crime. This approach has been criticised by some commentators, as it is clear that many cyberbullies are suffering emotional distress themselves and labelling them as criminals is unlikely to be helpful and may impact on their future educational progress. Education of young people, their teachers and parents is thought to be crucial in the prevention of cyberbullying. An important first step is to enable young people to explore their attitudes to what constitutes appropriate and inappropriate content to share. Education can enforce social norms about how young people engage with their peers in cyberspace i.e. in a respectful manner. Our children also need to be advised about categories for reporting incidents of cyberbullying and how to safely use the internet. To this end, the European Commission launched the Safer Internet programme 2009-2013, with the aim of empowering young people online by providing them with the information, skills and tools to deal with risks they may encounter in this virtual world.

3.2 Privacy as a Fundamental Right

In the 1950s, Hannah Arendt was one of the first scholars to observe the political importance of privacy.¹⁶⁰ Arendt's defence of the importance of the private sphere warns about dangers arising from the erosion of the private, a situation which some consider as deriving from the use of ICT as communication tools.

Ethically speaking, respect for freedom of the one person raises not only the question of violation of rights of another person but also the possibility of violating the person's own dignity. For example, if individuals decide to share their own private and intimate moments with the web community (think of recording and putting on the web explicit sexual images), can we say that their actions are ethically wrong because others may consider them detrimental to human beings' dignity? The advocates of freedom of expression would argue for the broadest possible notion of freedom of expression and autonomy, but they would have to contend with, for example, free circulation of extreme pornography (sodomasochism, sex brutality, etc.) by consenting adults.¹⁶¹ The opponents of this radical liberal expression of individuals' autonomy would, on the other hand, face arguments on censorship, on the ethical justification for the limitation of individuals' freedom, and the scope or limit of respect of ethical pluralism.

When individuals decide to share data that concern their own private sphere, their decision affects not only their own freedom but has implications, too, for all other users. As the example of online sex and/or pornography easily shows, a very 'liberal' interpretation of digital freedom may change the concept of sexuality, may shape social practices concerning sexuality, the body, gender norms, or the concept of beauty. The opportunities that technologies, especially in connection with the Internet, provide, may easily result in the erosion of privacy and, over time, also change the notion of social norms or the overall concept of the public sphere. Even though striking a balance between different rights, and the balancing of rights and social goods, is very difficult, linking the 'individual' rights to the impact on the community of

¹⁶⁰ Hannah Arendt, 1958, *The Human Condition*, University of Chicago Press.

¹⁶¹ Different is the debate on the ethics dimension of privacy protection for individuals not consenting to the sharing of their own data. But in this last case, the absence of individuals' consent rises questions related to subjects' right to self-determination and autonomy and then are ethically sensitive.

Internet users is an important step in assessing Internet governance. In this specific context, liberal versus more restrictive governance models are being proposed in the global debate over the ethics of Internet and the rights/values of individuals as citizens of the cyber-community.

Privacy has been conceived as an 'exclusion' device — as a tool to fend off the 'unwanted gaze'. However, by analysing the definitions of privacy it is clear that privacy has changed over time by giving shape ultimately to a right that is increasingly geared towards enabling the free construction of one's personality — the autonomous building up of one's identity, and the projection of fundamental democratic principles into the private sphere. A societal and academic debate has been taking place for some years now on the notion of privacy.¹⁶²

Some argue that *privacy* is a means of controlling information that should commonly be shared since in the web 2.0 e-privacy cannot properly be defended. This view, called 'post-privacy-movement', also advocates that actively giving up privacy would determine the flourishing of a personal and social virtue¹⁶³ based on people's freedom to introduce and share whatever data on their own lives they desire, including sexual behaviour/preferences. Also according to this view, such an approach should encourage people to cultivate more tolerance towards attitudes and behaviour of others. The opposite view states that the assumption that in the web 2.0 era it is difficult to guarantee privacy is not a sufficient reason to abandon the necessary protection of individuals' privacy. It states that a private sphere is a source where one is not required to immediately meet public expectations and conventional lifestyles. The two positions characterise the debate on both Internet governance and issues related to personal integrity and social communication.

3.2.1 Concerns Regarding the Current EU Legal Protection of Personal Data

According to a recent Eurobarometer (IP/11/742), 70% of Europeans are concerned that their personal data may be misused. They are worried that companies may be passing on their data to other companies without

their permission. 74% of Europeans think that disclosing personal data is increasingly part of modern life, but at the same time, 72% of Internet users are worried that they give away too much personal data, according to the Eurobarometer survey. They feel they are not in complete control of their data. This erodes their trust in online and other services and holds back the growth of the digital economy in general.

In the context of ICT development there is, therefore, a widespread public perception of significant ethical risks and legal uncertainty associated notably with online activity.¹⁶⁴ This is why it is time to build a stronger and more coherent data protection framework in the EU, backed by strong enforcement that will allow the digital economy to develop across the internal market, put individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities.¹⁶⁵

3.2.2 Safety of Personal Data

Increasingly, individuals upload their own personal data to the Internet¹⁶⁶ (social networks, cloud computing services, etc.). However, the European Directive on the protection of personal data does not apply to the individual who uploads data for 'purely personal' purposes or 'in the course of a household activity' (*the so-called 'household exemption'*).¹⁶⁷ Arguably it does not apply either to the organisation that provides the service, i.e. hosts and makes available the information uploaded by the individual (unless the service processes data for its own purposes) insofar as the service provider may not be deemed to be a controller. The result is a situation of lack of safeguards that may need to be addressed, particularly given the increase in the number of such situations. In this context, whoever offers services to a private individual should be required to provide certain safeguards regarding the security and, as appropriate, the confidentiality of the

¹⁶² Cf. the Flash Eurobarometer 241 on 'Information Society as seen by the EU citizens' (2008) and SPECIAL Eurobarometer 359 'Attitudes on Data Protection and Electronic Identity in the European Union' (2011).

¹⁶³ Other codes of conduct strictly distinguish between using public data (and making them public where this is deemed to be necessary) and, at the same time, protecting private data; cf. <http://www.ccc.de/hackerethics>.

¹⁶⁴ Special Eurobarometer (EB) 359, *Data Protection and Electronic Identity in the EU* (2011): http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

¹⁶⁵ Draft for a Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Version 56 (29/11/2011), 3.

¹⁶⁶ *The Future of Privacy*, p. 15-16.

¹⁶⁷ Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking, 5.

information uploaded, regardless of whether their client is a data controller.¹⁶⁸

3.2.3 Profiling and Data Mining

A consequence of the broad and flexible *concept of 'personal data'* is that there are numerous cases where it is not always clear whether individuals enjoy data protection rights and whether data controllers should comply with the obligations imposed by the Directive. There are situations which involve the processing of specific information which would require additional measures under EU law e.g. key-coded data, location data, 'data mining'.¹⁶⁹ 'Profiles', when they are attributed to a data subject, even make it possible to generate new personal data which are not those which the data subject has communicated to the controller. This future development of 'new data' (through data mining and profiling) should be taken into account when revising the Directive.¹⁷⁰

3.2.4 Sensitive Data

The processing of *sensitive data*, i.e. 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life', is currently already prohibited as a general rule, with limited exceptions under certain conditions and safeguards (Article 8 of the Directive) However, in the light of technological and other societal developments, there is a need to reconsider the existing provisions on sensitive data, to examine whether other categories of data should be added and to further clarify the conditions for their processing. This concerns, for example, genetic data and biometric data,¹⁷¹ which are currently not explicitly mentioned as a sensitive category of data.¹⁷² In order to guarantee lawfulness, personal data should be processed on the basis of the consent of the person

concerned. Consideration could be given to *broadening the situations where express consent is required*, currently limited to sensitive personal data.¹⁷³ However, it is doubtful whether the legal framework should require explicit consent as a general rule for all types of processing operations, including those currently covered by Article 7 of the Directive.¹⁷⁴ The controller should have the burden of proving that the data subject has given consent to the processing operation.¹⁷⁵

3.2.5 Giving and Withdrawing Consent

It would provide more legal certainty if the data protection legislative framework were to contain an express clause entitling an individual to *withdraw their consent*.¹⁷⁶ The same requirements including *unambiguous consent* apply both offline and online. As the risk of ambiguous consent is likely to be greater in the online world, this calls for specific attention. Unambiguous consent does not fit well with procedures to obtain consent based on inaction or silence on the part of individuals: a party's silence or inaction has inherent ambiguity. As a consequence of the requirement for consent to be *unambiguous*, data controllers are *de facto* encouraged to have in place procedures and mechanisms that leave no doubt that consent has been given, either on the basis of an express action carried out by the individual or by being clearly inferred from an action carried out by an individual. As a matter of good practice data controllers should consider putting in place relevant measures and procedures to show that consent has been given. The more complicated the environment in which they operate, the more measures will be necessary to *ensure that consent is verifiable*. This information should be put at the disposal of the data protection authority upon request.¹⁷⁷

¹⁶⁸ The Future of Privacy,18.

¹⁶⁹ Com (2010) 609 final, 5.

¹⁷⁰ Opinion of the Committee on industry, research and energy for the Committee on Civil liberties, Justice and Home Affairs on a comprehensive approach on personal data protection in the European Union, 11 May 2011, §7, Report of the European Parliament on a comprehensive approach on personal data protection in the European Union, European Parliament, 22 June 2011 (rapporteur: Axel Voss).

¹⁷¹ European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union, § 22.

¹⁷² Com (2010) 609 final, 9.

¹⁷³ Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions — 'A comprehensive approach on personal data protection in the European Union' *Official Journal C 181, 22/06/2011 p. 1 – 23 § 82*.

¹⁷⁴ Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, p. 37.

¹⁷⁵ Draft for a Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Version 56 (29/11/2011), 22 §30.

¹⁷⁶ Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, 37.

¹⁷⁷ Article 29 Data Protection Working Party, Opinion 15/2011

In the *online environment explicit consent* may be given by using electronic or digital signatures. However, it can also be given through clickable buttons depending on the context, sending confirmatory emails, clicking on icons, etc. Consent does not have to be recordable to be valid. However, it is in the interest of the data controller to retain evidence. Obviously, the strength of the evidence provided by a specific mechanism may vary, supplying more or less evidence of the consent. Consent that has been obtained through a clickable button with the identity of the individual supported by an email address only will have much less evidentiary value than a similar process, for example with recordable consent mechanisms. The need for strong evidence will also depend on the type of data collected and the purpose followed: an electronic signature will not be needed to consent to receiving commercial offers, but may be necessary to consent to the processing of certain types of financial data online.¹⁷⁸

Consent does not provide a valid ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent without detriment, especially when there is a clear imbalance between the data subject and the controller, e.g. in the employment sector. In this case, processing needs another legitimate basis, laid down by law.¹⁷⁹

3.2.6 Transparency

Transparency is a fundamental condition for enabling individuals to exercise control over their own data and to ensure effective protection of personal data. It is therefore essential that individuals should be well and clearly informed, in a transparent way, by data controllers about how and by whom their data are collected and processed, for what reasons, for how long, how it will be shared with others and what their rights are if

on the definition of consent, p. 23-25; See also Recommendation (2010) 13 of the Committee of Ministers of the Council of Europe to the member states on the protection of individuals with regard to automatic profiling of personal data in the context of profiling (23 november 2010), Section 3.6: 'When consent is required it is incumbent on the controller to prove that the data subject has agreed to profiling on an informed basis, as set out in Section 4'.

¹⁷⁸ Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, p. 26.

¹⁷⁹ Draft for a Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Version 56 (29/11/2011), 22 §§29-30.

they want to access, rectify or delete their data. Basic elements of transparency are the requirements that the information must be easily accessible and easy to understand, and that clear and plain language is used. This is particularly relevant in the online environment, where quite often privacy notices are unclear, difficult to access, non-transparent and not always in full compliance with existing rules. Where the data provider is based in a country other than that of the user, jurisdictional differences may have a profound impact on the way the data are handled. A case in point is online behavioural advertising, where both the proliferation of actors involved in the provision of behavioural advertising and the technological complexity of the practice make it difficult for an individual to know and understand if personal data are being collected, by whom, and for what purpose.¹⁸⁰

3.2.6.1 Mandatory Breach Notification

It is also important for individuals to be informed as quickly as possible when their data are accidentally or unlawfully destroyed, lost, altered, accessed by or disclosed to unauthorised persons. The recent revision of the e-Privacy Directive introduced a *mandatory personal data breach notification* covering, however, only the telecommunications sector. Given that risks of data breaches also exist elsewhere (e.g. the financial sector), the obligation to notify personal data breaches should be extended to other sectors. A consistent and coherent approach on this matter will have to be ensured even when the organisation breaching the confidentiality is not based within the EU.¹⁸¹

3.2.6.2 Managing One's Own Data

Individuals should always be able to *access, rectify, delete or block their data*, unless there are legitimate reasons, provided by law, for preventing this. These rights already exist in the current legal framework. However, the way in which these rights can be exercised is not harmonised. Moreover, this has become particularly challenging in the online environment, where data are often retained without the person concerned being informed and/or having given his or her consent. The example of online social networking is particularly

¹⁸⁰ Com (2010) 609 final, 6.

¹⁸¹ Com (2010) 609 final, 6-7; Article 29 Data Protection Working Party, Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments.

relevant here, as it presents significant challenges to the individual's effective control over his/her personal data. The European Commission has received various queries from individuals who have not always been able to retrieve personal data from online service providers, such as their pictures, and who have therefore been impeded in exercising their rights of access, rectification, deletion or blocking. *Such rights should therefore be made more explicit, clarified and, where necessary, strengthened.*¹⁸² The modalities for actual exercise of the rights of access, rectification, erasure or blocking of data have been improved (e.g. by introducing deadlines for responding to individuals' requests, by allowing the exercise of rights by electronic means or by providing that right of access should be ensured free of charge as a principle).

3.2.7 Right to Data Deletion

Any person should have a so-called '*right to be forgotten*',¹⁸³ which means that the data subject should have the right to ensure that their personal data will be deleted and no longer processed, where they have withdrawn their consent for processing or where they object to the processing of personal data concerning them. To tighten this up in the online environment, the right to deletion should also be extended in such a way that any publicly available copies or replications in websites and search engines should also be deleted by the controller who made the information public.¹⁸⁴ The European Commission has also proposed complementing the rights of data subjects by ensuring '*data portability*', i.e. providing the explicit right for an individual to withdraw his/her own data (e.g. his/her photos or a list of friends) from an application or service so that the withdrawn data can be transferred to another application or service, as far as technically feasible, without hindrance from the data controllers.¹⁸⁵

3.2.8 Special Protection for Minors

In the online context, children deserve specific protection, as they may be less aware of risks, consequences,

*safeguards and rights in relation to the processing of personal data. Children tend to underestimate risks linked to using the Internet and minimise the consequences of their behaviour.*¹⁸⁶ The lack of general rules on this in the existing legal framework leads to a fragmented approach and does not recognise the need for specific protection of children in specific circumstances, because of their vulnerability, and because it causes legal uncertainty, particularly as regards the way children's consent is obtained. Harmonising the conditions for allowing children and minors to exercise their rights at EU level, especially with regard to the age threshold, would certainly bring additional guarantees. It should also cover the requirement to use *online age verification mechanisms*.^{187,188}

In the context of *providing information to children*, special emphasis should be put on giving layered notices based on the use of simple, concise and educational language that can be easily understood. A shorter notice should contain the basic information to be provided when collecting personal data either directly from the data subject or from a third party (Articles 10 and 11 of the Directive). This should be accompanied by a more detailed notice, perhaps via a hyperlink, where all the relevant details are provided.¹⁸⁹

The interests of vulnerable adults would be better protected through additional provisions, specifically addressing the collection and further processing of their data. These provisions could cover the circumstances in which the consent of a representative or an authority is required, together with, or in place of, the consent of an incapable individual, and could extend to circumstances where it should not be possible to use consent as a basis for legitimising the processing of personal data.

¹⁸² Com (2010) 609 final, 7.

¹⁸³ The EGE prefers to use the expression '*right to data deletion*'.

¹⁸⁴ Draft for a Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Version 56 (29/11/2011), 25 § 47.

¹⁸⁵ Com (2010) 609 final, 8.

¹⁸⁶ Com (2010) 609 final, 6.

¹⁸⁷ There are different mechanisms and different thresholds. For example, age verification, rather than being subject to one single rule, could be based on a sliding scale approach whereby the mechanism to be used would depend on the circumstances, such as the type of processing (the purposes), whether particularly risky, type of data collected, data usages, (whether the data are intended for disclosure), etc.

¹⁸⁸ Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, p. 28.

¹⁸⁹ Article 29 Working Party, Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), 11 February 2009, p. 10.

Additional criteria should apply when the controller is established outside the EU/EEA with a view to ensuring that a sufficient connection exists with the EU territory and to avoid EU territory being used to conduct illegal data processing activities by controllers established in third countries. More harmonisation in regard to the obligation of controllers established in third countries to appoint a representative in the EU with the objective of giving more effectiveness to the role of the representative is recommended. In particular, the extent to which data subjects should be able to effectively exercise their rights against the representative should be clarified.¹⁹⁰

4. Sphere of Social Implications, Culture, Education and Environmental Protection

4.1 Social Inclusion in the Age of ICT

Rapid developments in, and the ubiquitous diffusion of, ICT increasingly means that to utilise many everyday services, one has to have access to ICT and the requisite skills and motivation to use the technology in order to fully participate in today's society. Digital inclusion is fast becoming a prerequisite for social inclusion. Thus, it is a matter of concern that despite the great strides made in creating the information society, there remains a 'digital divide' where due to age, gender, geographical location or socioeconomic status, there is unequal access to and use of ICT.

A large proportion of Internet users are young people,¹⁹¹ who are often not fully aware of the implications that may arise from their use of ICT. The commercial nature of social networks and the complexity of privacy protection, the difficulty of erasing data (including pictures and videos or participation in blogs) or the possible uncontrolled diffusion of data originally addressed to another cyber-user and then spread in cyber-space, are all examples of possible risks confronting Internet users.

¹⁹⁰ Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law, 31-32.

¹⁹¹ Economist Intelligence Unit. Closing Europe's digital divide. October 2008. http://graphics.eiu.com/upload/Intel_Digital_Divide.pdf. accessed on 2 December 2011.

Digital Divide Best Practice

A diverse range of initiatives have been undertaken in different countries with a view to closing the digital divide that exists between different sectors of society, e.g. due to issues relating to age, socio-economic status, geographic location and disability. Some of these initiatives have proven successful in helping to minimise the digital divide.

South Korea has emerged as one of the foremost countries in alleviating problems associated with the digital divide, with the Digital Opportunity Index, which measures the degree of balance within the information society, ranking it first among Organisation for Economic Co-operation and Development (OECD) countries for the last three years. South Korea took an assertive, highly focused and ultimately very successful approach to deal with the digital divide issue. This began in the late 1990s with the establishment of a specific body dedicated to this task, namely the Korean Agency for Digital Opportunity and Promotion (KADO). The KADO's role was to provide easy and affordable access to ICT services (e.g. IT education, the Internet and email) to individuals with disabilities, the elderly, low-income families and to those in rural communities. Since its inception the KADO has provided these services to over 10 million Koreans. In addition to establishing the KADO, the government also introduced specific legislation [i.e. the Digital Divide Act (2001)] and has produced two comprehensive 'Master Plans' to bridge the digital divide in 2001 and 2005 respectively. Given the success of its initiatives at a national level, South Korea has changed focus to provide more support to global informatisation and bridging the digital divide internationally, particularly within developing countries. As part of this change the KADO has been merged with the National Information Society Agency (NIA). The NIA now runs a number of initiatives, such as the IT and Policy Assistance Program and Korea IT Volunteers, with other countries to provide expertise, experience, training, technical assistance and best practice as part of national IT developments in these partner countries.

The One Laptop per Child project, which began in 2007 aims to provide the opportunity and resources to children to help facilitate their 'self-empowered' education in low-income countries. To date

the laptops have been supplied to over 2.5 million children and teachers in 42 countries, predominantly through government-led programmes. The success of this programme relates to the specific design and utility of the laptops themselves (i.e. XO laptops), particularly given the practical issues associated with ICT services in developing countries, such as unreliable or nonexistent electricity supplies and poor Internet connectivity. For example the XO laptops are inexpensive, powerful, robust, solar-chargeable, low-power and can interconnect wirelessly to create local networks. In addition, the laptops also utilise free and open source software.

In an effort to improve IT literacy in older people, 'The Log On, Learn Programme', a collaborative Irish project involving Intel, Microsoft and An Post (Ireland's national postal service), began in 2008. The project involves a secondary level students acting as mentors ('buddy') to an older person from their local community and teaching him/her basic IT skills (e.g. how to use a computer, word processing and Internet applications). The students benefit through the development of their research, marketing and teaching skills as well as through the interpersonal interactions, which foster intergenerational solidarity. To date more than 165 schools have enrolled, providing this one-to-one mentoring to over 3000 individuals. However, it is envisaged that with further roll out the programme has the capacity to train up to 30000 individuals.

In Australia a digital divide has been identified between rural and metropolitan areas. One initiative that attempts to address the digital divide in rural Victoria is the *access@schools* programme. This programme provides people in remote and rural areas with free or affordable access to the Internet and ICT facilities through local schools outside of school hours. The programme was originally launched in 2001 and provided ICT access to 12000 citizens through 145 schools. In light of the success of this pilot project further funding was provided through the Commonwealth Government to expand the programme.

In an effort to create a digitally-inclusive society, the Society for the Physically Disabled in Singapore, established the Infocomm Accessibility (IA) Centre as an innovative training facility for individuals with physical, sensory and developmental disabilities.

The IA Centre provides industry-relevant ICT training and IT-related apprenticeships as well as an assistive technology loan library, with a view to improving both the independence and employability of those with disabilities.

What these projects serve to illustrate is the importance in having both access as well as the knowledge, skills and supportive organisational and societal structures in order to achieve digital inclusion for all.

The International Telecommunication Union (ITU),¹⁹² the United Nations' agency for ICT, publishes comprehensive ICT statistics from 152 countries on an annual basis. In its 2011 report it notes that in all countries from which data are available and without exception, Internet usage is higher amongst individuals with a secondary or tertiary educational qualification than those with a lower level of education.¹⁹³ In Europe only 10 % of people over the age of 64 use the Internet, as compared to 73 % of those between 16 and 24 years.¹⁹⁴ While age itself is not a barrier to using digital technologies, older people tend to face other obstacles such as cost, skills, disability access and attitude, as well as lack of awareness and understanding.^{195,196}

On the basis of these considerations the definition of policies which optimise market and socio-economic indicators inputs should not neglect, *inter alia*, the need to guarantee alternative access to services by people who, owing to socio-cultural (or simply for individual choice) factors, prefer conventional non-digital tools to make their purchases or access their rights as members

¹⁹² <http://www.itu.int/en/about/Pages/overview.aspx>, accessed on 1 December 2011.

¹⁹³ ITU. Measuring the Information Society 2011 http://www.itu.int/ITU-D/ict/publications/idi/2011/Material/MIS_2011_without_annex_5.pdf, accessed on 1 December 2011.

¹⁹⁴ Economist Intelligence Unit. Closing Europe's digital divide. October 2008. http://graphics.eiu.com/upload/Intel_Digital_Divide.pdf. accessed on 2 December 2011.

¹⁹⁵ E-communications household survey by the European Commission (2011). http://ec.europa.eu/public_opinion/archives/ebs/ebs_362_en.pdf, accessed on 2 December 2011.

¹⁹⁶ Peacock SE, Kunemund H. European Journal of Ageing 2007; 4:191-200.

of a community (particularly regarding political participation or health-related services¹⁹⁷).

The list of possible digital gaps includes several vulnerable groups: older generations having grown up in a pre-Internet era; less educated people; marginalised groups within the European Union; and, from a global viewpoint, less (digitally covered) countries or regions in the EU and elsewhere in the developed and the developing world. All gaps can be described with regard to the capacity of using ICT in everyday life, but also with regard to having fewer educational or financial resources to compete with those who up to now successfully have used ICT to pursue their political, commercial, scientific or other goals.

4.2 E-Government

The UN E-Government Survey of 2010 begins with the following statement: 'E-government is a powerful tool for human development and essential to the achievement of the internationally agreed development goals including the Millennium Development Goals. Many countries are experiencing its transformative power in revitalizing public administration, overhauling public management, fostering inclusive leadership and moving civil service towards higher efficiency, transparency and accountability. They recognize e-government as a way of realizing the vision of a global information society. In contrast, countries slow to embrace e-government tend to remain mired in the typical institutional pathologies of supply-driven services and procedures, remoteness between government and citizen, and opaque decision-making processes.

Society experiences rapid, continuous and incessant change. The drive to invent, reinvent and discard almost continuously is a unique human pursuit in an effort to deliver progress and prosperity for humankind. E-government is aimed at facilitating this change without 'leaving anyone behind' who wishes to participate in public social and/or political affairs. ICT are certainly welcome on all the different levels of individual and

cultural expression, social interaction and political participation, but from the perspective of governments it is imperative that the rights of those who wish to not take part in the ICT revolution must be respected. While these citizens' rights are certainly not to be interpreted as trumping innovation and progress in ICT, a responsible implementation means that their needs are as good as possible accommodated. As a consequence of not choosing to incorporate ICT into their daily lives, it is likely that individuals will increasingly see their choices limited in the digital age. Therefore, it is important that in areas where society places obligations on such individuals e.g. submitting tax returns, mechanisms unrelated to ICT are in place to help all citizens to meet their obligations.

4.3 Education

In the domain of education, e-learning-tools need to be carefully assessed in the way they transform European traditional face-to-face-communication between teachers and students. The style of learning and communicating information seems to be changing through the influence of ICT, especially web-based information and educational tools. Searching rather than reading becomes the method of choice for building up literacy skills. Educational regimes and institutions will have to improve access to information on the one hand and, on the other hand, build a literate identity for individuals but also for communities and for organisations. It seems clear that we are facing profound transformations in our patterns of processing information and shaping our educational infrastructure.

4.3.1 Culture

ICT is a domain where every culture may express itself, in its peculiarity. In a globalised world, every culture may communicate through ICT with any other, in a very rapid way; everyone has the chance to take part, actively, in multicultural life. The free flow of information gives an opportunity for increasing intercultural dialogue, and boosts individuals' chances of sharing trans-cultural knowledge and broadening their own outlook beyond cultural boundaries. ICT may enable the protection of minority languages and cultures where efforts are made for those within the cultures to interact with one another. On the other hand ICT may tend to make cultures more uniform, assimilating the differences (e.g. using one language, English) and aligning the standard of communication in all countries of the world, with the risk of affecting cultural diversity.

¹⁹⁷ Some have advocated that e-health, tele-medicine and e-care may offer better opportunities of contact between medical or care staff members and patients, especially in regions where adequate health care cannot be provided, e.g. in rural regions. Nevertheless, some have also advocated that intensified application of ICT in medicine and health care is problematic towards the patient-doctor relationship, the online pharmacy and risks of misuse of drugs, the e-driven informed consent procedures, e-prescriptions, etc.

4.4 E-Health

The growth of new health information technology opportunities brings a responsibility to design interoperable, easy to use, engaging, and accessible e-Health applications that communicate the right information needed to guide health care and health promotion for diverse audiences. Moreover, the wider deployment of e-Health raises certain ethical and regulatory concerns. One of the fundamental challenges lies in ensuring that patient data remain confidential and secure in order to build trust and confidence in e-Health systems. Appropriate measures should be put in place that can be reasonably expected to safeguard the security and integrity of personal medical information.

Heretofore the clinical encounter between doctor and patient has been physical and concerns have been expressed that the move to a virtual environment could undermine the doctor-patient relationship, especially amongst older populations. Other commentators have pointed to the positive collaborative aspects of this sort of interaction, with patients developing a greater sense of responsibility, accountability and knowledge allowing them to participate in medical decision-making.¹⁹⁸ There are however variations in patient preferences and many patients are happy to defer to their doctors' decisions.¹⁹⁹ The relationship between doctor and patient is embedded in values of commitment, trust, privacy, confidentiality and responsibility, and it is vital that e-Health should facilitate the realisation of these principles.

There is an enormous amount of medical information to be found on the Internet. This information, however, tends not to be screened, edited or assessed for accuracy and can be inexact or even misleading. It can be difficult for patients to judge the quality of the information presented on the many websites that offer health information and advice, and patients can also experience difficulties in putting the information into the context of their specific clinical situation. Both the Italian National Bioethics Committee²⁰⁰ and the Nuffield Council²⁰¹ have recommended that all websites

containing health information should develop quality criteria including the basis of the information, the authors, funding arrangements, and how any personal data will be used, and that ideally such websites should seek accreditation from recognised schemes.

The distribution of the benefits and risks of e-Health must be carefully considered. It is well established that those with lower educational and income levels have worse health. If more healthcare services are shifted to new media, we could leave behind those with limited health literacy or access to technology. Ensuring that new technologies empower people, rather than exacerbate health inequalities, needs to be at the forefront of the exciting developments in this area.

4.5 E-environment

The influence of the use of ICT on the environment is complex and may have positive and negative consequences. ICT may provide tools for the protection of environment: monitoring environmental issues, managing urban environment systems, communicating environmental knowledge, disseminating information to the public, stimulating active participation of citizens, enabling efficient use of resources, reducing the consumption of energy and essential natural resources (reducing the consumption of paper through electronic and paperless communication), bettering the use of natural resources. Examples include using technologies to improve practices in agriculture including minimisation of chemical usage, monitoring air and water pollution, prediction of environmental changes permitting action to be taken to protect where appropriate and improving the efficiency of the energy, transportation, and goods and services sectors. At the same time, the sustainability of these technologies must be managed to avoid unintended consequences such as increased consumption of scarce resources and a very large increase in energy usage and environmental damage from electronic waste (e-pollution).

Although ICT require energy resources, they may offer many ecological opportunities. ICT may have positive and negative consequences on the environment and on environmental sustainability. The positive impact of ICT is generally considered very high, so that it may balance some negative aspects. ICT may improve environmental

¹⁹⁸ Wald HS, Dube CE and Anthony DC. Patient Education and Counseling 2007;68:218-224.

¹⁹⁹ Levinson W, Kao A, Kuby A et al. Journal General Internal Medicine 2005;20:531-535.

²⁰⁰ http://www.governo.it/bioetica/eng/pdf/ethics_health_and_new_information_tecnologies_20060421.pdf, accessed on 19 January 2012.

²⁰¹ <http://www.nuffieldbioethics.org/sites/default/files/>

[Medical%20profiling%20and%20online%20medicine%20%20the%20ethics%20of%20personalised%20health-care%20in%20a%20consumer%20age%20\(Web%20version%20-%20reduced\).pdf](#), accessed on 11 January 2012.

performances and may offer tools for the protection of the environment in many different ways:

- *Direct effects*, which arise from the design, production, distribution, maintenance and disposal of ICT goods and services by the ICT industry²⁰².
- *Indirect effects*, which arise from the application and use of ICTs in society, in government and public institutions, in research and scientific communities. ICTs may offer promising solutions for enhancing our capacity to give warning of, predict and track environmental changes and disasters, developing appropriate management that are able to minimize risks and maximize adaptation strategies. Of course we can not predict, but enhance the ability to anticipate change designing the future ecological scenario, in order to be in a better position to adapt to it²⁰³.
- *Systemic effects*, which arise from changes in social and organizational structures enabling the availability, accessibility, application and use of ICT goods and services. In this aspect ICTs may contribute to reducing pollution and the consumption of energy²⁰⁴. In this sense, the choices of organizations and communities about how to use ICTs to change their

structures will play a potentially significant role in determining whether there is a successful global response to the challenge of environmental issues.

At the same time, ICTs may have a negative impact on the environment: consumption of energy, not fully recyclable apparatus' and technology (toxic e-waste pollution). Electronic waste has become a major issue of digital ethics. It deals with the ICT devices (hardware waste and recycling of old computers) that already today have devastating consequences on the environment.

Intelligent Transportation Systems

Information and Communication Technologies (ICT) are in the early stages of transforming transportation systems. Intelligent Transportation Systems (ITS) are generally regarded as the integrated application of computer, sensor, electronics and communication technologies to deliver a safer, more efficient and more sustainable transport system. ITS can empower commuters, road network providers, and actual devices, such as traffic lights with actionable information, thereby facilitating better informed decisions which can help save lives, time and money. Future developments in this area are likely to focus on thing-to-thing, vehicle-to-person, vehicle-to-vehicle and vehicle-to-infrastructure communications, the so-called 'internet of things'. The basic concept involves the pervasive use of Radio Frequency Identification Devices (RFID) tags, sensors, actuators, and mobile vehicles, which through unique addressing systems, are able to communicate with each other and cooperate in reaching common goals. Networking of previously offline objects, like cars and roads may represent the next big stage in the evolution of ICT.

The growth of ICT has already resulted in novel applications in the surface transport sector including improved road safety, traffic management systems, the provision of information to and from vehicles (e.g. navigational aids) and seamless financial transactions (e.g. tolls). Key enabling technologies include global positioning systems (GPS) which receive signals from several satellites to calculate position, wireless networks, radiowave and infrared beacons, as well as dedicated short range communications (DSRC) specifically designed for automotive use allowing two-way wireless communication between vehicles and roads.

²⁰² The so called 'green ICTs' are technologies which are ethically designed in order to constantly facilitate the control of energy consumption: i.e. smart ICT applications, sensor networks and applications in smart power grids, smart buildings/housing, intelligent transportation systems and smart industrial processes make significant contributions to more efficient resource use and reduce greenhouse gas emissions and other pollutants. In particular, 'intelligent transport systems' may render transport more efficient, fast and cheap; 'telework' may be a solution for traffic and fuel pollution. Green digital intelligence may monitor, control, adjust, manage new green industry sectors that are ecologically friendly.

²⁰³ Examples of such technological transformation are: planning strategies in order to monitor environmental issues on a global scale (to address environmental degradation and climate change; to combat and slow down global warming, reducing CO₂ emissions and accelerating green growth; to predict disaster or damages) or on a local scale (to manage urban environment systems, monitoring energy distribution, air and water pollution; to improve practices in agriculture and forestry).

²⁰⁴ i.e. 'Paper Consumption Reduction', reducing the consumption of paper through electronic and paperless communication; 'Dematerialization', controlling and limiting the printing of documents by exchanging information electronically; 'Wireless Network Energy Savings', controlling the consumption of the energy of mobiles, constantly monitoring the level of temperature in order to guarantee the functioning of mobiles without energy waste.

Despite the fact that the number of road fatalities in the European Union (EU) has almost halved in the last decade, there were still 34.500 people killed in European roads in 2009. Quite apart from the devastating human toll, the cost of such tragedies in 2009 was estimated to be €130 billion. Intelligent Transportation Systems provide the tools to make transformational improvements in safety and can assist in realising the EU goal of halving overall road fatalities by 2020. Most developments in transportation safety in the last 50 years were designed to minimise injury to passengers in the event of a collision e.g. seatbelts, airbags. ITS has shifted the focus from collision protection to prevention. Advanced emergency braking systems (AEBS), lane departure warning systems (LDW) and intelligent speed adaptation are already available in a limited number of cars. In the case of AEBS, which triggers full on braking when it calculates there is an acute risk of a rear end collision and the driver has failed to react, the European Commission has set 1 November 2013 as the date for when AEBS becomes mandatory for new type trucks over 3.5 tonnes and passenger vehicles with more than nine seats.

More recent developments have focused on the design of intelligent vehicles which have location, acceleration, orientation and proximity sensors all transmitting and gathering data to and from nearby cars and road infrastructure. Networked vehicles could communicate real time data about driving conditions ahead and have the potential to reduce collisions through advisories and warnings. Vehicle operators could be alerted to an accident ahead, poor road conditions such as black ice and advice on remedial actions to be taken could be provided. Vehicles could automatically take evasive actions in the case of the driver not responding to a warning and vehicles could even refuse dangerous instructions from the driving e.g. speeding on wet roads. The intelligent car initiative, one of the flagship projects of the EU i2010 programme similarly aims to harness these new developments in ICT to improve road safety. While the advent of wholly autonomous cars is some years away, in 2011 Google began test driving its self driving car on public roads. To date, the seven autonomous test cars have driven over 190.000 miles on busy city streets, motorways and mountainous roads with only occasional human intervention. Unlike human motorists, autonomous cars will not suffer from distraction, fatigue or intoxication and as such offer the possibility of safer transportation.

Good traffic management can also reduce congestion on our roads, It is estimated that 10% of the EU road network is affected by congestion, at a yearly cost of 0.9-1.5% EU GDP. A number of ITS applications such as traffic light optimisation, ramp metering and congestion charging can contribute to enhancing the operational performance of road networks. If traffic lights are coordinated in an intelligent way, based on dynamic information collected from the road infrastructure and the vehicles which use it, a road network can be used with optimal capacity during quiet times as well as in peak times with competing traffic demands. A number of European citizens have introduced congestion pricing schemes; charging for entry into urban centres at peak times. In 2007, Stockholm introduced congestion charging using RFID tags installed in cars which communicated with receivers at the entry points into the city and triggered automatic payments. Within three years, there was a 50% reduction in traffic wait time, CO2 emissions in the inner city were cut by 14-18% and 60.000 additional passengers were using public transport on a daily basis. ITS helps reduce the environmental impact of road travel by optimising trips, reducing accidents and congestion as well as enhancing vehicle and driver performance. Optimal route planning will reduce the number of kilometres driven, and better control systems for the car will make the ride more energy efficient. Vehicles equipped with eco-driving features can provide feedback to motorists on how to drive at the most fuel-efficient speed across a number of different road conditions. Moreover, by providing people with real-time information on departure and arrival times, thereby reducing travel uncertainty, public transport can be made more attractive to travellers. The widespread deployment of such ITS applications should aid in meeting the EU goal to reduce greenhouse gas emissions to 20% below 2008 levels.

The importance of ITS in delivering improvements in transport efficiency, safety and sustainability has been recognised by the European Commission in its 2008 'Action Plan for the Deployment of Intelligent Transport System in Europe'. The Action Plan was followed by the adoption of Directive 2010/40/EU aimed at providing a framework for the coordinated implementation of ITS across the EU. There are however a number of challenges involved in developing and deploying ITS. In order to realise the full potential of ITS to the transportation network,

it must operate at scale, both nationally and across borders. The current lack of technical standards in this area make it difficult to ensure interoperability however, the European Commission has undertaken to develop specifications to overcome this obstacle as a priority action in Directive 2010/40/EU/ Furthermore, data collected by ITS applications can effectively track movements by vehicles and individuals through the transport system. While this information is helpful from a transport planning perspective, there are legitimate concerns regarding the protection of such personal information. Article 13 of the Directive 2010/40/EU provides an undertaking to refer this issue, as appropriate to the European Data Protection Supervisor and request an opinion of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data.

4.6 Political Dimension

Blogs, social networks and online video platforms are now widely available for everyone with access to the Internet. The opportunities provided by technology are rightly considered of key importance for facilitating political participation, thereby strengthening democracy.

The participatory dimension of ICT and especially of web 2.0 based programming allows more participatory democracy in political decisions.²⁰⁵ In terms of an individual's blogging or grassroots communications, more and more people, ranging from single individuals to discordant communities, are able to spread their opinion and to look for companions sharing their views. The non-hierarchical approach of web 2.0 based communications also fosters the opportunity for more and more people to find information beyond political or mainstream channels. ICT can therefore amplify political participation of individuals and encourage the diffusion of 'non conventional' ideas that contribute to

²⁰⁵ The Internet can also provide tools to help overcome access barriers. Take the example of Egypt. After the Internet was shut down and Egyptians could not be heard outside their borders, a small team of Googlers working with people from Twitter and SayNow, a voice and text company acquired by Google just a week earlier, worked over a weekend to give people a new tool enabling them to leave voice messages that are posted on Twitter. The tool is called 'Speak2Tweet' and it fits with our mission of lowering barriers to access to information and making communication tools easy to use and more widely available.

political pluralism and democratic debate across the world.²⁰⁶

The Internet provides a new input into the political domain and it is possible that the Internet enables a new kind of 'digital citizenship' with specific rights²⁰⁷: the right to connection; the right to net neutrality (which excludes the content control powers and duties of network operators); the right to freedom of expression with the subsequent exclusion of forms of censorship; the right of access to web content. This new dimension should not be seen as a category that replaces the traditional forms of citizenship but as an expansion of the concept of citizenship, understood as a set of rights and powers belonging to every person, wherever they may be in the world.

Another impact these technologies have on shaping the political culture is the claim of transparency. Civil societies groups, the community of hackers, and up-and-coming political parties focusing on web activities are strongly in favour of ensuring that political decision-making processes become more transparent than they have traditionally been. Established political parties, national and international authorities (not least at the EU level) are challenged to cope with the emerging claim for transparency if they are willing to meet expectations to build and sustain trust in the results and procedures of their work. It is also claimed that the blog-culture and social networks bring about more *participation* and therefore more *diversity* in a media-driven world.

The use of ICT may also impact on the collective history of groups. Many welcome the fact that ICT present multiple opportunities to literally '(re-)write' history in a more 'democratic' way, as could recently be observed in the role of social media in the Arab Spring revolutions. ICT may indeed enable citizens to take a broad participatory and plural approach to the documentation of historical events. ICT in this way certainly can play an important role in political participation, empowering people to present their 'own' views and testimonies instead of having to rely only upon sources often considered as

²⁰⁶ Clearly risks of diffusion of detrimental ideological positions exist, such as ideologies conducing to racism, violence, ethnic discrimination, etc. Here, a similar ethical analysis on how to balance freedom of speech with the right to be protected against discrimination of other violations of rights is necessary as was the case in the above-stated conflict in the general social sphere.

²⁰⁷ S. Rodota', hearing to EGE, <http://ec.europa.eu/bepa/european-group-ethics/docs/pdf/s-rodota-pres.pdf>

the 'official' history. The bottom-up documentation of political actions must not, however, be conceived naively, especially not when new media are involved. The 'deliberate selective views' of the representation of facts involve not only professional journalism (as is the case, for example, when war journalists may not report independently but are 'embedded' in an army) but also grass-root movements whose reports can easily be one-sided; re-designed photographs, for example, have for a long time been a topic broadly discussed in media theory and media ethics,²⁰⁸ and need to be continuously closely examined in connection with ICT.

4.7 E-Commerce

According to the Communication adopted by the Commission in January 2012 (COM(2011) 941 and 942), the EU Single Market for e-commerce is still not functioning as it should because there are significant differences in the rules, standards and practices applied to e-commerce within individual Member States. As a result, companies find it difficult to provide online services or to sell goods across EU borders, and citizens miss out on the opportunity to purchase goods and services from websites based in other EU countries.

Some suggest that the first beneficiary of a better-functioning Internal Market for e-commerce would be European consumers who would benefit from a wider range of goods and services and lower prices, thanks in particular to online price and quality comparisons. A better-functioning Internal Market for e-commerce could also create jobs, and help people to look for jobs or work from home. It could bring environmental benefits because it could reduce the need for physical production methods (e.g. through more purchases of digital music or online newspapers) and cut the frequency of certain journeys (e.g. more working from home or provision of advice online). A study into e-commerce in goods²⁰⁹ showed that consumers can save about € 11.7 billion a year (an amount equivalent to 0.12 %

of EU GDP) thanks to lower prices and wider choice. If e-commerce were to grow to 15 % of the total retail sector and Single Market barriers were eliminated, total consumer welfare gains would reach around € 204 billion, equivalent to 1.7 % of EU GDP.

But a better e-commerce system in the EU would also respond to specific ethical concerns that may be identified by Internet users. For example, 'Notice-and-action' procedures refer to rules on removal or blocking of access to illegal content by an online company, after it has received a request to do so. Internet users can submit a notification of illegal content that they have found displayed on the website of an online intermediary (such as a social network, an online vendor or a search engine). To avoid liability, the e-commerce Directive obliges the online intermediary to take action as soon as it becomes aware of the illegal content. Such action can take the form of takedown (removing content) or blocking (disabling access to content). In responses to the public consultation on e-commerce, stakeholders complained that it is not clear how these procedures are meant to work. As a result, illegal content stays online for too long, companies face legal uncertainty and the rights of content providers (like individuals who upload content on the Internet) are not always respected.²¹⁰

The European Commission has also published a proposal for a directive on consumer rights (EC/2011/83). It addresses technology changes (like e-commerce or online auctions) but it does not cover the specific case of cloud computing where security failures may lead to harmful consequences for individuals, ranging from undesired spam to identity theft. The recent revision of the e-Privacy Directive introduced a mandatory

²⁰⁸ Susan Sontag, *Regarding the pain of others*, 1st ed. (New York: Farrar Straus and Giroux, 2003). Analysing 20th century examples of photo documentaries, Sontag shows how documentary photographs are often manipulated in order to create public emotions of shame or compassion. Public perception is also directed when certain images are repeated over and over again, while other events are barely covered. Here, the Internet certainly has a critical role.

²⁰⁹ Civic Consulting (2011). 'Consumer market study on the functioning of e-commerce'. http://ec.europa.eu/consumers/consumer_research/market_studies/e_commerce_study_en.htm.

²¹⁰ As regards the e-commerce Directive's provisions on the liability of service providers, it should be noted that the Directive states that online service providers that are simply 'transmitting' content on the Internet (for instance companies that provide consumers with access to the Internet) cannot be held liable for illegal content that is uploaded by third parties. For example, an Internet access provider cannot be held liable for providing access to an illegal website. Online service providers that 'host' content on the Internet (for instance websites on which you can view content that users themselves put online) cannot be held liable for illegal content uploaded onto their websites by others, as long as they are not aware of it. However, as soon as they become aware of this illegal content (for example via a notification), they are obliged to remove it or to block access to it immediately. Governments may not impose a general obligation on online service providers to monitor the content that they transmit or host. http://ec.europa.eu/consumers/redress_cons/adr_policy_work_en.htm

personal data breach notification, which covers, however, only the electronic communications sector and not other uses of ICT.

4.7.1 Data Mining

Financial and insurance companies have mined their data for several years, in order to detect patterns of fraudulent credit card use or in identifying behaviour patterns of customers that pose risks to the industry²¹¹. Thus, data mining is not new, but is a technique that is being developed and deployed on an increasingly large scale. The mining of data in individual databases in order to identify new information is simple; cross-correlation of the information in multiple databases poses serious issues.

Commercial organisations have become active in using data mining in order to design effective sales campaigns, target marketing plans in an effort to match products with customers, and design new products to increase sales and profitability.²¹² Data mining is also being used by law enforcement agencies to investigate criminal activities and in an effort to avert terrorist actions. The Office of the Director of National Intelligence in the United States of America published a report in 2010²¹³ outlining the various data mining approaches being adopted and developed for the purpose of retrieval and analysis of intelligence information. Data mining promises considerable potential benefits, not least in the area of clinical research where it is being used to identify potential chemical compounds for clinical trials and in analysing the huge amount of research results obtained by molecular medicine, such as genetic or genomic signatures.²¹⁴ Outside of R&D there are many potential applications from modelling of healthcare to pharmacovigilance, to understanding prescribing behaviour and aiding clinical decision-making.²¹⁵

Data mining practices that involve the use of personal data raise a number of privacy concerns. When data

relating to activities and characteristics of individuals are mined, they can reveal large amounts of previously unknown personal information that the subject of the data never intended to be disclosed, even though the separate pieces of data may have each been gathered with their consent. This concern is exacerbated by the fact that data subjects are often unaware that their data are being used in this way, thereby limiting their ability to seek access to the data generated.²¹⁶ As it is not possible to predict what kind of patterns or information will be revealed, it is not possible to clearly specify the exact purpose for which the data are being used. Thus, it is unclear whether data mining is compatible with the 'use limitation' and 'purpose specification' principles of Directive 95/46/EC.

The fundamental problem of privacy violation is further amplified if data sets used in data mining are incomplete or incorrect, thereby rendering the process inaccurate.²¹⁷ Data are gathered from many different sources, not all of commensurate quality. As previously mentioned, if data subjects are unaware that such data exist, they are denied the opportunity of correcting any inaccuracies.

4.7.2 Internet of Things (IoT)

The Internet of things is a promising ICT sector (think of the smart meter, smart grid and electric cars). Potential uses of IoT include the home environment, smart city and health monitor devices. The use of IoT changes radically the relationship between humans and the interconnected autonomous objects, giving to the last ones autonomy towards the interaction with human beings. This new use of technological mediums therefore opens a number of ethics questions related to autonomy (of things and humans); Security (dual use; freedom, liberty); equity/ equality / justice / fairness (access; treatment; discrimination / discriminatory interfaces). Similarly the encoding of data concerning the human users of IoT and their transmission to IoT control centralised systems open issues related to data profiling, confidentiality and autonomy, such as other uses of RFID.

²¹¹ Nonyelum Ogwueleka F. *Journal of Engineering Science and Technology* 2011; 6(3): 311 - 322

²¹² Chou PB, Grossman E, Gunopulos D et al. *Proc Sixth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* 2000:447-56.

²¹³ http://www.dni.gov/reports/2010_ODNI%20Data%20Mining%20Report.pdf, accessed on 10 January 2012.

²¹⁴ Bensmail H, Haoudi A. *J Biomed Biotechnol* 2005;2005(2):63-34.

²¹⁵ Hampton T. *JAMA* 2011;306(2): 144.

²¹⁶ Van Wel, L. and Royackers, L. *Ethics and Information Technology*, 2004;6:129-140.

²¹⁷ Wahlstrom K and Roddick JF. *Selected Papers from the second Australian Institute Conference on Computer Ethics* 2000;1:22-27.

4.7.3 *E-advertising*

Advertising is a form of communication used to encourage or persuade an audience (viewers, readers or listeners) to continue or take some new action. Most commonly, the desired result is to drive consumer behavior with respect to a commercial offering, although political and ideological advertising is also common. Advertising messages are usually paid for by sponsors and viewed via various traditional media; including mass media such as newspaper, magazines, television commercial, radio advertisement, outdoor advertising or direct mail; or new media such as websites and text messages. Clearly the volume of Internet users has induced ICT to massive use this commercial tool for financing the services provide to their users. Although this mechanism does not open new ethical considerations on fair trade and business, some use of advertising may be ethically problematic in particular when concerned with porn, paedophilia, bestiality and divulcation of political views which contravene human rights and human dignity.

4.8 *Conclusions*

ICT may well challenge centuries-old concepts like time and the relation of oneself towards the past, the present, and the future: How do we situate ourselves in the present that transcends the physical space of perception and 'real-life' experience; the notion of space and the local background shaping one's identity changes, too; the perception of oneself and others, and even the formation of group identities undergo radical changes compared to traditional identity concepts. This 'digital turn' of society raises multiple philosophical, social, political, legal, ethical, and also psychological questions.²¹⁸ To address them thoroughly is impossible in this Opinion. Therefore, the EGE emphasises that the political and legal regulations must be complemented by broader considerations, and points to several areas that raise ethical concerns and should be further examined, even though these may not translate into immediate political governance or legal regulation. The EGE therefore deems it necessary to make a number of recommendations (set out in the next chapter) for responsible implementation of the European Digital Agenda.

²¹⁸ Cf. as a good example for a broader approach: Sherry Turkle, *Life on the Screen: Identity in the Age of the Internet* (New York: Simon & Schuster, 1995); Jayle Gackenbach, ed. *Psychology and the Internet: Intrapersonal, Interpersonal, and Transpersonal Implications* (San Diego: 1998); Mark Smith, Kollock, Peter, ed. *Communities in Cyberspace* (London: Routledge, 1999).

PART C: 5 RECOMMENDATIONS

5.1 *The Ethical Framework of the Opinion*

In March 2011, President Jose Manuel Barroso requested the EGE to draft an Opinion on the ethical issues arising from the rapid expansion of Information and Communication Technologies, stating that the Opinion could 'offer a reference point to the Commission to promote responsible use of the Digital Agenda for Europe and facilitating the societal acceptance of such an important policy item'.

The EGE recognises the role Information and Communication Technologies play in European and global society and welcomes the European Commission's efforts to implement the Digital Agenda for Europe in a responsible and innovative way. The group also underlines the efforts the European Union is making in designing its policy frames in accordance with the fundamental values of the European Union and underlines the need to build this process in a democratic and transparent way. ICT enables globalisation in ways not predicted when globalisation was first discussed, and the impact of this new, global world must be considered through the lens of the fundamental values of the European Union

The EGE has chosen to focus mainly on Internet technologies, realising that it is impossible to address the vast range of issues that are encompassed within the scope of Information and Communication Technologies (ICT) as a whole. As a consequence, the security issues arising from ICT will be examined by the EGE in a subsequent Opinion to be provided to the Commission, as requested by President Barroso, in 2013. The EGE has also decided not to address issues related to IPR and it is aware of the controversy related to the on-going and future negotiations of the Anti-Counterfeiting Trade Agreement (ACTA).

The following EGE recommendations will therefore be of a general nature and will include access to ICT, identity, e-commerce, privacy, data protection and a number of social questions linked to the use of ICT in the EU and globally.

This Opinion is set within the context of the fundamental rights and values stated in the Treaty on European Union as they form an ethical basis for the recommendations.

Article 2: The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail.

Article 3: 1. The Union's aim is to promote peace, its values and the well-being of its peoples. (...)

3. The Union shall establish an internal market. It shall work for the sustainable development of Europe based on balanced economic growth and price stability, a highly competitive social market economy, aiming at full employment and social progress, and a high level of protection and improvement of the quality of the environment. It shall promote scientific and technological advance. It shall combat social exclusion and discrimination, and shall promote social justice and protection, equality between women and men, solidarity between generations and protection of the rights of the child. It shall promote economic, social and territorial cohesion, and solidarity among Member States. It shall respect its rich cultural and linguistic diversity, and shall ensure that Europe's cultural heritage is safeguarded and enhanced. (...)

5. In its relations with the wider world, the Union shall uphold and promote its values and interests and contribute to the protection of its citizens. (...)

Promoting this framework of values, together with the commitment to peace and the well-being of the Union's peoples, is the main objective of the Union in all policies including the Digital Agenda and ICT Governance. For this Opinion, the group emphasises especially the importance of the following principles:

- **Human dignity:** The Charter of Fundamental Rights of the European Union states that 'Human dignity is inviolable. It must be respected and protected' (Article 1);²¹⁹

²¹⁹ 'The dignity of the human person is not only a fundamental right in itself but constitutes the real basis of fundamental rights' (Declaration concerning the explanations relating to the Charter of Fundamental Rights).

- **Respect of freedom** which secures, inter alia, the right to uncensored communication and agency in the digital era;
- **Respect for democracy, citizenship and participation** which includes, inter alia, protection against unjustified exclusion and protection against unlawful discrimination;
- **Respect of privacy** which secures, inter alia, the personal private sphere against unjustified interventions;
- **Respect of autonomy and informed consent** which secures, inter alia, the right to information and consent to the use of data or actions that are based on the data-processing;
- **Justice** which secures, inter alia, the equal access to ICT, and a fair sharing of its benefits;
- **Solidarity** among European citizens aims, inter alia, at the inclusion of everyone who wishes to participate in ICT, but also aims to secure the social inclusion of those who, for example, either cannot participate in online practices or wish to maintain alternative social interactions.

The EGE acknowledges the number of positive actions already undertaken by the European Union and its Institutions and makes a number of recommendations to guarantee that the European Digital Agenda can contribute to the flourishing and prosperity of the Union while respecting the values on which Europe is founded and that it continues to embrace.

5.2 Right of Access to ICT

The European Charter of Fundamental Rights requires that everyone has the opportunity to contribute to shaping European Society, which of course includes use of ICT. The protection of the principle of equality therefore is relevant in several domains of an individual's life, such as education, work, commerce and health. The EGE welcomes actions by the EC in the ICT sector and invites the EU to actively participate and promote access to ICT in European societies, while safeguarding access to basic societal services by citizens unwilling to use ICT tools or unable to use them, by virtue of being incapacitated for technical, educational or socio-economical reasons.

- The EGE recommends that the EU secure and promote **the right of access to the Internet**. The EGE

underlines that this approach should also be promoted internationally with specific attention for less developed regions of the world.

- The EGE calls for **educational programmes** to enable individuals to develop technical and /or digital literacy: tools to simplify the applications of ICT, and increase digital literacy in the EU population, addressing especially the requirements of persons with special needs: tools that educate people on how to use the Internet (e.g. from online banking to e-reading).
- The EGE calls for educational programmes to foster and raise awareness and responsibility concerning ICT's impact on one's personal, social and moral identity.
- The EGE welcomes actions on **open access** taken by the EU and encourages further actions in this area to be explored.

5.3 Recommendations Concerning Individual Identity

Concepts of personal identity – i.e. the *identification* concerning the authenticity of a user who engages in the multiple activities that ICT makes possible, and the individual identity that refers to the identity of a person, including his or her values, goals, or self-interpretation – take on new forms and change considerably in the 'digital era'. In the previous part, the EGE has addressed several ethical challenges that need further analysis and examination with respect to the question of identity, and the group recommends a number of actions:

- The Group is of the view that in order to support the **responsible use** of ICT technologies envisaged by the European Digital Agenda, the EU should support the development of educational tools aimed at creating and developing 'social literacy' amongst users including supporting the personal responsibility that should be exercised. Programmes should aim to foster respect, tolerance and sensitivity when communicating digitally.
- Due to the increasingly complex and multiple options offered by the Internet, the EGE is of the view that additional **safeguards** should be in place **for children and adolescents**, in order to ensure a safe environment in which to learn and play. Thus, the Group recommends that awareness raising activities for children, adolescents, their parents and

teachers be incorporated in EU educational programmes and policy actions.

- The EGE recommends that the EU provides means to **foster responsibility** amongst those using ICT, whether individual users or those providing services. This should address accountability, identification, and traceability for Internet identities.
- The EGE acknowledges the studies that demonstrate the **psychological impact** of ICT usage on personal development. The Group recommends that the EU take steps to raise the awareness of these changes by promoting and financing further research, particularly monitoring the impact of ICT on the development and concepts of identity in *Horizon 2020*.

5.4 The Right to Privacy and Protection of Data

For those who wish to embrace innovations in the ICT arena, it is important that they be facilitated in that endeavour, while retaining their right to autonomy and personal privacy. While the concept of privacy is somewhat difficult to explain, many people retain a 'sense of privacy', *i.e.* an understanding that certain aspects of their life are no one's business but their own. This view is perpetuated through the frequent descriptions of the concept of privacy as an individual's right to be left alone or a barrier against intrusion from the outside world. Privacy facilitates our understanding of our sense of self, *i.e.* the recognition that our thoughts and our actions are our own, which is essential for the attribution of moral responsibility. This enables an individual to exercise some level of control over the information he/she makes available to particular parties, thereby preserving his/her autonomy and personal privacy.

Individuals need *sufficient control of their online data* to enable them to use the Internet responsibly. Clarification concerning the conditions for the data subject's consent²²⁰ should therefore be provided, in order to always guarantee informed consent and ensure that the individual is fully aware that he or she is consenting to data processing and what it entails, in line with

²²⁰ This is however complicated by the fact that, in some cases, it is not even clear what would constitute freely given, specific and informed consent to data processing, such as in the case of behavioural advertising, where Internet browser settings are considered by some, but not by others, to deliver the user's consent.

Article 8 of the EU Charter of Fundamental Rights. Clarity on key concepts can also favour the development of self-regulatory initiatives to develop practical solutions consistent with EU law (Com (2010) 609 final, 9). Privacy by design (privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal) should be incorporated into informed consent procedures.

The EGE welcomes and supports the proposed revision of the EU data protection regulatory framework adopted by the Commission in January 2012, the Group underlined that during the inter-institutional debate on the proposed regulatory frame the following recommendations are taken into account:

- The Group recommends that **the characteristics that qualify data as personal data** be clarified, and its relevance to different ICT uses (such as IP addresses, unique RFID-numbers, geo-location data), as well as the development of new data types. This clarification should then be incorporated into the EU data protection regulatory frame.
- In the light of technological and other societal developments, there is a need to reconsider the existing provisions on **sensitive data**, to examine whether other categories of data should be added and to further clarify the conditions for their processing. This concerns, for example, genetic data and biometric data.
- **Transparency** is a fundamental condition for enabling individuals to exercise control over their own data and to ensure effective protection of personal data. It is therefore essential that individuals should be well and clearly informed, in a **simple and transparent** way, by data controllers about how and by whom their data are collected and processed, for what reasons, for how long and what their rights are if they want to access, rectify or delete their data. Basic elements of transparency are the requirements that the information must be easily accessible and easy to understand.
- In order for processing of personal data to be lawful, **personal data** should be processed on the basis of the **explicit consent** of the person concerned (including withdrawal provisions) or some other legitimate basis.

- **Consent should be given by any appropriate method** enabling a freely given specific, informed and unambiguous indication of the data subject's wishes, ensuring that individuals are fully aware that they give their consent including the ticking of a box when visiting an Internet website. Silence or inactivity should therefore not constitute consent. Any use/transmission of data for a different purpose than the one consented by the subject data (for example e-commerce or police) should not be allowed unless justified by appropriate legislation.
- **Consent may always be withdrawn** without negative consequences for the data subject. Data subjects should have the right to require that their personal data be erased and there will be no further processing of the data. In principle data previously analysed must be deleted unless retention can be justified. Informed consent procedures should clarify the conditions when withdrawal is not feasible. The data controller must be sufficiently certain that the person giving consent is actually the data subject and instruments to certify consent on the use of data (for example with digital or electronic signatures) need to be established in ICT requiring subjects' data.
- **Children and vulnerable adults** deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data.
- The Group supports the idea underlying the so called 'right to be forgotten', in the online environment the EGE recommends that the **right to deletion of personal data** should be extended in such a way that any publicly available copies or replications should be deleted.
- The EGE recommends that the processing of personal data of subjects residing in the EU by a controller not established in the EU/EEA is subjected to the EU normative frame on data protection.

5.5 Social Aspects: Digital divide

5.5.1 Digital Divide

Implementing the principles of justice and non-discrimination is a key factor to consider in promoting the use of ICT in different societal domains, from e-Government to e-Health and from e-Business to e-Services. This use of ICT acquires ethical sensitivity when it completely substitutes conventional kinds of

service provisions and then affects the community of European citizens. Innovative forms of commerce, administration and health may indeed provide better quality and more sustainable services to citizens. This goal is certainly to be sustained and encouraged, but those who promote these policies must keep in mind that they may affect the principle of participatory justice and the access to services by individuals and groups who either have no access, cannot or do not wish to use these services.

Society experiences rapid, continuous and incessant change. The drive to invent, reinvent and discard almost continuously is a unique human pursuit in an effort to deliver progress and prosperity for humankind. The society we live in today is dominated by technology and most of us accept that the ever-changing developments in technology have transformed, or have the potential to transform, the way we live and relate to one another. There are those however, who for a myriad of reasons, actively choose not to participate in the digital arena and as an expression of their personal autonomy, this choice should be respected. Nonetheless, as a consequence of not choosing to incorporate ICT into their daily lives, it is likely that these individuals will increasingly see their choices being limited in the digital age. Notwithstanding that fact, it is important is that such 'digital recluses' should not be excluded from accessing essential services or from meeting their societal obligations (e.g. voting, paying taxes) on the basis of their decision to eschew digital technologies. In the interests of inclusion and solidarity, this places a responsibility on wider society to support the provision of alternative means of meeting such obligations at least in the short to medium term.

In order to guarantee the right of citizens to play an active role in European society while respecting their choice of whichever available tools they use to do so, the EGE makes the following recommendations:

- The EGE recognises that **disadvantaged and marginalised groups** may require different designs, content and applications to suit their specific requirements. To this end, the EGE recommends that measures centred around direct provision, subsidies and regulation be examined by the EU to ensure that such groups are not excluded from playing a full and active role in the digital society.
- The EGE recognises the efforts of the Commission to bridge the **digital divide**, including collaboration with international partners, and recommends

that the EU adopts strategies, which go beyond offering public access, and incorporate measures to ensure that people can make effective use of the access. This includes providing people with the skills and motivation to harness the potential of ICT through educational and mentoring programmes, which engage the individual in a process of learning, in a way which is meaningful and relevant to them.

- The EGE recommends that in areas where society places obligations on citizens or where access to essential services are predicated on ICT use, mechanisms unrelated to ICT be established in the short to medium term.

5.5.2 Work-Life Balance

The EGE while recognising the potential benefits offered by increased connectivity within the sphere of work, wishes to highlight the risk of the *always-on* culture in working life, where 'flexible working' can in reality mean the flexibility to be working atypical and long hours, which can impact negatively on family life. The use of ICT needs to be monitored and managed effectively by both employee and employer.

- The EGE urges the EU to encourage and support organisations to develop explicit policies to ensure the optimal use of ICT while **respecting the work-life balance**. Such policies should aim to foster an organisational culture which does not create an expectation that employees should be 'on-call' during non-work hours. This should also be considered in the corporate responsibility programmes and labour regulations.

5.6 Political participation

The influence ICT may have in shaping the political domain raises concerns about citizens' rights to free information, the ability of pressure or special interest groups to modify perceptions and the power of the State to censor data on the Internet. Due to the massive impact of ICT in modern society (as described in the first part of this Opinion) governments around the world are seeking to interact with the online space with new tools: filtering and blocking, registration requirements, surveillance powers, intermediary liability, etc.). The structure of knowledge and communication tools, in all their uses, opens questions about the channelling of knowledge and information in the digital sphere to shape reality and public perception — including the possible spread

of distorted information through the digital world for political purposes. The EGE recommends the following:

- The EGE acknowledges that the basic nature of Internet is the free and active participation of its users. The Group highlights the need for **keeping the Net a free and neutral space**. This freedom must not contravene the fundamental ethical values of the EU.
- The Internet must remain a communication domain where **freedom of expression is protected from censorship** within the framework of the Charter of Fundamental Rights.
- The EGE recognises the need to balance top-down Internet governance by governmental agencies with bottom-up participatory approaches by the Internet community. The EGE emphasises the need that when the EU, Member States and relevant stakeholders deliberate, a **transparent and participatory model is appropriately incorporated in the decision making process**. This applies to all regulatory initiatives on ICT.

5.7 Recommendations Concerning the Sphere of Commerce

5.7.1 Commercial Transactions

The EGE underlines the need to defend rights and interests of European citizens. It therefore welcomes the approach proposed by the European Commission on Corporate Social Responsibility, advocating that to meet their responsibilities, enterprises should have in place a process to integrate social, environmental, ethical, human rights and consumer concerns into their business operations and core strategy in close collaboration with their stakeholders (COM(2011) 681 final). The EGE also welcomes actions by the EU and international bodies to preserve net neutrality (as in COM2011) 222 final); however, it underlines the need to apply the measures on responsibility (from individuals to companies to society to governments) proposed in this Opinion. Tools aiming to achieve these goals, from corporate social responsibility (COM2011) 681 final) to a code of conduct (actions by the Commission concerning responsible use of cloud computing, Internet of things, recommendation on responsible innovation - 2012, etc.) should be encouraged and their implementation sustained. The EGE therefore recommends:

- The EGE acknowledges that a **balance** must be **found between commercial and non-commercial**

uses of ICT. The EGE recommends that the European Commission: 1) Using its data protection legislation, ensure that social media networks protect the data submitted by users in a responsible manner; 2) Educate users so as to ensure that they understand that most of the social media networks are commercial organisations that need to use data for commercial purposes in order to provide the services users enjoy; 3) uses all available means to provide a social networking space (probably on existing networks) that is free of commercial exploitation, for those users who choose it, recognising that the users may have to pay for this privilege.

- The EGE is of the view that in order for people to enter a commercial contract, the terms and conditions of that contract should be presented to the users in clear, concise and intelligible terms.

5.7.2 Corporate Social Responsibility

Protection of privacy is embraced by the principles, including in the Corporate Social Responsibility strategy adopted by the European Commission adopted which in October 2011. The Strategy describes how enterprises can benefit from CSR while contributing to society as a whole by making every effort to meet their social responsibilities.

- The EGE welcomes this initiative and recommends that the EU encourages companies to take privacy into consideration when applying their CSR policy – also using the technological solutions such as Privacy impact assessment, Privacy enhancing technology and privacy by design.

5.8 Cross-Correlative Data Mining

Cross-correlative data mining may be of real significance when databases collected from many sources are analysed together to provide information that is not contained in the individual databases. Linking shopping data collected through store cards with bank data and/or health data, for example, provides insights into an individual's habits which may not have been immediately obvious. The above actions often make use of citizens' data without their specific consent for such a use and may allow profiling of unaware and uninformed people with possible risks of stigmatisation and violation of privacy. The EGE therefore recommends:

- **Individuals should be explicitly informed** by businesses, State bodies or research bodies that their information may be mined for specific purposes. This will ensure that individuals can make informed choices about the services they access and use. Specific consent should always be sought when databases are correlated. The EGE calls for further research into the **privacy implications of cross correlated data mining**, so that this technique can serve society in terms of the potential benefits it may offer, while protecting the human rights. The Group also recommends that the EU further explores if and under which conditions sensitive data can or cannot be used, including cross-correlative data mining.

5.9 Environment and Raw Materials

The area of ICT and the environment is complex: ICT may have positive and negative consequences on environment. The impact of ICT on the environment may be extremely positive: it may be a tool for the protection of environment: monitoring environmental issues, managing urban environment systems, communicating environmental knowledge, disseminating information to the public, stimulating active participation of citizens, enabling efficient use of resources, reducing the consumption of energy and essential natural resources (e.g. reducing the consumption of paper through electronic and paperless communication), bettering the use of natural resources. Examples of such transformation include using ICT to improve practices in agriculture, to monitor air and water pollution, to predict disaster, improve the efficiency of the energy, transportation, and goods and services sectors. The use of electronic devices such as mail or videoconference services may also reduce the need for transportation.

At the same time, the sustainability of these technologies must also be managed to avoid unintended consequences such as increased energy consumption, waste of used electronic devices and the use of raw materials such as rare earth elements. Many electronic devices need extensive use of rare elements (such as tantalum, lanthanum or dysprosium) and modern batteries need large quantities of lithium. The need for such materials is creating social and environmental problems in countries producing the minerals containing these elements. At the same time production of some components is limited to some countries. These facts create a dependence of energy and raw materials for the use of ICT producing an added state of vulnerability that has to be taken into account.

- The EGE recommends that the ecological effects of ICT (use of energy, production of waste and use of raw materials) are quantified, recognised, analysed and communicated and that exploitation of natural resources is minimised.
- The EGE recommends that the EU investigates the vulnerability of the ICT system due to the scarcity of raw materials.
- The Group is aware that several reports have stressed that the production of some minerals which are essential raw materials for the production of hardware in ICT is carried out under inhuman conditions. The Group therefore appeals to the EU to work towards the improvement of working conditions of persons working in this sector, in order to respect the human rights. This should also be incorporated in EU financed development programmes.

5.10 Concluding Recommendation

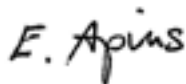
The EGE recognises the potential of the Digital Agenda for Europe (DAE) for the European Union, and stresses the need to promote a responsible, inclusive and socially sustainable implementation of this important policy sector. The Group therefore advocates the need to promote DAE actions in accordance with European Union fundamental values. It equally underlines the need for education and research in the ethical, legal, social and environmental areas to be financed in the Horizon 2020 ICT Programmes.

The European Group on Ethics in Science and New Technologies



The Chairperson: Julian Kinderlerer

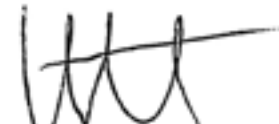
The members:



Emmanuel Agius

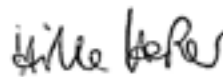


Peter Dabrock



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



Groupe européen d'éthique
des sciences et des nouvelles
technologies auprès
de la Commission européenne

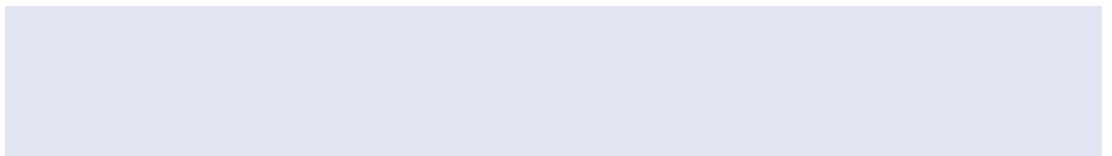
AVIS DU GROUPE EUROPÉEN
D'ÉTHIQUE DES SCIENCES
ET DES NOUVELLES TECHNOLOGIES
AUPRÈS DE LA COMMISSION EUROPÉENNE

Éthique des technologies de l'information et de la communication

Référence: avis requis par le **président Barroso**

Rapporteurs: **Julian Kinderlerer, Peter Dabrock,
Hille Haker, Herman Nys;**

Seul le texte original en anglais est authentique.



ANNEX 1 PARTIE C: 5 RECOMMANDATIONS

5.1 Cadre éthique de l'avis

En mars 2011, M. le Président José Manuel Barroso a demandé au GEE d'élaborer un avis sur les questions éthiques que soulève l'expansion rapide des technologies de l'information et de la communication, déclarant que cet avis doit «pouvoir servir de point de référence pour la Commission, dans sa promotion d'une utilisation responsable de l'agenda numérique pour l'Europe et dans son action pour faciliter l'acceptation, par la société, de cet élément important de sa stratégie».

Le GEE reconnaît le rôle joué par les technologies de l'information et de la communication dans la société, tant au niveau européen que mondial, et salue les efforts de la Commission européenne pour mettre en œuvre l'agenda numérique pour l'Europe de façon responsable et novatrice. Le groupe souligne également les efforts déployés par l'Union européenne pour concevoir ses cadres stratégiques conformément aux valeurs fondamentales de l'Union européenne et souligne la nécessité d'élaborer ce processus de façon démocratique et transparente. Les TIC facilitent la mondialisation d'une façon qui n'avait pas été prévue lorsque le sujet de la mondialisation a été abordé pour la première fois, et l'impact de ce nouveau monde globalisé doit être considéré sous l'angle des valeurs fondamentales de l'Union européenne.

Conscient qu'il est impossible de couvrir le très large éventail des questions que recouvrent les technologies de l'information et de la communication (TIC), le GEE a choisi de se concentrer essentiellement sur les technologies Internet. Par conséquent, les questions de sécurité posées par les TIC seront examinées par le GEE dans un avis ultérieur à remettre à la Commission, comme demandé par M. le Président Barroso, en 2013. Le GEE a également décidé de ne pas couvrir les questions liées aux droits de propriété intellectuelle et prend acte de la controverse que suscitent les négociations en cours et futures de l'accord commercial anti-contrefaçon (ACAC).

Les recommandations suivantes du GEE auront par conséquent un caractère général et incluront l'accès aux TIC, l'identité, le commerce électronique, la protection de la vie privée, la protection des données et diverses questions sociales liées à l'utilisation des TIC dans l'Union européenne et dans le monde.

Le présent avis s'inscrit dans le contexte des valeurs et droits fondamentaux énoncés dans le traité sur l'Union européenne, qui constituent un fondement éthique pour les recommandations qu'il contient.

Article 2: L'Union est fondée sur les valeurs de respect de la dignité humaine, de liberté, de démocratie, d'égalité, de l'État de droit, ainsi que de respect des droits de l'homme, y compris des droits des personnes appartenant à des minorités. Ces valeurs sont communes aux États membres dans une société caractérisée par le pluralisme, la non-discrimination, la tolérance, la justice, la solidarité et l'égalité entre les femmes et les hommes.

Article 3: 1. L'Union a pour but de promouvoir la paix, ses valeurs et le bien-être de ses peuples. (...)

3. L'Union établit un marché intérieur. Elle œuvre pour le développement durable de l'Europe fondé sur une croissance économique équilibrée et sur la stabilité des prix, une économie sociale de marché hautement compétitive, qui tend au plein emploi et au progrès social, et un niveau élevé de protection et d'amélioration de la qualité de l'environnement. Elle promeut le progrès scientifique et technique. Elle combat l'exclusion sociale et les discriminations, et promeut la justice et la protection sociales, l'égalité entre les femmes et les hommes, la solidarité entre les générations et la protection des droits de l'enfant. Elle promeut la cohésion économique, sociale et territoriale, et la solidarité entre les États membres. Elle respecte la richesse de sa diversité culturelle et linguistique, et veille à la sauvegarde et au développement du patrimoine culturel européen. (...)

5. Dans ses relations avec le reste du monde, l'Union affirme et promeut ses valeurs et ses intérêts et contribue à la protection de ses citoyens. (...)

Le principal objectif de l'Union dans toutes les politiques, y compris l'agenda numérique et la gouvernance des TIC, est la promotion de ce cadre de valeurs, ainsi que l'engagement en faveur de la paix et du bien-être des peuples de l'Union. Aux fins de cet avis, le groupe souligne particulièrement l'importance des principes suivants:

- la **dignité humaine** - la Charte des droits fondamentaux de l'Union européenne dispose que

«[L]a dignité humaine est inviolable. Elle doit être respectée et protégée.» (Article 1);²²¹

- le **respect de la liberté**, qui garantit notamment le droit à la communication et à l'agence sans censure dans l'ère numérique;
- le **respect de la démocratie, de la citoyenneté et de la participation** qui inclut notamment la protection contre l'exclusion injustifiée et la protection contre la discrimination illégale;
- le **respect de la vie privée** qui garantit notamment la sphère privée personnelle contre les interventions injustifiées;
- le **respect de l'autonomie et du consentement éclairé** qui garantit notamment le droit à l'information et au consentement à l'utilisation des données ou aux actions qui reposent sur le traitement des données;
- la **justice** qui garantit notamment l'égalité d'accès aux TIC et une répartition équitable de ses bénéfices;
- la **solidarité** parmi les citoyens européens a notamment pour objectif l'inclusion de quiconque souhaite participer aux TIC, mais elle vise également à garantir l'inclusion sociale de ceux qui, par exemple, ne peuvent pas participer à des pratiques en ligne ou souhaitent maintenir des interactions sociales alternatives.

Le GEE salue les nombreuses actions positives déjà entreprises par l'Union européenne et ses institutions et formule diverses recommandations visant à faire en sorte que l'agenda numérique pour l'Europe contribue à la prospérité de l'Union tout en respectant les valeurs qui la fondent et qu'elle continue de promouvoir.

5.2 Droit d'accès aux TIC

La Charte européenne des droits fondamentaux exige que chacun ait la possibilité de contribuer à construire la société européenne, ce qui inclut évidemment l'utilisation des TIC. La protection du principe d'égalité

²²¹ «La dignité de la personne humaine n'est pas seulement un droit fondamental en soi, mais constitue la base même des droits fondamentaux.» (Déclaration concernant les explications relatives à la Charte des droits fondamentaux).

s'applique par conséquent dans plusieurs domaines de la vie d'une personne, comme l'éducation, le travail, le commerce et la santé. Le GEE se félicite des mesures prises par la Commission européenne dans le secteur des TIC et invite l'Union européenne à participer activement et à promouvoir l'accès aux TIC dans les sociétés européennes, tout en garantissant l'accès aux services sociétaux de base par les citoyens qui ne sont pas disposés à utiliser les outils TIC ou qui ne sont pas en mesure de les utiliser, en raison de difficultés techniques, éducatives ou socio-économiques.

- Le GEE recommande à l'UE de garantir et promouvoir le **droit d'accès à Internet**. Le GEE souligne que cette approche devrait également être promue à l'échelle internationale en accordant une attention particulière aux régions les moins développées du monde.
- Le GEE appelle à la mise en place de **programmes éducatifs** permettant aux personnes de développer une culture technique et/ou numérique: des outils qui visent à simplifier les applications des TIC et à accroître la culture numérique au sein de la population de l'UE, qui répondent spécialement aux attentes des personnes qui ont des besoins particuliers et qui informent le public sur la façon d'utiliser Internet (par exemple, de la banque en ligne à la lecture numérique).
- Le GEE appelle à la mise en place de programmes éducatifs qui responsabilisent et sensibilisent à l'impact des TIC sur l'identité personnelle, sociale et morale de chacun.
- Le GEE se félicite des mesures prises par l'UE en matière de **libre accès** et appelle à l'étude de nouvelles mesures dans ce domaine.

5.3 Recommandations concernant l'identité individuelle

Les concepts d'identité personnelle – *l'identification*, à savoir l'authentification de l'identité d'un utilisateur prenant part aux multiples activités rendues possibles par les TIC, et *l'identité individuelle*, à savoir l'identité d'une personne, y compris ses valeurs, ses objectifs, ou son auto-interprétation – revêtent de nouvelles formes et évoluent considérablement dans l'«ère numérique». Dans la partie précédente, le GEE a abordé plusieurs défis éthiques qui commandent une analyse et un examen plus approfondis de la question de l'identité. Le groupe recommande diverses mesures:

- le groupe est d'avis que, pour favoriser **l'utilisation responsable** des TIC envisagée dans l'agenda numérique pour l'Europe, l'UE devrait soutenir le développement d'outils éducatifs visant à créer et à développer chez les utilisateurs une «culture sociale» qui engloberait notamment la responsabilité personnelle qu'il y a lieu d'exercer. Des programmes tendant à encourager le respect, la tolérance et la sensibilité lors de la communication numérique devraient être mis en place;
- compte tenu de la complexité et de la multiplicité croissantes des possibilités offertes par Internet, le GEE est d'avis que de nouvelles **protections** devraient être mises en place à l'intention **des enfants et des adolescents**, afin de leur garantir un environnement sûr pour apprendre et se divertir. Par conséquent, le groupe recommande que des activités de sensibilisation ciblant les enfants, les adolescents, leurs parents et les enseignants soient intégrées aux programmes et actions de l'UE en matière d'éducation;
- le GEE recommande que l'UE agisse de manière à **responsabiliser** les utilisateurs des TIC, qu'il s'agisse de particuliers ou de prestataires de services. Ses actions devraient porter sur les questions de la responsabilité, de l'identification et de la traçabilité des identités Internet;
- le GEE prend acte des études démontrant **l'impact psychologique** de l'utilisation des TIC sur le développement personnel. Le groupe recommande à l'UE de prendre des mesures de sensibilisation à ces changements en promouvant et en finançant de nouvelles activités de recherche, et particulièrement en mesurant l'impact des TIC sur le développement et les concepts d'identité dans l'initiative *Horizon 2020*.

5.4 Le droit à la protection de la vie privée et des données à caractère personnel

Il est important que tous ceux qui souhaitent embrasser les innovations dans le domaine des TIC se voient faciliter la tâche, tout en conservant leur droit à l'autonomie et à la vie privée. Il est certes difficile d'expliquer le concept de vie privée, mais pour beaucoup, ce concept évoque l'«intimité». Ils entendent par là que certains aspects de leur vie ne concernent qu'eux. Cette interprétation est fréquemment prolongée par une description du concept de vie privée comme étant le droit d'une personne de ne pas être dérangée ou comme étant une

barrière contre toute intrusion du monde extérieur. La «vie privée» facilite notre perception de nous-mêmes, c'est-à-dire la reconnaissance du fait que nos pensées et nos actions nous sont propres, condition essentielle à l'attribution d'une responsabilité morale. Cela permet à la personne d'exercer un certain degré de contrôle sur les informations qu'elle met à la disposition d'autrui, préservant de ce fait son autonomie et sa vie privée.

Les personnes doivent disposer d'un *contrôle suffisant de leurs données en ligne* pour être en mesure d'utiliser Internet de façon responsable. Il conviendrait donc de clarifier les conditions du consentement²²² de la personne concernée, afin de garantir qu'il soit toujours accordé en connaissance de cause, et de s'assurer que l'intéressé est pleinement conscient qu'il donne son autorisation et sait de quel traitement il s'agit, conformément à l'article 8 de la Charte des droits fondamentaux de l'Union européenne. La clarification des notions clés peut également favoriser les initiatives en matière d'autoréglementation visant à dégager des solutions pratiques conformes au droit de l'Union (Com(2010)⁶⁰⁹ final, 9). Le respect de la vie privée lors de la conception (la protection de la vie privée et des données à caractère personnel est prise en compte tout au long du cycle de vie des technologies, depuis le stade de leur conception jusqu'à leur déploiement, utilisation et élimination finale) devrait être pris en compte dans les procédures de consentement éclairé.

Le GEE salue et soutient la proposition de révision du cadre réglementaire de l'UE en matière de protection des données adoptée par la Commission en janvier 2012. Il souhaite que, pendant le débat interinstitutionnel sur le cadre réglementaire proposé, les recommandations suivantes soient prises en considération:

- le groupe recommande que les **caractéristiques qualifiant les «données à caractère personnel»** soient clarifiées, de même que leur application à différents usages des TIC (adresses IP, numéros RFID uniques, données de géolocalisation) et au développement de nouveaux types de données. Cette clarification devrait ensuite être intégrée au

²²² La question est cependant compliquée par le fait que, dans certains cas, on ne voit pas clairement ce qui constituerait un consentement libre, exprès et éclairé à un traitement de données, comme dans le domaine de la publicité comportementale en ligne où certains considèrent, mais pas d'autres, que les paramètres du navigateur de l'internaute expriment son consentement.

cadre réglementaire de l'UE en matière de protection des données;

- eu égard aux évolutions technologiques et sociétales, il y a lieu d'examiner les dispositions en vigueur concernant les **données sensibles**, afin de déterminer s'il conviendrait d'y soumettre d'autres catégories de données et de préciser davantage les conditions applicables à leur traitement. Sont concernées, par exemple, les données génétiques et biométriques;
- la **transparence** est une condition fondamentale pour permettre aux personnes concernées d'exercer un contrôle sur leurs propres données et pour assurer une protection effective des données à caractère personnel. Il est donc primordial que les responsables du traitement informent les personnes concernées correctement et clairement, de façon **simple et transparente**, afin qu'elles sachent qui recueillera et traitera leurs données, selon quelles modalités, pour quels motifs et pendant combien de temps, et qu'elles connaissent leurs droits en ce qui concerne l'accès à ces données, leur rectification ou leur suppression. La transparence repose sur des éléments fondamentaux, tels qu'un accès aisé à l'information, qui doit être facile à comprendre;
- pour que le traitement des données à caractère personnel soit légal, **les données à caractère personnel** devraient être traitées sur la base du **consentement exprès** de la personne concernée (incluant un droit de retrait) ou de tout autre fondement légitime;
- le **consentement devrait être donné par toute méthode appropriée** permettant une indication librement donnée, expresse, éclairée et non ambiguë des souhaits de l'intéressé, qui garantisse que la personne concernée est pleinement consciente qu'elle donne son consentement, notamment en cochant une case lorsqu'elle consulte un site Internet. Le silence ou l'inaction ne devraient donc pas être constitutifs d'un consentement. Toute utilisation ou transmission des données dans un but autre que celui consenti par l'intéressé (par exemple, commerce électronique ou maintien de l'ordre) ne devrait pas être autorisée, sauf si la législation applicable le justifie;
- **le consentement peut toujours être retiré** sans conséquences négatives pour l'intéressé.

Les personnes concernées devraient avoir le droit d'exiger que leurs données à caractère personnel soient effacées et ne subissent aucun traitement ultérieur. En principe, les données analysées antérieurement doivent être supprimées, sauf si leur conservation est justifiable. Les procédures de consentement éclairé devraient préciser les conditions dans lesquelles le retrait n'est pas possible. Le responsable du traitement doit être suffisamment assuré que la personne signifiant son consentement est réellement l'intéressé, et des instruments de certification du consentement à l'utilisation des données (par exemple, signatures numériques ou électroniques) doivent être intégrés dans les TIC requérant la communication de données à caractère personnel;

- les **enfants** et les **adultes vulnérables** requièrent une protection particulière, car ils peuvent être moins conscients des risques, des conséquences, des garanties et des droits liés au traitement de leurs données à caractère personnel;
- le groupe soutient l'idée du «droit à l'oubli». Dans un environnement en ligne, le GEE recommande que le **droit à la suppression des données à caractère personnel** soit étendu de telle manière que les copies ou reproductions accessibles au public soient supprimées;
- le GEE recommande que le traitement des données à caractère personnel des personnes résidant sur le territoire de l'UE par un responsable établi en dehors de l'UE/EEE soit soumis au cadre normatif de l'UE en matière de protection des données.

5.5 Aspects sociaux: la fracture numérique

5.5.1 La fracture numérique

L'application des principes de justice et de non-discrimination est un facteur clé à prendre en considération lorsqu'on promeut l'utilisation des TIC dans différents domaines sociétaux, de l'administration en ligne à la santé en ligne et du commerce électronique aux services en ligne. Cette utilisation des TIC devient éthiquement sensible quand elle se substitue complètement aux formes classiques de la prestation de services et influe dès lors sur toute la communauté des citoyens européens. Les modalités innovantes dans les domaines du commerce, de l'administration et de la santé peuvent en effet offrir aux citoyens des services de meilleure qualité et plus durables. Cet objectif

mérite certainement d'être soutenu et encouragé, mais ceux qui promeuvent ces politiques ne doivent pas oublier que celles-ci peuvent compromettre le principe de justice participative et l'accès aux services des personnes et des groupes qui n'ont pas accès à ces modalités nouvelles ou qui ne peuvent ou ne souhaitent pas y recourir.

La société connaît des changements rapides, constants et incessants. L'inventer, le recyclage et l'élimination en quasi-continu sont les manifestations d'une quête exclusivement humaine qui vise à faire progresser et prospérer l'humanité. La société où nous vivons aujourd'hui est dominée par la technologie et la plupart d'entre nous admettent que l'évolution permanente de la technologie a transformé, ou peut transformer, notre manière de vivre et nos relations réciproques. Certains toutefois, pour une foule de raisons, choisissent de ne pas prendre part à la société numérique, exprimant ainsi leur autonomie personnelle. Leur choix doit être respecté, bien qu'il soit probable qu'en refusant d'intégrer les TIC dans leur vie quotidienne, ces personnes voient le champ de leurs options rétrécir de plus en plus dans l'ère numérique. En dépit de cela, il importe que ces «reclus numériques» ne soient pas privés de la possibilité d'accéder à des services essentiels ou de s'acquitter de leurs obligations sociétales (par exemple le vote ou le paiement de l'impôt) du fait de leur rejet des technologies numériques. Dans l'intérêt de l'inclusion et de la solidarité, la société au sens large se voit donc tenue de favoriser la fourniture de moyens alternatifs de satisfaire à ces obligations, ne serait-ce qu'à court ou moyen terme.

Pour garantir aux citoyens leur droit de jouer un rôle actif dans la société européenne tout en respectant leurs choix en matière d'outils utilisables à cet effet, le GEE formule les recommandations suivantes:

- le GEE reconnaît que les **groupes désavantagés et marginalisés** peuvent requérir des conceptions, applications et contenus différents pour répondre à leurs besoins spécifiques. À cet effet, le GEE recommande que des mesures axées sur la fourniture directe, les subventions et la réglementation soient examinées par l'UE, afin que ces groupes ne soient pas privés de la possibilité de jouer pleinement un rôle actif dans la société numérique;
- le GEE reconnaît les efforts consentis par la Commission pour réduire la **fracture numérique**, y compris sa collaboration avec des partenaires

internationaux, et recommande que l'UE adopte des stratégies qui ne consistent pas seulement à ouvrir l'accès au public mais qui intègrent également des mesures permettant un exercice effectif de cet accès. Cela implique d'instruire le public et de le motiver à tirer parti du potentiel des TIC au moyen de programmes éducatifs et de tutorat, qui engagent chacun dans un processus d'apprentissage utile et judicieux;

- le GEE recommande que, dans les domaines où la société impose des obligations aux citoyens ou dans lesquels l'accès aux services essentiels repose sur l'utilisation des TIC, des mécanismes indépendants des TIC soient établis à court ou moyen terme.

5.5.2 Équilibre entre vie professionnelle et vie privée

Tout en reconnaissant les avantages potentiels d'une connectivité accrue dans la sphère du travail, le GEE souhaite mettre en évidence le risque de la culture de la «connexion permanente» dans la vie professionnelle, où «travail flexible» pourrait être synonyme de travail à toute heure et sans limite, avec de possibles incidences négatives sur la vie de famille. L'utilisation des TIC doit être surveillée et gérée efficacement à la fois par l'employé et l'employeur.

- Le GEE invite l'UE à encourager et aider les organisations à élaborer des politiques explicites garantissant une utilisation optimale des TIC **dans le respect de l'équilibre entre vie professionnelle et vie privée**. Ces politiques devraient viser à encourager une culture organisationnelle qui ne sous-entende pas que les employés sont «d'astreinte» en dehors des heures de travail. Ce point devrait également être abordé dans les programmes en matière de responsabilité des entreprises et dans la réglementation du travail.

5.6 Participation politique

L'influence que les TIC peuvent avoir sur le domaine politique soulève des inquiétudes en ce qui concerne le droit des citoyens à la libre information, la capacité des groupes d'intérêts ou de pression à modifier les perceptions et le pouvoir de l'État de censurer des données sur Internet. Compte tenu de l'impact massif des TIC sur la société moderne (comme décrit dans la première partie du présent avis), les gouvernements du monde entier cherchent à interagir avec l'espace en ligne à l'aide de nouveaux outils: filtrage, exigences

d'enregistrement, pouvoirs de surveillance, responsabilité des intermédiaires, etc.). La structure des outils de la connaissance et de la communication, tous usages confondus, soulève la question de l'orientation de la connaissance et de l'information dans la sphère numérique dans le but de façonner la réalité et la perception du public – y compris la diffusion possible d'informations faussées via les canaux numériques à des fins politiques. Le GEE recommande ce qui suit:

- le GEE reconnaît que le trait fondamental de l'Internet est la participation libre et active de ses utilisateurs. Le groupe souligne la nécessité de faire en sorte que **le Net reste un espace libre et neutre**. Cette liberté ne doit pas aller à l'encontre des valeurs éthiques fondamentales de l'UE;
- l'Internet doit rester un domaine de communication où **la liberté d'expression est protégée contre la censure** dans le cadre de la Charte des droits fondamentaux;
- le GEE reconnaît la nécessité de contrebalancer la gouvernance descendante de l'Internet par des organismes gouvernementaux appliquant des approches participatives ascendantes qui associent la communauté Internet. Il souligne qu'**un modèle transparent et participatif devrait être dûment intégré au processus décisionnel** associant l'UE, les États membres et les parties prenantes, et ce pour toute initiative en matière de réglementation des TIC.

5.7 Recommandations au sujet de la sphère du commerce

5.7.1 Les transactions commerciales

Le GEE souligne la nécessité de défendre les droits et intérêts des citoyens européens. Il salue donc l'approche proposée par la Commission européenne en matière de responsabilité sociale des entreprises, selon laquelle, pour s'acquitter de leur responsabilité, les entreprises doivent engager, en collaboration étroite avec les parties prenantes, un processus destiné à intégrer les préoccupations en matière sociale, environnementale, éthique, de droits de l'homme et des consommateurs dans leurs activités commerciales et leur stratégie de base (COM(2011) 681 final). Le GEE salue également les actions de l'UE et des organismes internationaux pour préserver la neutralité du Net (COM(2011) 222 final); toutefois, il souligne la nécessité d'appliquer les mesures en matière de responsabilité

(des particuliers aux entreprises, en passant par la société et les gouvernements) proposées dans le présent avis. La mise en place et en œuvre d'outils visant à atteindre ces objectifs, de la responsabilité sociale des entreprises (COM(2011) 681 final) à un code de conduite (actions menées par la Commission au sujet de l'utilisation responsable de l'informatique en nuage et de l'Internet des objets, recommandation concernant l'innovation responsable - 2012, etc.) devrait être encouragée et soutenue. Le GEE recommande donc ce qui suit:

- le GEE constate qu'un équilibre doit être trouvé entre les utilisations commerciales et non commerciales des TIC. Il recommande à la Commission européenne: 1) de s'assurer, en se fondant sur sa législation en matière de protection des données, que les réseaux de médias sociaux protègent de façon responsable les données communiquées par les utilisateurs; 2) d'éduquer les utilisateurs de sorte qu'ils comprennent que la plupart des réseaux de médias sociaux sont des organisations commerciales qui doivent utiliser les données à des fins commerciales pour pouvoir fournir aux utilisateurs les services dont ils profitent; 3) d'employer tous les moyens disponibles pour offrir aux utilisateurs qui le souhaitent un espace de réseautage social (probablement sur les réseaux existants) qui soit exempt d'exploitation commerciale, sachant que les utilisateurs pourraient devoir payer pour ce privilège;
- le GEE est d'avis qu'aux fins de la conclusion d'un contrat commercial, les conditions de ce contrat doivent être présentées aux utilisateurs dans des termes clairs, concis et intelligibles.

5.7.2 Responsabilité sociale des entreprises

La protection de la vie privée est couverte par une série de principes, notamment ceux repris dans la stratégie de responsabilité sociale des entreprises (RSE) adoptée par la Commission européenne en octobre 2011. La stratégie explique comment les entreprises peuvent tirer parti de la RSE tout en contribuant à la société dans son ensemble en faisant tout leur possible pour s'acquitter de leurs responsabilités sociales.

- Le GEE se félicite de cette initiative et recommande à l'UE d'encourager les entreprises à prendre en considération la vie privée dans l'application de leur politique de RSE – tout en utilisant les solutions technologiques relatives à l'évaluation des répercussions sur la vie privée, au renforcement du

respect de la vie privée et à la protection intégrée de la vie privée.

5.8 Exploration de données par corrélation croisée

L'exploration de données par corrélation croisée peut présenter un intérêt réel lorsque des bases de données collectées auprès de diverses sources sont analysées ensemble pour détecter des informations qui ne sont pas contenues dans des bases déterminées. Par exemple, le fait de relier des données d'achats par cartes de magasin à des données bancaires et/ou de santé peut donner un éclairage sur des comportements individuels qui n'étaient éventuellement pas immédiatement évidents. Ce type de corrélation exploite souvent les données de citoyens sans le consentement exprès de ceux-ci et peut déboucher sur un profilage dissimulé et non consenti, avec un possible risque de stigmatisation et de violation de la vie privée. Le GEE recommande donc ce qui suit:

- **les personnes concernées devraient être expressément informées** par les entreprises, les instances nationales ou les organismes de recherche du fait que leurs informations peuvent faire l'objet d'une exploration à des fins spécifiques. Les intéressés pourront ainsi faire des choix éclairés au sujet des services auxquels elles accèdent et qu'elles utilisent. Le consentement exprès devrait toujours être sollicité lorsque des bases de données sont mises en corrélation. Le GEE préconise une réflexion approfondie au sujet **des répercussions sur la vie privée de l'exploration de données par corrélation croisée**, de sorte que cette technique puisse rendre service à la société en raison de ses avantages potentiels, tout en protégeant les droits humains. Le groupe recommande également que l'UE réfléchisse plus avant à la question de savoir si, et dans quelles conditions, les données sensibles peuvent être utilisées, y compris au moyen d'une exploration par corrélation croisée.

5.9 Environnement et matières premières

La problématique des TIC et de l'environnement est complexe: les TIC peuvent avoir des conséquences positives et négatives sur l'environnement. L'impact des TIC sur l'environnement peut être extrêmement positif. Ce peut être un outil pour la protection de l'environnement: suivi des questions environnementales, gestion des systèmes environnementaux

urbains, communication des connaissances environnementales, diffusion de l'information auprès du public, stimulation de la participation active des citoyens, promotion de l'utilisation efficace des ressources, réduction de la consommation d'énergie et de ressources naturelles essentielles (par exemple, réduction de la consommation de papier grâce à la communication électronique ou sans papier), amélioration de l'utilisation des ressources naturelles. Les exemples d'une telle transformation incluent l'utilisation des TIC pour améliorer les pratiques agricoles, surveiller la pollution de l'air et de l'eau, prévoir les catastrophes et améliorer l'efficacité des secteurs de l'énergie, du transport, ainsi que des biens et services. L'utilisation de dispositifs électroniques tels que les services de messagerie électronique ou de vidéoconférence peut également réduire le besoin de transport.

En même temps, la durabilité de ces technologies doit également être gérée pour éviter des conséquences non voulues telles que la consommation accrue d'énergie, les déchets issus des dispositifs électroniques usagés et l'utilisation de matières premières telles que des éléments de terres rares. De nombreux dispositifs électroniques nécessitent une exploitation extensive d'éléments rares (tels que le tantale, le lanthane ou le dysprosium) et les batteries modernes ont besoin de grandes quantités de lithium. La demande de ces matières crée des problèmes sociaux et environnementaux dans les pays où l'on extrait les minerais qui les contiennent. En même temps, la production de certains composants est limitée à quelques pays. Ces faits créent une dépendance envers l'énergie et les matières premières pour l'utilisation des TIC, produisant un état de vulnérabilité accrue qui doit être pris en compte.

- Le GEE recommande que les effets écologiques des TIC (utilisation de l'énergie, production de déchets et utilisation des matières premières) soient quantifiés, identifiés, analysés et communiqués, et que l'exploitation des ressources naturelles soit réduite au minimum.
- Le GEE recommande à l'UE d'étudier la vulnérabilité du système des TIC, compte tenu de la rareté des matières premières.
- Le groupe sait que plusieurs rapports ont souligné que l'extraction de certains minerais constituant des matières premières essentielles à la fabrication des équipements de TIC est effectuée dans des conditions inhumaines. Le groupe appelle donc l'UE

à œuvrer à l'amélioration des conditions de travail dans ce secteur, afin de faire respecter les droits de l'homme. Ce point devrait également être intégré dans les programmes de développement financés par l'UE.

5.10 Recommandation finale

Le GEE reconnaît le potentiel de l'agenda numérique pour l'Europe et souligne la nécessité de promouvoir une mise en œuvre responsable, inclusive et socialement durable de cet important secteur stratégique. Le groupe plaide donc en faveur de la promotion des mesures s'inscrivant dans le cadre de l'agenda numérique pour l'Europe dans le respect des valeurs fondamentales de l'Union européenne. Il souligne également la nécessité de financer l'éducation et la recherche sur le plan éthique, juridique, social et environnemental dans le volet TIC de l'initiative Horizon 2020.



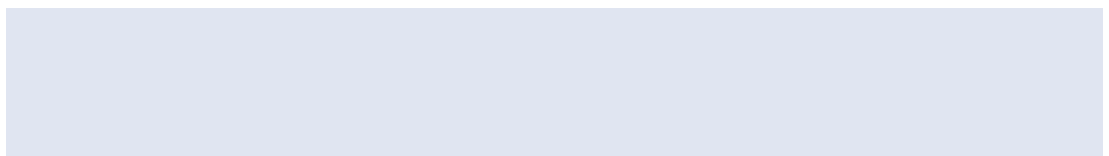
**Europäische Gruppe
für Ethik in Naturwissenschaften
und neuen Technologien
bei der Europäischen Kommission**

STELLUNGNAHME DER EUROPÄISCHEN
GRUPPE FÜR ETHIK
IN NATURWISSENSCHAFTEN
UND NEUEN TECHNOLOGIEN
BEI DER EUROPÄISCHEN KOMMISSION

Ethik der Informations- und Kommunikationstechnologien

Bezug: Ersuchen von **Präsident Barroso**
Berichterstatter: **Julian Kinderlerer, Peter Dabrock,**
Hille Haker, Herman Nys;

Nur der Originaltext auf Englisch ist authentisch.



ANNEX 2 TEIL C: 5 EMPFEHLUNGEN

5.1 *Ethischer Rahmen der Stellungnahme*

Präsident José Manuel Barroso hat die EGE im März 2011 um eine Stellungnahme zu den ethischen Fragen, die sich aus der raschen Ausdehnung von Informations- und Kommunikationstechnologien (IKT) ergeben, ersucht und unterstrichen, dass die Stellungnahme der Kommission als Bezugspunkt für die Förderung eines verantwortungsvollen Umgangs mit der Digitalen Agenda für Europa dienen und die Akzeptanz eines derart wichtigen politischen Anliegens in der Gesellschaft erleichtern könnte.

Die EGE erkennt an, dass Informations- und Kommunikationstechnologien eine wichtige gesellschaftliche Rolle in Europa und der gesamten Welt spielen, und sie begrüßt die Bemühungen der Europäischen Kommission um eine verantwortungsvolle und innovative Umsetzung der Digitalen Agenda für Europa. Die Gruppe möchte zudem die Anstrengungen hervorheben, die die Europäische Union unternimmt, um ihre politischen Rahmen in Übereinstimmung mit den Grundwerten der Europäischen Union zu gestalten, und sie weist darauf hin, dass dieser Prozess demokratisch und transparent sein muss. Informations- und Kommunikationstechnologien eröffnen Globalisierungsmöglichkeiten, die zu Zeiten, als das Thema Globalisierung erstmals erörtert wurde, noch unvorstellbar waren, und die Auswirkungen dieser neuen, globalisierten Welt müssen im Lichte der Grundwerte der Europäischen Union betrachtet werden.

Die EGE hat sich vor allem mit den Internettechnologien befasst, weil ihr bewusst ist, dass es nicht möglich ist, die gesamte umfangreiche Palette der mit dem IKT-Bereich zusammenhängenden Themen zu behandeln. Die sich aus den IKT ergebenden Sicherheitsfragen werden daher in einer nachfolgenden Stellungnahme der EGE behandelt werden, die der Kommission auf Ersuchen von Präsident Barroso im Jahr 2013 vorzulegen ist. Die EGE hat sich zudem dafür entschieden, nicht auf das Thema Rechte an geistigem Eigentum einzugehen, und sie ist sich auch der Kontroverse um die laufenden und die künftigen Verhandlungen über das Anti-Produktpiraterie-Handelsabkommen ACTA bewusst.

Die nachfolgenden Empfehlungen der EGE sind daher allgemeiner Art und beziehen sich auf die Themen Zugang zu IKT, Identität, elektronischer Handel, Schutz

der Privatsphäre, Datenschutz und bestimmte soziale Fragen im Zusammenhang mit der Nutzung von IKT in der EU und der gesamten Welt.

Diese Stellungnahme fußt auf den im Vertrag über die Europäische Union verankerten Grundrechten und Werten, die auch die ethische Grundlage für die Empfehlungen bilden.

Artikel 2: Die Werte, auf die sich die Union gründet, sind die Achtung der Menschenwürde, Freiheit, Demokratie, Gleichheit, Rechtsstaatlichkeit und die Wahrung der Menschenrechte einschließlich der Rechte der Personen, die Minderheiten angehören. Diese Werte sind allen Mitgliedstaaten in einer Gesellschaft gemeinsam, die sich durch Pluralismus, Nichtdiskriminierung, Toleranz, Gerechtigkeit, Solidarität und die Gleichheit von Frauen und Männern auszeichnet.

Artikel 3: 1. Ziel der Union ist es, den Frieden, ihre Werte und das Wohlergehen ihrer Völker zu fördern. (...)

3. Die Union errichtet einen Binnenmarkt. Sie wirkt auf die nachhaltige Entwicklung Europas auf der Grundlage eines ausgewogenen Wirtschaftswachstums und von Preisstabilität, eine in hohem Maße wettbewerbsfähige soziale Marktwirtschaft, die auf Vollbeschäftigung und sozialen Fortschritt abzielt, sowie ein hohes Maß an Umweltschutz und Verbesserung der Umweltqualität hin. Sie fördert den wissenschaftlichen und technischen Fortschritt. Sie bekämpft soziale Ausgrenzung und Diskriminierungen und fördert soziale Gerechtigkeit und sozialen Schutz, die Gleichstellung von Frauen und Männern, die Solidarität zwischen den Generationen und den Schutz der Rechte des Kindes. Sie fördert den wirtschaftlichen, sozialen und territorialen Zusammenhalt und die Solidarität zwischen den Mitgliedstaaten. Sie wahrt den Reichtum ihrer kulturellen und sprachlichen Vielfalt und sorgt für den Schutz und die Entwicklung des kulturellen Erbes Europas. (...)

5. In ihren Beziehungen zur übrigen Welt schützt und fördert die Union ihre Werte und Interessen und trägt zum Schutz ihrer Bürgerinnen und Bürger bei. (...)

Die Förderung dieses Werterahmens bildet zusammen mit dem Eintreten für den Frieden und für den Wohlstand aller EU-Bürger das Hauptziel, das die Union in

all ihren Politikbereichen einschließlich der Digitalen Agenda und der IKT-Governance verfolgt. Bei dieser Stellungnahme hat die Gruppe vor allem auf folgende Grundsätze besonderes Augenmerk gelegt:

- **Menschenwürde:** Die Charta der Grundrechte der Europäischen Union besagt: „Die Würde des Menschen ist unantastbar. Sie ist zu achten und zu schützen.“ (Artikel 1);²²³
- **Wahrung der Freiheit** und insbesondere des Rechts auf eine zensurfreie Kommunikation und Agentur im digitalen Zeitalter;
- **Wahrung von Demokratie, Bürgerrechten und Bürgerbeteiligung** einschließlich Schutz vor Ausgrenzung und unzulässiger Diskriminierung;
- **Wahrung der Privatsphäre** einschließlich Schutz vor ungerechtfertigten Eingriffen in die Privatsphäre;
- **Wahrung der Selbständigkeit und Aufklärungspflicht bei Einwilligungen**, u.a. zum Schutz des Rechts auf Information und auf Aufklärung im Vorfeld einer Zustimmung zur Datenverwendung oder zu sich auf die Verarbeitung dieser Daten gründenden Maßnahmen;
- **Gerechtigkeit**, u.a. zwecks Sicherstellung eines gleichberechtigten Zugangs zu IKT und einer gerechten Nutzung ihrer Vorteile;
- **Solidarität** unter den EU-Bürgern, u.a. zwecks Einbeziehung von jedem, der an IKT mitwirken möchte, aber auch zur Sicherstellung der gesellschaftlichen Eingliederung von Personen, die sich beispielsweise nicht an Online-Praktiken beteiligen können oder alternative soziale Interaktionsformen beibehalten möchten.

Die EGE begrüßt die positiven Maßnahmen, die die Europäische Union und ihre Organe bereits ergriffen haben und unterbreitet nachfolgend eine Reihe von Empfehlungen, durch die sichergestellt werden soll, dass die Europäische Digitale Agenda unter Wahrung der Werte, auf die sich Europa gründet und die Europa

nach wie vor anstrebt, zum Blühen und Gedeihen der Union beitragen kann.

5.2 Recht auf Zugang zu IKT

Die Europäische Charta der Grundrechte sieht vor, dass jede Person die Möglichkeit haben muss, einen Betrag zur Gestaltung der europäischen Gesellschaft zu leisten, was natürlich auch die Nutzung von IKT einschließt. Der Schutz des Gleichheitsprinzips ist daher in mehreren Lebensbereichen wie Bildung, Beschäftigung, Handel und Gesundheit von besonderer Bedeutung. Die EGE begrüßt die von der Europäischen Kommission im IKT-Bereich ergriffenen Maßnahmen und ersucht die EU, sich an der Nutzung von IKT in den europäischen Gesellschaftssystemen zu beteiligen und den Zugang zu IKT zu fördern, gleichzeitig aber auch Bürgern, die aus technischen, bildungsspezifischen oder sozioökonomischen Gründen nicht auf IKT-Werkzeuge zurückgreifen können oder wollen, den Zugang zu grundlegenden sozialen Diensten zu garantieren.

- Die EGE empfiehlt der EU, **das Recht auf Zugang zum Internet** zu wahren und zu stärken. Die EGE betont, dass ein solches Vorgehen auch auf internationaler Ebene gefördert und dabei besonderes Gewicht auf die weniger entwickelten Regionen der Welt gelegt werden sollte.
- Die EGE fordert die Einrichtung von **Bildungsprogrammen**, durch die der Einzelne in die Lage versetzt wird, seine technische und/oder digitale Kompetenz zu verbessern (z.B. durch Werkzeuge zur Vereinfachung von IKT-Anwendungen), und die auf die Verbesserung der digitalen Kompetenz der gesamten EU-Bevölkerung abstellen und sich insbesondere mit den Anforderungen von Menschen mit besonderen Bedürfnissen befassen (Werkzeuge zum Erlernen des Umgangs mit dem Internet, angefangen beim Internetbanking bis hin zu elektronischen Büchern).
- Die EGE fordert die Einrichtung von Bildungsprogrammen zur Sensibilisierung für die Auswirkungen der IKT auf die persönliche, gesellschaftliche und moralische Identität des Einzelnen und zur Schaffung eines größeren Verantwortungsbewusstseins für diese Identität.
- Die EGE begrüßt die von der EU ergriffenen Maßnahmen zur Förderung eines **offenen Zugangs** und regt an, dass weitere Maßnahmen auf diesem Gebiet sondiert werden sollten.

²²³ „Die Würde des Menschen ist nicht nur ein Grundrecht an sich, sondern bildet das eigentliche Fundament der Grundrechte.“ (Erklärung zu den Erläuterungen zur Charta der Grundrechte).

5.3 Empfehlungen zum Thema individuelle Identität

Konzepte, die sich mit der persönlichen Identität des Einzelnen (d.h. mit der *Identifizierung* zwecks Prüfung der Echtheit eines sich mit den zahlreichen durch IKT ermöglichten Tätigkeiten befassenden Nutzers und mit der individuellen Identität einer Person und ihrer Werte, Ziele oder Selbstsicht) befassen, nehmen im „digitalen Zeitalter“ neue Formen an und unterliegen einem starken Wandel. Die EGE hat im vorhergehenden Teil verschiedene ethische Herausforderungen angesprochen, die in Bezug auf die Frage der Identität der weiteren Analyse und Prüfung bedürfen, und die Gruppe empfiehlt diesbezüglich folgende Maßnahmen:

- Um eine **verantwortungsvolle Nutzung** der in der Digitalen Agenda für Europa vorgesehenen IKT zu fördern, sollte die EU nach Auffassung der Gruppe die Entwicklung von Bildungswerkzeugen unterstützen, die dazu dienen, eine „soziale Kompetenz“ der Nutzer zu schaffen und auszuprägen; dies schließt die Unterstützung eines eigenverantwortlichen Handelns ein. Es sollten einschlägige Programme aufgelegt werden, die auf die Förderung von Respekt, Toleranz und Einfühlungsvermögen bei der digitalen Kommunikation abstellen.
- Da die vom Internet gebotenen Möglichkeiten immer zahlreicher und immer komplexer werden, ist die EGE der Auffassung, dass zusätzliche **Sicherheitsvorkehrungen für Kinder und Jugendliche** getroffen werden sollten, damit diese in einer sicheren Umgebung lernen und spielen können. In diesem Sinne empfiehlt die Gruppe die Integration von Aufklärungsmaßnahmen für Kinder und Jugendliche und ihre Eltern und Lehrer in die Bildungsprogramme und die politischen Maßnahmen der EU.
- Die EGE empfiehlt der EU, Mittel zur **Stärkung des Verantwortungsbewusstseins** der Nutzer und der Anbieter von IKT-Diensten bereitzustellen. Konkret sollte es dabei um die Themen Rechenschaftspflicht, Identifizierung und Rückverfolgbarkeit der Internetidentität gehen.
- Die EGE hat die Studien, die die **psychologischen Auswirkungen** der Nutzung von IKT auf die persönliche Entwicklung aufgezeigt haben, zur Kenntnis genommen. Die Gruppe empfiehlt der EU, das Bewusstsein für diese Veränderungen zu schärfen und zu diesem Zweck weitere

Forschungsmaßnahmen auf diesem Gebiet zu fördern und zu finanzieren und insbesondere die Auswirkungen von IKT auf die Entwicklung und die Identitätskonzepte im Rahmen von „Horizont 2020“ zu überwachen.

5.4 Das Recht auf Privatsphäre und Datenschutz

Für Menschen, die von IKT-Innovationen Gebrauch machen wollen, ist es wichtig, dass sie dabei unterstützt werden, gleichzeitig aber ihre Eigenständigkeit und ihre Privatsphäre gewahrt bleiben. Obschon der Begriff „Privatsphäre“ nicht einfach zu erklären ist, haben doch die meisten Menschen das Empfinden, dass bestimmte Aspekte ihres Lebens nur sie selbst etwas angehen. Dass „Privatsphäre“ regelmäßig als der nicht-öffentliche Bereich definiert wird, in dem ein Mensch unbehelligt von äußeren Einflüssen sein Recht auf freie Entfaltung der Persönlichkeit wahrnehmen kann, stärkt dieses Empfinden. Die Privatsphäre erleichtert dem Menschen das Verständnis von sich selbst, sprich: die Erkenntnis, dass sein Denken und sein Handeln sein eigen sind, was wiederum eine wesentliche Voraussetzung dafür ist, dass er moralische Verantwortung übernehmen kann. Dies ermöglicht dem Einzelnen, ein gewisses Maß an Kontrolle über die Informationen auszuüben, die er anderen gibt und so seine Eigenständigkeit und seine Privatsphäre zu wahren.

Um das Internet verantwortungsvoll nutzen zu können, benötigt jeder Mensch *hinreichende Kontrolle über seine Onlinedaten*. Daher sollten die Bedingungen für die Einwilligung der betroffenen Person²²⁴ stets klargestellt werden, damit gewährleistet ist, dass die Einwilligung nach erfolgter Aufklärung erteilt wurde („informierte Einwilligung“) und die betroffene Person sich vollauf darüber im Klaren war, dass sie einer Verarbeitung ihrer Daten im Sinne von Artikel 8 der Charta der Grundrechte der Europäischen Union zustimmt und welche Folgen dies hat. Klarheit über Schlüsselbegriffe kann zudem der Entwicklung von Selbstregulierungsinitiativen zur Ausarbeitung von praktischen, im Einklang mit dem EU-Recht stehenden Lösungen förderlich sein (siehe

²²⁴ Ein erschwerender Umstand ist allerdings, dass in manchen Fällen gar nicht klar ist, worin die betreffende aus freiem Willen und nach vorheriger Aufklärung erteilte Zustimmung zu einer spezifischen Datenverarbeitung besteht. Dies gilt beispielsweise für die verhaltensorientierte Werbung im Internet, bei der die Einwilligung des Nutzers nach Auffassung mancher (aber eben nicht aller) im Wege der Browsereinstellungen erteilt wird.

KOM (2010) 609 endg., S. 9). Fester Bestandteil aller eine „informierte Einwilligung“ voraussetzenden Verfahren sollte daher ein „eingebauter Datenschutz“ sein (d.h. der Schutz der Privatsphäre und der Datenschutz werden in den gesamten Lebenszyklus von Technologien eingebettet, angefangen bei der Konzeption über die Einführung und Verwendung bis hin zur Abschaffung).

Die EGE begrüßt und befürwortet den Vorschlag zur Neufassung des EU-Datenschutzrahmens, den die Kommission im Januar 2012 angenommen hat. Die Gruppe hat betont, dass bei der interinstitutionellen Debatte über den Vorschlag folgende Empfehlungen berücksichtigt werden sollten:

- Die Gruppe empfiehlt, dass klargelegt werden sollte, **welche Merkmale Daten zu personenbezogenen Daten machen**, welche Bedeutung dies für die verschiedenen Nutzungsformen von IKT (IP-Adressen, RFID-Nummern, Geolokationsdaten usw.) hat, und wie sich dies auf die Entwicklung neuer Datenarten auswirkt. Diese Präzisierungen sollten sodann in den Datenschutzrahmen der EU einfließen.
- Es ist angesichts der technologischen und der sonstigen gesellschaftlichen Entwicklung notwendig, die geltenden Bestimmungen über **sensible Daten** zu überdenken, zu prüfen, ob andere Datenkategorien hinzugefügt werden sollten und näher zu klären, unter welchen Bedingungen sie verarbeitet werden dürfen. Beispielsweise betrifft dies genetische und biometrische Daten.
- **Transparenz** ist eine grundlegende Voraussetzung für die Kontrolle des Einzelnen über seine Daten und für einen wirksamen Schutz personenbezogener Daten. Daher ist es von wesentlicher Bedeutung, dass jeder Einzelne von dem für die Verarbeitung seiner Daten Verantwortlichen auf **einfache und transparente** Weise hinreichend darüber aufgeklärt wird, wie, von wem, aus welchen Gründen und für welchen Zeitraum seine Daten gesammelt und verarbeitet werden, und welche Rechte er hat, wenn er seine Daten einsehen, berichtigen oder löschen möchte. Grundlegender Bestandteil dieser Transparenz ist die Anforderung, dass diese Informationen ohne Weiteres verfügbar und leicht verständlich sein müssen.
- Damit die Verarbeitung personenbezogener Daten rechtmäßig ist, sollten **personenbezogene Daten** stets auf der Grundlage einer **ausdrücklichen Einwilligung** der betroffenen Person (mit Bestimmungen über das Recht auf Rücknahme der Einwilligung) oder auf einer sonstigen zulässigen Rechtsgrundlage verarbeitet werden.
- **Die Einwilligung sollte in jeder geeigneten Form möglich sein**, so dass die betroffene Person ihre Wünsche frei, konkret, informiert und unzweideutig zum Ausdruck bringen kann und damit sichergestellt ist, dass sich der Einzelne voll und bewusst ist, dass er seine Einwilligung erteilt (beispielsweise durch Ankreuzen eines Kästchens auf einer Webseite). Wenn keine Äußerung oder Handlung erfolgt, sollte dies mithin keine Einwilligung darstellen. Jede Verwendung oder Übermittlung von Daten zu einem anderen als dem von der betroffenen Person gebilligten Zweck (z.B. im elektronischen Handel oder zu polizeilichen Zwecken) sollte nur zulässig sein, wenn dies einschlägige Rechtsvorschriften so vorsehen.
- **Die Einwilligung sollte jederzeit widerrufen werden können**, ohne dass dies negative Konsequenzen für die betroffene Person hat. Die betroffene Person sollte verlangen können, dass ihre personenbezogenen Daten gelöscht und nicht weiter verarbeitet werden. Grundsätzlich sollten alle Daten nach ihrer Analyse gelöscht werden, wenn eine weitere Vorhaltung nicht gerechtfertigt ist. Die Bedingungen, unter denen eine Rücknahme der Einwilligung nicht möglich ist, sollten in den Verfahrensbestimmungen über die „informierte Einwilligung“ detailliert dargelegt werden. Der für die Verarbeitung Verantwortliche muss hinreichende Gewissheit haben, dass es sich bei dem Einwilligenden tatsächlich um die betroffene Person handelt, und für IKT, die eine Verarbeitung von Daten der betroffenen Person erforderlich machen, müssen Instrumente für den Nachweis der Einwilligung zur Datennutzung (wie die digitale oder elektronische Unterschrift) verfügbar sein.
- **Kinder und hilfebedürftige Erwachsene** benötigen einen besonderen Schutz ihrer personenbezogenen Daten, weil ihnen die Risiken, Folgen und Sicherheitsgarantien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten sowie ihre diesbezüglichen Rechte möglicherweise weniger bekannt sind.
- Die Gruppe unterstützt die dem sogenannten Recht auf Vergessen zugrunde liegende Idee und

empfiehlt für den Onlinebereich, das **Recht auf Löschung personenbezogener Daten** dahingehend auszuweiten, dass sämtliche öffentlich verfügbaren Originale und Kopien gelöscht werden müssen.

- Die EGE empfiehlt, auch die Verarbeitung personenbezogener Daten von in der EU ansässigen betroffenen Personen durch einen nicht in der EU bzw. im EWR niedergelassenen für die Verarbeitung Verantwortlichen durch den normativen Rahmen der EU für den Datenschutzbereich zu regeln.

5.5 Soziale Aspekte: die digitale Kluft

5.5.1 Die digitale Kluft

Ein zentraler Faktor, den es bei allen Überlegungen über die Förderung der Nutzung von IKT in unterschiedlichen gesellschaftlichen Bereichen - von der elektronischen Verwaltung bis zu elektronischen Gesundheitsdiensten und vom elektronischen Geschäftsverkehr bis zu elektronischen Dienstleistungen - zu berücksichtigen gilt, ist die Umsetzung des Gerechtigkeitsprinzips und des Nichtdiskriminierungsgrundsatzes. Ethisch betrachtet wird eine solche Nutzung von IKT immer dann heikel, wenn sie vollständig an die Stelle herkömmlicher Dienstleistungen tritt und sich so auf die Gemeinschaft aller EU-Bürger auswirkt. Innovative Formen des Handels, der Verwaltung und der Gesundheitsversorgung können in der Tat eine bessere Qualität und nachhaltigere Dienste für den Bürger mit sich bringen. Dieses Ziel ist zweifelsohne beizubehalten und zu fördern, aber wer diese Politik propagiert, sollte stets im Hinterkopf behalten, dass sie möglicherweise den Grundsatz der partizipatorischen Gerechtigkeit berührt und sich auch auf den Dienstleistungszugang von Einzelnen und Gruppen auswirken kann, die keinen Zugang zu Dienstleistungen haben oder von diesen keinen Gebrauch machen können oder wollen.

Die Gesellschaft unterliegt einem raschen, kontinuierlichen und ständigen Wandel. Der innere Drang, nahezu fortwährend Neues zu erfinden bzw. wiederzuerfinden und Altes abzulegen, ist ein nur dem Menschen eigener Wesenszug, der auf dessen Streben nach Fortschritt und Wohlstand für die Menschheit beruht. Die heutige Gesellschaft wird von Technik beherrscht, und die meisten Menschen sind davon überzeugt, dass die immer neuen technologischen Entwicklungen ihr Leben und ihre Beziehungen zueinander verändert haben oder verändern können. Es gibt aber auch Menschen, die aus einer Vielzahl von Gründen nicht am digitalen Leben teilnehmen möchten, und diese Entscheidung,

die ja Ausdruck ihrer persönlichen Eigenständigkeit ist, muss respektiert werden. Da sie die IKT nicht in ihr tägliches Leben einfließen lassen, besteht gleichwohl die Wahrscheinlichkeit, dass ihre Wahlmöglichkeiten im digitalen Zeitalter zunehmend geringer werden. Nur weil sie sich dafür entschieden haben, den digitalen Technologien die kalte Schulter zu zeigen, sollten derartige „digitale Hinterwäldler“ aber unabhängig davon nicht vom Zugang zu wesentlichen Diensten ausgeschlossen werden, und ihnen darf auch nicht die Möglichkeit genommen werden, ihren gesellschaftlichen Pflichten (Teilnahme an Wahlen, Entrichten von Steuern usw.) nachzukommen. Im Interesse von Integration und Solidarität ist es mithin die Aufgabe der breiten Gesellschaft, sich dafür einzusetzen, dass zumindest kurz- und mittelfristig alternative Möglichkeiten zur Erfüllung dieser Pflichten geschaffen werden.

Damit das Recht der Bürger auf eine aktive Rolle in der europäischen Gesellschaft gewahrt bleibt und ihre Entscheidung bezüglich der von ihnen dafür ausgewählten Mittel respektiert wird, unterbreitet die EGE folgende Empfehlungen:

- Die EGE erkennt an, dass es anderer Konzepte, Inhalte und Anwendungen bedarf, um den besonderen Anforderungen von **benachteiligten** und **marginalisierten Gruppen** gerecht zu werden. Zu diesem Zweck empfiehlt die EGE der EU, zu prüfen, inwieweit mit Maßnahmen zur direkten Bereitstellung der betreffenden Dienste, mit Finanzhilfemaßnahmen und mit Regulierungsmaßnahmen sichergestellt werden kann, dass diese Gruppen nicht von einer umfassenden und aktiven Rolle in der digitalen Gesellschaft ausgeschlossen werden.
- Die EGE begrüßt die Anstrengungen der Kommission zur Beseitigung der **digitalen Kluft** und insbesondere die Zusammenarbeit mit internationalen Partnern, und sie empfiehlt der EU die Annahme von Strategien, die über die Bereitstellung eines öffentlichen Zugangs hinausgehen und Maßnahmen einschließen, welche darauf abstellen, dass von diesem Zugang auch effektiv Gebrauch gemacht werden kann. Dabei sollte es unter anderem darum gehen, Menschen die nötigen Fähigkeiten und die nötige Motivation zu vermitteln, damit diese das Potenzial von IKT im Rahmen von Bildungs- und Mentoringprogrammen, bei denen sie in einen sinnvollen und für sie nützlichen Lernprozess eingebunden werden, ausschöpfen können.

- Die EGE empfiehlt, dass in Bereichen, in denen die Bürger bestimmten gesellschaftlichen Verpflichtungen unterliegen oder in denen der Zugang zu wesentlichen Diensten ohne Rückgriff auf IKT nicht möglich ist, kurz- oder mittelfristig IKT-unabhängige Verfahren eingeführt werden.

5.5.2 Vereinbarkeit von Berufs- und Privatleben

Die EGE ist sich bewusst, welche Möglichkeiten eine stärkere Vernetzung im Berufsleben bietet, möchte aber auf die Risiken hinweisen, die die Kultur der ständigen Erreichbarkeit im Berufsleben mit sich bringt, so dass sich hinter dem Begriff „flexible Arbeitszeiten“ in Wirklichkeit die „Flexibilität“ verbirgt, dass atypisch und länger gearbeitet wird, was sich negativ auf das Familienleben auswirken kann. Daher sollten Arbeitnehmer wie Arbeitgeber die Nutzung von IKT in diesem Bereich überwachen und wirksam steuern.

- Die EGE drängt die EU, Organisationen dazu anzuregen und dabei zu unterstützen, explizite Strategien für eine optimale Nutzung von IKT zu entwickeln, bei der die **Vereinbarkeit von Berufs- und Privatleben** gewährleistet bleibt. Ziel derartiger Strategien sollte die Förderung einer Unternehmenskultur sein, bei der nicht erwartet wird, dass die Beschäftigten in ihrer Freizeit „auf Abruf“ bereitstehen. Dieser Aspekt sollte auch in die Programme zum Thema soziale Verantwortung von Unternehmen und in die Arbeitsordnungen einfließen.

5.6 Politische Mitbestimmung

Der Einfluss, den die IKT auf die Politikgestaltung haben können, gibt, was das Recht des Bürgers auf freie Information, die Fähigkeit von Interessengruppen zur Wahrnehmungsveränderung und die Möglichkeiten des Staates zur Internetzensur angeht, Anlass zu Bedenken. Angesichts des großen, im ersten Teil dieser Stellungnahme beschriebenen Einflusses von IKT auf die moderne Gesellschaft setzen die Regierungen in der ganzen Welt neue Mittel ein, um mit der Onlinewelt zu interagieren: Filter und Sperren, Registrierungspflicht, Überwachungsbefugnisse, Haftung von Intermediären usw. Die Struktur der zur Wissensvermittlung und zur Kommunikation eingesetzten Instrumente wirft bei all ihren Verwendungsformen Fragen bezüglich der Lenkung von Wissen und Informationen zum Zwecke der Realitäts- und Meinungsbildung im digitalen Zeitalter auf, darunter das Risiko einer möglichen Online-Verbreitung von verzerrt dargestellten Informationen zu

politischen Zwecken. Diesbezüglich empfiehlt die EGE folgende Maßnahmen:

- Die EGE erkennt an, dass die Grundeigenschaft des Internets die freie und aktive Mitwirkung seiner Nutzer ist. Sie betont die Notwendigkeit, **die Freiheit und die Neutralität des Internets zu wahren**. Gleichwohl darf diese Freiheit nicht den grundlegenden ethischen Werten der EU zuwiderlaufen.
- Das Internet muss ein Kommunikationsbereich bleiben, in dem **die Meinungsfreiheit** nach Maßgabe der Charta der Grundrechte **gegen Zensur geschützt wird**.
- Die EGE sieht die Notwendigkeit eines ausgewogenen Verhältnisses zwischen einer von oben nach unten erfolgenden Steuerung des Internet durch Regierungsstellen und den von unten nach oben gerichteten partizipatorischen Ansätzen der Internetgemeinschaft. Sie betont daher, dass die EU, die Mitgliedstaaten und sonstige wichtige Akteure bei ihren gemeinsamen Beratungen ein **transparentes Mitbestimmungskonzept in den Entscheidungsfindungsprozess einbeziehen** sollten. Dies gilt für alle Regulierungsmaßnahmen im IKT-Bereich.

5.7 Empfehlungen für den Handelsbereich

5.7.1 Handelsgeschäfte

Die EGE unterstreicht die Notwendigkeit, die Rechte und die Interessen der EU-Bürger zu wahren. Sie begrüßt daher die von der Europäischen Kommission vorgeschlagene Strategie für die soziale Verantwortung der Unternehmen, welche vorsieht, dass die Unternehmen, um ihrer Verantwortung nachkommen zu können, auf ein Verfahren zurückgreifen können sollen, mit dem soziale, ökologische, ethische, Menschenrechts- und Verbraucherbelange in enger Zusammenarbeit mit den „Stakeholdern“ in die Betriebsführung und in ihre Kernstrategie integriert werden (KOM(2011) 681 endg.). Die EGE begrüßt zudem die von der EU und von internationalen Gremien ergriffenen Maßnahmen zur Wahrung der Netzneutralität (siehe beispielsweise KOM(2011) 222 endg.), weist jedoch auf die Notwendigkeit der in dieser Stellungnahme vorgeschlagenen Maßnahmen zum Thema Verantwortung (des Einzelnen, von Unternehmen, der Gesellschaft und der Regierungen) hin. Daher sollte die Schaffung von geeigneten Instrumenten (und deren Umsetzung) gefördert

werden, mit denen sich diese Ziele verwirklichen lassen – und zwar angefangen bei der sozialen Verantwortung der Unternehmen (KOM(2011) 681 endg.) bis hin zu einem einschlägigen Verhaltenskodex (Maßnahmen der Kommission für eine verantwortungsvolle Nutzung des „Cloud computing“, „Internet der Dinge“, Empfehlung für verantwortungsvolle Innovationen - 2012 usw.). Zu diesem Zweck empfiehlt die EGE folgende Maßnahmen:

- Die EGE erkennt an, dass es ein **ausgewogenes Verhältnis zwischen der Nutzung von IKT zu kommerziellen Zwecken und ihrer Verwendung zu nicht kommerziellen Zwecken** zu schaffen gilt. Sie empfiehlt der Europäischen Kommission, 1.) ihre Datenschutzvorschriften zur Anwendung zu bringen und dafür Sorge zu tragen, dass soziale Netzwerke verantwortungsvoll mit den ihnen von ihren Nutzern mitgeteilten Daten umgehen; 2.) die Nutzer darüber aufzuklären, dass es sich bei sozialen Netzwerken zumeist um gewerbliche Unternehmen handelt, die die Daten für kommerzielle Zwecke verwenden müssen, um die von ihnen angebotenen Dienste erbringen zu können; 3.) alle verfügbaren Mittel für die Schaffung eines (voraussichtlich auf den bestehenden Netzen aufbauenden) Raums der sozialen Netze bereitzustellen, in dem es keine gewerbliche Nutzung gibt und der allen Nutzern offensteht (wenngleich sie unter Umständen für dieses Vorrecht bezahlen müssen).
- Die EGE ist der Auffassung, dass Menschen, die einen Handelsvertrag abschließen möchten, in eindeutiger, präziser und verständlicher Weise über die Bestimmungen und Bedingungen eines solchen Vertrags aufgeklärt werden sollten.

5.7.2 Soziale Verantwortung der Unternehmen

Für den Schutz der Privatsphäre sind insbesondere die Grundsätze der im Oktober 2011 von der Europäischen Kommission angenommenen Strategie für die soziale Verantwortung der Unternehmen maßgeblich. Die Strategie zeigt auf, wie Unternehmen sich ihre soziale Verantwortung zunutze machen und gleichzeitig einen Beitrag zur Gesellschaft insgesamt leisten können, in dem sie sich nach Kräften bemühen, ihren sozialen Verantwortlichkeiten nachzukommen.

- Die EGE begrüßt diese Initiative und empfiehlt der EU, die Unternehmen dazu zu ermutigen, bei der

Umsetzung ihrer Politik für ihre soziale Verantwortung auch dem Schutz der Privatsphäre Rechnung zu tragen und dabei auch auf technologische Lösungen wie Datenschutz-Folgenabschätzungen, Technologien für einen besseren Schutz der Privatsphäre und einen „eingebauten Datenschutz“ zu setzen.

5.8 Kreuzkorrelative Datenerschließung

Die kreuzkorrelative Datenerschließung kann eine wichtige Rolle spielen, wenn aus einer Vielzahl von Quellen zusammengestellte Datenbanken gemeinsam analysiert werden, um Informationen zu erschließen, die in den einzelnen Datenbanken als solche nicht enthalten sind. So liefert beispielsweise die Verknüpfung von über Kundenkarten zusammengetragenen Einkaufsdaten mit Bankdaten und/oder mit Gesundheitsdaten Aufschlüsse über die Gewohnheiten eines Menschen, die ansonsten vielleicht nicht auf Anhieb erkennbar gewesen wären. Eine derartige Datenverknüpfung erfolgt oftmals unter Verwendung von Daten von Bürgern, die einer solchen Verwendung nicht ausdrücklich zugestimmt haben, und diese kann die Erstellung des Profils von nicht aufgeklärten und sich dieser Möglichkeit gar nicht bewussten Personen ermöglichen, wobei das Risiko einer Stigmatisierung dieser Personen und einer Verletzung ihrer Privatsphäre bestehen kann. Daher empfiehlt die EGE folgende Maßnahmen:

- **Einzelpersonen sollten** von Unternehmen, staatlichen Stellen und Forschungsgremien **ausdrücklich darüber informiert werden**, dass ihre Daten zu bestimmten Zwecken einer Datenerschließung unterzogen werden können. Auf diese Weise wäre sichergestellt, dass jeder Einzelne eine „informierte“ Entscheidung darüber treffen kann, auf welche Dienste er zurückgreift. Immer wenn Datenbanken zueinander in Beziehung gesetzt werden sollen, sollte zuvor die ausdrückliche Einwilligung der betroffenen Personen eingeholt werden. Daher sollten weitere Forschungsarbeiten über die **Auswirkungen der kreuzkorrelativen Datenerschließung auf die Privatsphäre** durchgeführt werden, damit die potenziellen Vorteile dieses Verfahrens der Gesellschaft zum Nutzen gereichen können, gleichzeitig aber die Menschenrechte gewahrt bleiben. Zudem empfiehlt die EGE der EU, näher zu prüfen, ob bzw. unter welchen Bedingungen sensible Daten – u.a. für die kreuzkorrelative Datenerschließung – verwendet werden können.

5.9 Umwelt und Rohstoffe

Das Verhältnis zwischen den IKT und der Umwelt ist überaus komplex, denn die IKT können sich sowohl positiv als auch negativ auf die Umwelt auswirken. So können die IKT äußerst positive Auswirkungen auf die Umwelt haben, wenn sie als Mittel zum Schutz der Umwelt genutzt werden, sei es zur Überwachung von Umweltaspekten, zur Steuerung von Systemen zum Schutz der städtischen Umwelt, zur Weitervermittlung von Umweltkenntnissen, zur Verbreitung von Informationen an die Öffentlichkeit, zur Förderung einer aktiven Bürgerbeteiligung, zur Vereinfachung einer effizienten Ressourcenverwendung, zur Minderung des Verbrauchs von Energie und wichtigen natürlichen Ressourcen (Beispiel: Reduzierung des Papierverbrauchs durch elektronische und papierlose Kommunikation) oder für eine bessere Nutzung natürlicher Ressourcen. Als Beispiel für eine solche Transformation ist insbesondere die Nutzung von IKT zur Verbesserung landwirtschaftlicher Praktiken, zur Überwachung der Luft- und der Wasserverschmutzung, zur Katastrophenvorhersage sowie zur Effizienzverbesserung in den Bereichen Energie, Verkehr, Güter und Dienstleistungen zu nennen. Auch kann der Rückgriff auf elektronische Kommunikationsmittel wie E-Mail oder Videokonferenzen zu einem geringeren Verkehrsaufkommen beitragen.

Gleichzeitig gilt es an der Nachhaltigkeit dieser Technologien zu arbeiten, um nicht eingeplante Folgen wie einen höheren Energieverbrauch, die Entsorgung gebrauchter Elektronikgeräte oder die Verschwendung von Rohstoffen wie seltenen Erden zu vermeiden. Zahlreiche Elektronikgeräte erfordern in der Herstellung einen extensiven Rückgriff auf seltene chemische Elemente wie Tantal, Lanthan oder Dysprosium, und moderne Batterien und Akkus bestehen größtenteils aus Lithium. In den Ländern, die Mineralien, welche diese Elemente enthalten, fördern, führt die Nachfrage nach diesen Metallen zu sozialen und ökologischen Problemen. Außerdem werden bestimmte Elemente überhaupt nur in einigen wenigen Ländern gefördert. Wer IKT nutzen möchte, ist mithin auf Energie und auf bestimmte Rohstoffe angewiesen, und den damit verbundenen Unsicherheiten gilt es Rechnung zu tragen.

- Die EGE empfiehlt, die Auswirkungen von IKT auf die Umwelt (Energieverbrauch, Abfallproduktion und Rohstoffeinsatz) zu quantifizieren, anzuerkennen, zu analysieren und zu kommunizieren und die Ausbeutung natürlicher Ressourcen auf ein Minimum zu beschränken.

- Die EGE empfiehlt der EU, die Unsicherheiten, die wegen der Rohstoffknappheit in Bezug auf das derzeitige IKT-System bestehen, näher zu analysieren.
- Der Gruppe ist bekannt, dass bereits in mehreren Berichten bemängelt wurde, dass bestimmte Mineralien, die von wesentlicher Bedeutung für die Herstellung von IKT-Hardware sind, unter menschenunwürdigen Bedingungen gefördert werden. Die Gruppe fordert die EU daher auf, sich für bessere Arbeitsbedingungen der in diesem Sektor tätigen Personen einzusetzen, so dass die Menschenrechte gewahrt werden. Diese Anforderung sollte auch in die von der EU finanzierten Entwicklungsprogramme aufgenommen werden.

5.10 Abschließende Empfehlung

Die EGE erkennt das Potenzial der Digitalen Agenda für Europa an und unterstreicht die Notwendigkeit einer verantwortungsvollen, integrativen und sozial nachhaltigen Umsetzung dieser wichtigen Politik. Die Gruppe empfiehlt daher, die Maßnahmen der Digitalen Agenda für Europa in Übereinstimmung mit den Grundwerten der Europäischen Union zu fördern. Zudem betont sie die Notwendigkeit, im Rahmen der IKT-Programme von „Horizont 2020“ Bildungs- und Forschungsmaßnahmen in den Bereichen Ethik, Recht, Gesellschaft und Umwelt zu finanzieren.

EGE Secretariat

Address:

European Commission
Berl 8/362
1049 Brussels
Fax +32 22994565
E-mail: BEPA-ETHICS-GROUP@ec.europa.eu
Internet: http://ec.europa.eu/european_group_ethics/index_en.htm



Maurizio Salvi

MBA, MBS, PhD, D. Biotech.
European Commission
Head BEPA Ethics sector
Head of the EGE Secretariat
General Secretary EC IBD

Berl 8/359 — 1049 -Brussels
E-mail: maurizio.salvi@ec.europa.eu



Kim Hoang Le

European Commission
EGE Secretariat

Berl 8/362 — 1049 Brussels
Tel. +32 22999228
E-mail: Kim-Hoang.LE@ec.europa.eu



Adriana-Sorina OLTEAN

European Commission
EGE Secretariat

Berl 8/362 — 1049 Brussels
Tel. +32 22993016
E-mail: Adriana-Sorina.Oltean@ec.europa.eu

Opinion No. 26
Ethics of Information and Communication Technologies

Luxembourg: Publications Office of the European Union

2012 — 87 pp. — 21 x 29.7 cm

ISBN 978-92-79-22734-9

doi:10.2796/13541

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- via EU Bookshop (<http://bookshop.europa.eu>);
- at the European Union's representations or delegations. You can obtain their contact details on the Internet (<http://ec.europa.eu>) or by sending a fax to +352 2929-42758.

Priced publications:

- via EU Bookshop (<http://bookshop.europa.eu>).

Priced subscriptions (e.g. annual series of the *Official Journal of the European Union* and reports of cases before the Court of Justice of the European Union):

- via one of the sales agents of the Publications Office of the European Union (http://publications.europa.eu/others/agents/index_en.htm).

