THE USV ANNALS OF ECONOMICS AND PUBLIC ADMINISTRATION | VOLUME 13, ISSUE 2(18), 2013

INTERNET OF THINGS – SOME ETHICAL ISSUES

Lecturer PhD **Daniela POPESCUL**
„Alexandru Ioan Cuza" University of Iaşi, Romania
rdaniela@uaic.ro

Professor PhD **Mircea GEORGESCU**
„Alexandru Ioan Cuza" University of Iaşi, Romania
mirceag@uaic.ro

Abstract:
The purpose of this study is to treat aspects that are related to the sensitivity of data, information and knowledge transmitted through Internet of Things, helping all people interested in these new ICT technologies to become aware of some ethical issues. In this new media, which is no more in its infancy, the vulnerabilities and attacks are various, caused by technological advances and proliferated through lack of users' awareness. This warning message is needed because of data, information and knowledge transfer from virtual to physical devices that are connected to wireless networks of different sizes and importance. The transfer is augmented by the extended use of new technologies as RFID, NFC, sensors, 3G and 4G and brings along the adjustment of the traditional information security threats to this new environment, as well as the emergence of new characteristic dangers. The problems treated here are of interest both for each of us, as individuals, and for the organizations managers – especially in a world in which the borderline between the physical and virtual life is becoming more and more difficult to draw.

Key words: ICT ethics, Internet of Things, NFC, RFID, sensors

JEL classification: L86, M15

INTRODUCTION

The aspects related to ethics in information and communication technology have been a subject of study for the academic world and the wide public since the appearance of computers and the prefiguration of artificial intelligence. Thus, it is said that information and communication technologies are of an emergent and creative nature (Berthon, Leyland and Watson, 2008), and explicitly or implicitly they overtake some of our tasks and delicately induce certain moods or even force certain behavior patterns, following their own development and functioning logic, imperatively heading to maximum efficiency. Society can only answer to this by adapting and accepting the situation (Niculescu-Dincă, 2010). Currently, research goes round the so-called green technologies (Radu, 2012-1, 2012-2, 2013-1), calm technologies (Ţugui, 2011-1, 2011-2), Big Data (Davis, 2012, Danubianu, Bărîlă, 2013), cloud computing (Ţugui and Şiclovan, 2013), the impact of socializing networks on people and communities (Fukuyama, 2002, Bard and Söderqvist, 2010, Man, 2013, Stoica, 2013, Radu, 2013-2, Vătuiu and Udrică, 2013, Jeder, 2013, Maxim and Socaciu, 2013).

One of the contemporary technological accomplishments which raises a great number of ethical questions is the Internet of Things. In the Internet of Things, the physical things connect to other physical things, using wireless communication and offering contextual services. According to Business Insider, which quotes one of Morgan Stanley`s predictions (Danova, 2013), more than 75 billions of objects will be connected to the Internet of Things by 2020. Hence, in 2011, the European Commissioner, Gerald Santucci, head of Internet of Things and Future Internet Enterprise Systems Unit from the European Committee underlined the fact that "The Internet of Things does not refer only to things, but also to the relationship between the objects which surround the people daily and the people themselves" and he was wondering: "What place will the human beings have in a world in which 7 billions of people live together with 70 billion cars and a few thousand of billions of objects connected to an infrastructure of global networking, having the ability of self-

coordination, self-configuring and self-diagnosis?" (Santucci, 2011). Similar questions are asked by Sarma, Brock and Ashton, 2000, Karimi, 2013, Van den Hoven, 2013 and they are also the topic of this paper.

INTERNET OF THINGS SPECIFIC TECHNOLOGIES AND CHARACTERISTICS – DRIVERS OF ETHICAL PROBLEMS

The ethical issues are caused by the expansion on a very large scale of the IoT specific technologies and characteristics. IoT is based on a global infrastructure network which connects physical and virtual objects in a unique way, by exploiting the data captured by the sensors, the equipment used for communication and localization. The RFID technology lies at the basis of this development, but the concept of Internet of Things has spread by incorporating technologies such as Near Field Communication, 2D bar codes, wireless sensors, localization technologies, 3 or 4G communications.

RFID (Radio Frequency Identification) is a technology which uses electromagnetic fields to automatically identify objects, by labeling them with a chip or two antennae, called „tag". The tag sends a unique electronic code which is read by a reader which can be placed anywhere. The tags are all different and RFID can be used to automatically track objects, including those attached to people (ski pass, driving license, time tags, bracelets for pupils) and those injected or implanted within human or animal skin (for medical purposes, but also for the VIP access in certain areas – for example Baja Beach Club from Barcelona), making an inventory on the spot for all the products in a warehouse or the shopping basket in a supermarket. Also, tags can be attached to mobile phones for various reasons, so on.

The sensors included in the connected objects can be of different natures – of proximity, temperature, ambient light, accelerometers and others. Only a small part of the electronic and household devices sold nowadays do not include sensors - a smart phone or a tablet, for example, is equipped with at least 10 sensors. They play a very important role in establishing the relationship between the virtual world and the parameters of the physical world and they allow the objects to react to the changes from the environment where they are placed. Some of these sensors are nanosensors, namely sensors of dimensions of one billionth of a meter. They can be used to diagnose illnesses such as AIDS, to detect the level of pollution in water, to be attached to robots which help and save lives in case of disasters and so on. Starting from the abundance of sensors in contemporary world, we can speak about Remote Emotive Computing (REC) – a technique of retrieving and processing human emotions with computers based on sensors. An example of REC use is given by Karimi, 2013, who invites us to imagine an individual who is monitored all the time by sensors which note all of his actions, feelings and movements. The received data is sent to an application which gives back answers related to food, life style or … getting involved in a relationship. In such a case, the car driven by the individual might alert the police if it "feels" that the person drank alcohol. According to Wheatley, 2013, Google sent in 2012 a request to patent a device which receives the environment sounds heard at the same time with a conversation on a computer microphone or phone so that it could identify exactly what the user is doing and could make an advertisement highly adapted to the surrounding environment. A similar technology, but more debatable from the ethical point of view, was accomplished by Verizon who wishes to integrate active web cameras in TVs, DVRs or phones and monitor the users' everyday activities.

IoT uses also localization technologies. There are available many devices which can localize a certain object at a certain moment, the most popular one being GPS. *GPS (Global Positioning Solutions)* is a system controlled and financed by the American Department of Defense. GPS uses satellites to monitor (vertically and horizontally) the position held by a user, his speed and current timing, depending on the place he is in. It can be used anywhere in the world, including on planes and ships. The GPS receptors estimate the position according to the satellites which orbit the earth

at a speed of approximately 3 km/ s. There are visible 5 to 8 satellites from any spot on earth. Consequently, the accuracy in positioning is quite high, 100 m horizontally and 156 m vertically, but the error rate is quite small, only a few meters.

NFC (Near Field Communication) is a radio device, on a frequency of 13.56 MHz, which can establish the communication between two objects which are in an area of up to 20 cm. The data exchange speed can reach a maximum of 424 kbit/s, and the time to make the connection is smaller than 1/10 seconds. The possible uses of NFC are contactless payments (by simply approaching the mobile phone to a special reader), sharing information in social networks, replacing identity cards or door keys, so on. According to Wikipedia (2013), in Germany, Austria, Finland, New Zeeland, Italy, Iran and Turkey there have been set up NFC payment devices for public transport networks.

3G is the acronym used for the third generation of mobile phones. The technology used to transfer voice and data (including videos) allows downloading software, email and instant messaging communication. *4G* is a combination between 3G and WiMax. WiMax (Worldwide Interoperability for Microwave Access) has a larger coverage area and a wider band than Wi-Fi. 4G combines the area of great 3G coverage with the WiMax speed, the result being the mobile access to Ethernet speeds (approximately 10 Mbps), in local networks as well as in large ones.

The combination of these technologies can create science fiction environments in which more and more activities will be accomplished unrelated to the objects surrounding us, being capable to communicate and this gives the possibility to make new businesses, inconceivable today. The services offered by technology might be adapted depending on the actions done by the individual, the device, the infrastructure or nature at that particular moment. Other potential uses of the Internet of Things are those related to households, smart cities and health monitoring devices. Taking into consideration these aspects, a report from the European Commission made by Van den Hoven, 2013, in the context of the Digital Agenda for Europe mentions the characteristics of the Internet of Things (IoT) which might cause ethical problems:

• *Ubiquity, omnipresence* – the user is attracted to IoT, devoured by it, there is no clear way out, a way to give up using the artifacts (which will no longer be possible at some point, due to the producers which will equip them with Internet connection devices);

• *Miniaturization, invisibility* – computers, as they are nowadays, will disappear – the devices will be smaller and smaller, transparent, thus avoiding any inspections, audit, quality control and accounting procedures;

• *Ambiguity* – the distinction between the natural objects, artifacts and beings will be more and more difficult to be made as a consequence of the easy transformation from one category into another based on tags, advanced design and absorption in new networks of artifacts. There will appear serious problems of identity and system boundaries;

• *Difficult identification* – in order to be connected to the IoT, the objects will have an identity. The access to these „armies" of objects, the management of these identities might raise great interest and cause serious problems of security and control in a globalized world;

• *Ultra-connectivity* – the connections will increase in number and reach unprecedented scales of objects and people. Consequently, the quantities of transferred data and products will increase greatly (Big Data), and they could be maliciously used;

• *Autonomous and unpredictable behavior* – the interconnected objects might interfere spontaneously in human events, in unexpected ways for the users or the designers. The people will be part of the IoT environments together with artifacts and devices, thus creating hybrid systems with unexpected behavior. The incremental development of IoT will lead to emerging behaviors without the users fully understanding the environment they are exposed to;

• *Incorporated intelligence*, which makes the objects be seen as substitutes for the social life – the objects will be intelligent and dynamic, with an emerging behavior; they will be extensions (not only external) of the human mind and body. Being deprived of these devices will lead to problems – see the teenagers who consider themselves cognitively or socially handicapped without Google, a

smart phone or social media;

• *Difficult control* – the IoT control and governance will not be centralized, as a consequence of the great number of hubs, switches and data. The information flows will be eased; the transfers will be quicker and cheaper, not easy to be controlled. There will appear emerging properties and phenomena which will require monitoring and governance in an adequate way and this will further influence the accountancy and control activities.

ETHICAL CHALLENGES IN IOT

Ethics in the TIC field refers to the use according to the social behaviour standards. The majority of ethical debates appear around property, accessibility, acuracy and private use of information. According to authors Valacich and Schneider (2010, p. 484), an ethical behaviour requires:

• *enforce the property rights* on information;
• *ensure the access* to information;
• *ensure the integrity* of the information;
• enforce the right to *private life.*

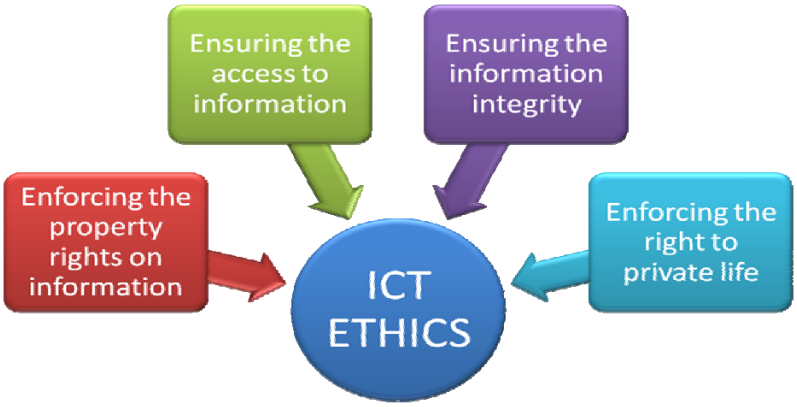

Figure 1 – Central ICT ethics issues – accesibility, privacy, property and integrity of information

Source: Valacich, J., Schneider, C., *Information Systems Today. Managing in the Digital World*, 4th Edition, Pearson Publishing House, Boston, 2010, p. 484

The impact of technologies and the characteristics mentioned above on the four features of the ethical behaviour are presented in figure 2.

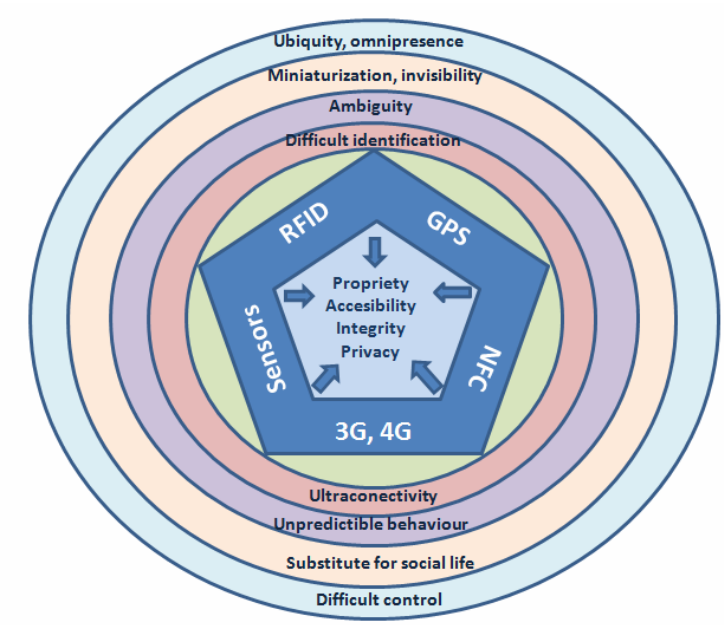

Figure 2 – The impact of IoT technologies and characteristics on the ethical behavior

A few of the ethical issues which derive from these characteristics are discussed in the following part.

As regards the *property right on data and information*, the difficulties will appear from the correct identification of the authors – for example, an answer to the question ”Who is the owner of the data retrieved by the sensors of the objects connected to the Internet of Things?” is hard to imagine at this point. When the information is personal or financial data, things get more serious. The IoT omnipresence will make the boundaries between the public and private space be invisible, and people will not know where their information ends up. The Big Brother type surveillance, namely monitoring the individuals without them being aware of it will be possible. The objects will be equipped with sensors which will allow them to ”see”, ”hear” or even ”smell”. The data registered by the sensors will be sent in great quantities and in different ways through networks, which will bring prejudice to the individual private life. By means of RFID, GPS and NFC technologies, the geographic place where a person is and his movements from one place to another can be easily found without his knowledge. The information collected from a chip implanted with the person’s consent (for medical purposes) might be maliciously used. There might be also created individual profiles depending on their consumption habits and evil outsiders might make decisions related to them.

Related to *accessibility* of information, if a contemporary attack on a PC might cause information loss or spreading, a virus or hacker attack in IoT might have a direct influence on people’s lives. For example, interfering in the control system of a car connected to IoT might endanger the life of the passengers – this type of attacks have already been proven as possible (for example, the hackers could interfere on the on-board computer by an MP3 players). Recent news from Sky News, 2013 mention sales on the black market of the computer worm called Stuxnet and the experts in IT security say that it could be used to attack any physical target which is related to computers. The list of vulnerable systems is almost endless – it includes the electric heating systems, food distribution networks, hospitals, traffic lights systems, transport networks and even weirs. The attack scenarios which might be envisaged starting from here are scaring.

The digital divide will increase in the Internet of Things, as it will be understood only by experts. It is debatable whether there is possible a fair distribution of benefits and costs as well as the real presence of equal opportunities in accessing the IoT advantages. Moreover, the communication from one device to another will influence people’s lives in ways which are hard to imagine as long as there will not be a coherent, legal and democratic frame to delineate the limits of

this process.

CONCLUSIONS

Even in the context of the non-exhaustive overview of the above presented dangers, we believe that the Internet of Things represents, if incorrectly managed, a danger from the perspective of ethics for the contemporary individuals and organizations. Every individual needs to be ensured that he/she will be protected by effective technical solutions, re-interpreted and updated for IoT (as, for example, encryption techniques, ID management, privacy enhancing technologies, digital watermarking, electronic signature etc..), legal/regulatory mechanisms (consumers consent, legislation limiting the data collected and used by third parties, accountability of transactions mediated by IO etc.), economical measures (self-regulation, codes of conduct, consumer education, privacy certification) and social ones (public awareness, disclosure, public advocacy, consumer rights). After these first steps of awareness, further research must be done methodically on interventions needed to prevent the turning of IoT into a feared and intrusive Big Brother.

REFERENCES

1. Bard, A., Söderqvist, J. (2010), Netocraţia - *Noua elită a puterii şi viaţa după capitalism*, Editura Publica.
2. Berthon, P., Leyland, P., Watson, R. (2008), *From Genesis to Revelation: The Technology Diaspora*, Communications of the ACM, December 2008, Vol. 51, No. 12, pp. 151-154.
3. Danova, T., (2013) *Morgan Stanley: 75 Billion Devices Will Be Connected To The Internet Of Things By 2020*, http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10#ixzz2jIo3UCkd, 2.10.2013, accessed at 13.10.2013.
4. Danubianu, M., Bărîlă, A. (2013), *Big Data – a chance to change the academic scene?,* Proceedings of the International Conference SMART 2013 - Social Media in Academia: Research and Teaching, June 6-9, Bacau, Romania (edited by Bogdan Patrut), Medimond - Monduzzi Editore International Proceedings Division, Bologna, Italy, pp. 175-181.
5. Davis, K. (2012), *Ethics of Big Data: Balancing Risk and Innovation*, O`Reilly Media Press, Sebastopol.
6. Fukuyama, F. (2002), *Marea ruptură. Natura umană şi refacerea ordinii sociale*, Editura Humanitas, Bucureşti.
7. Jeder, D. (2013), *M-learning and social media in the professional development of teachers,* Proceedings of the International Conference SMART 2013 - Social Media in Academia: Research and Teaching, June 6-9, Bacau, Romania (edited by Bogdan Patrut), Medimond - Monduzzi Editore International Proceedings Division, Bologna, Italy, pp. 199 -201.
8. Karimi, K. (2013), *Why harp on Internet of Things security and privacy issues?*, The Embedded Beat, la https://community.freescale.com/community/the-embedded-beat/blog/2013/09/13/why-harp-on-internet-of-things-security-and-privacy-issues, 13.09.2013, accessed at 14.09.2013.
9. Man, Y. (2013) *The correct use of communities formed on the basic of social media,* Proceedings of the International Conference SMART 2013 - Social Media in Academia: Research and Teaching, June 6-9, Bacau, Romania (edited by Bogdan Patrut), Medimond - Monduzzi Editore International Proceedings Division, Bologna, Italy, pp. 116-122.
10. Maxim, I., Socaciu, I. T. (2013), *Social media facilities in collaborative learning*, Proceedings of the International Conference SMART 2013 - Social Media in Academia: Research and Teaching, June 6-9, Bacau, Romania (edited by Bogdan Patrut), Medimond - Monduzzi Editore International Proceedings Division, Bologna, Italy, pp. 220-223.
11. Niculescu-Dincă, V. (2010), *Integritate prin design – despre tehnologie şi etică*, dosar Dilema Veche, anul VII, nr. 331, 17-23 iunie 2010, p. VII.
12. Radu, D. L. (2012), *Company Characteristics and Consumer Preferences – Prerequisites for Adopting Decisions Involving Organizations in Green ICT Innovation*, 19th IBIMA conference

on Innovation Vision 2020: Sustainable growth, Entrepreneurship, Real Estate and Economic Development, 2012, pp. 1488-1493.
13. Radu, D. L. (2012), *Innovation, ICTS and Environment- A Complex and Controversial Relationship*, 6th International Conference on Globalization and Higher Education in Economics and Business Administration, Iasi, pp. 1256-1261.
14. Radu, D. L. (2013) - 1, *The Role of Consumers, Producers, and Regulatory Authorities in the Evolution of Green ICTs*, 21th IBIMA conference on Vision 2020: Innovation, Development Sustainability, and Economic Growth, 27-28 June, pp. 963-970.
15. Radu, D. L. (2013) - 2, *The Influence of Social Media on Green IT*, Proceedings of the International Conference SMART 2013 - Social Media in Academia: Research and Teaching, June 6-9, Bacau, Romania (edited by Bogdan Patrut), Medimond - Monduzzi Editore International Proceedings Division, Bologna, Italy, pp. 213-219.
16. Santucci, G. (2011), *The Internet of Things: A Window to Our Future,* la http://www.theinternetofthings.eu /content/g%C3%A9rald-santucci-internet-things-window-our-future, accessed at 2.09.2013.
17. Sarma, S., Brock, D. L., Ashton, K. (2000), *The Networked Physical World. Proposals for Engineering the Next Generation of Computing, Commerce & Automatic-Identification*, White Paper of the Auto-ID Center at the MIT, Cambridge, MA.
18. Stoica, M. (2013), *Universities in the era of Web 2.0. Social Media facilitating improvement of quality of education*, Proceedings of the International Conference SMART 2013 - Social Media in Academia: Research and Teaching, June 6-9, Bacau, Romania (edited by Bogdan Patrut), Medimond - Monduzzi Editore International Proceedings Division, Bologna, Italy, pp. 109-115.
19. Ţugui, A. (2011), *Calm Technologies: A New Trend for Educational Technologies*, World Future Review, 3 (1).
20. Ţugui, A. (2011), *Educational Technologies Oriented towards Calm Technologies*, Analele Universităţii Alexandru Ioan Cuza Iaşi.
21. Ţugui, A., Şiclovan, A. (2013), *Social Media interaction via Cloud Computing,* Proceedings of the International Conference SMART 2013 - Social Media in Academia: Research and Teaching, June 6-9, Bacau, Romania (edited by Bogdan Patrut), Medimond - Monduzzi Editore International Proceedings Division, Bologna, Italy, pp. 239-245.
22. Valacich, J., Schneider, C., (2010), *Information Systems Today. Managing in the Digital World*, Ediţia a 4-a, Editura Pearson, Boston
23. Van den Hoven, J. (2013), *Internet of Things Factsheet Ethics*, http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation, 28.02.2013, accessed at 2.09.2013.
24. Vătuiu, T., Udrică, M. (2013), *Virtual learning environment as part of lifelong learning*, Proceedings of the International Conference SMART 2013 - Social Media in Academia: Research and Teaching, June 6-9, Bacau, Romania (edited by Bogdan Patrut), Medimond - Monduzzi Editore International Proceedings Division, Bologna, Italy, pp. 123-128.
25. Wheatley, M. (2013), *Big Brother's Big Data: Why We Must Fear The Internet Of Things?*, http://siliconangle.com/blog/2013/01/10/big-brothers-big-data-why-we-must-fear-the-internet-of-things/, 10.01.2013, accessed at 14.09.2013.