TRUESSEC.EU – EUROPEAN VALUES AND THE DIGITAL SINGLE MARKET FROM AN ETHICAL PERSPECTIVE

Hristina Veljanova

Researcher, University of Graz, Institute of Philosophy, Section Political Philosophy
Heinrichstraße 26/II, 8010 Graz, AT
hristina.veljanova@uni-graz.at; https://philosophie-gewi.uni-graz.at/de/politische-philosophie/

Keywords: ***ICT products and services, ethical issues and challenges, privacy, security***

Abstract: *At the IRIS2017 Griesbacher/Staudegger/Stelzer introduced the Horizon2020 project TRUESSEC.eu. Their contribution was entitled «SSH in ICT Using the Example of TRUESSEC.EU». This year, preliminary project findings will be elaborated from a multidisciplinary perspective. This contribution maps out the ethical issues and challenges that arise when using ICT products and services. These issues and challenges are analysed with a view to fundamental rights and European values. In a next step, the findings will be integrated within the TRUESSEC.eu Multidisciplinary Criteria Catalogue.*

1. TRUESSEC.eu and the Digital Single Market

TRUESSEC.eu is a Coordination and Support Action (CSA) funded by the European Commission. It focuses on certification and labelling of trustworthiness properties of ICT products and services. By taking a multidisciplinary approach and merging Social Sciences and Humanities (SSH) and ICT, the project aims at strengthening the promotion, protection and respect of human rights and European values in light of the European Union's efforts to boost the digital single market.

As a response to the low level of trust of Europeans in companies operating online as well as the numerous concerns they have about being asked to disclose too many personal data[1], the main aim of the TRUESSEC.eu project is to provide an answer to the question: *How can ICT products and services be made more trustworthy?*. Ethics, as one of the disciplines represented in the project, can offer valuable insights into the matter. Ethics can help identify the main issues and challenges that arise when using and designing ICT products and services. Moreover, ethics can also help define from a normative perspective the main elements and requirements that present a necessary condition for building trustworthy ICT products and services. Both of these aspects will serve as a solid ground for the development of the TRUESSEC.eu Multidisciplinary Criteria Catalogue for Trustworthy ICT Products and Services. Against this background, this contribution builds upon the findings of the Support study of ethical issues which was prepared as part of the TRUESSEC.eu project.

2. Ethical Issues and Challenges in the ICT Environment

Due to the numerous benefits and conveniences ICT offers, ICT products and services have become a constituent and indispensable part of our lives and the societies we live in. However, great technological potential and power usually give rise to important questions such as: What are the ethical implications of the unprecedented development and use of more and more sophisticated ICT? What impact does this have on European values and fundamental rights?

[1] Cf. Griesbacher/Staudegger/Stelzer 2017, p. 469.

Questions about ICT and its impact on individuals and society have generally been framed within various branches of ethics such as information ethics, computer ethics, cyberethics, ethics of technology and Internet ethics. Even though the distinction between all these types of «ethics» will not be elaborated in this contribution, at this point it can still be observed that they clearly point out the necessity to place issues and reflections related to ICT in an ethical context.

2.1. Privacy and ICT: Purpose and Collection Limitation

Today ICT products and services have found their application in many different contexts such as e-commerce, e-banking, e-health, e-governance, education etc. The common denominator of these various applications is that they all demand from the individual (acting as a user) to directly or indirectly «feed in» some personal data as a precondition for using them in the first place. With this in mind, at this point it is important to make a distinction between ethically sensitive and non-sensitive data and to clarify under what circumstances and for what kind of data ethical concerns may arise. Spiekermann, for example, argues that the collection of personal data is the main object of ethical concerns. However, she highlights that this is only the case when the context and purpose for data collection differ from the initial ones for which data was collected and needed.[2] Based on this, purpose and collection limitation, and here legitimacy should be added as well, are an essential aspect when discussing data. This would suggest that when personal data is collected by institutions, organisations or companies for legitimate purposes and when there are legitimate expectations from the individual to provide such data, this should not be considered ethically problematic. However, concerns arise when such data is shifted from one context to another, which may allow new classifications and categorisations that may prove to be harmful and discriminatory.[3] The reason this is worrisome lies in the fact that data as such can tell a lot about one individual and may (directly or indirectly) give away very personal and intimate aspects of her life which the individual never intended to reveal in the first place. For example, data may give information about location and movements of a person, her interests and habits, purchasing history, income, financial situation, health conditions, political preferences, religious beliefs, and many others aspects.

2.2. Autonomy and Informed Consent

Purpose and collection limitation closely relate to the idea of user's personal autonomy and the possibility for an informed consent. In the context of ICT products and services, autonomy can be analysed from the perspective of having control and choice over personal data that are disclosed as a result of using such products and services. Control is an important part of autonomy since it relates to the possibility of the user to have greater influence over data she consented to be collected. This influence usually takes the form of the user having access to her personal data, having the possibility to correct it, delete it or to oppose to any further data processing.

Autonomy is closely connected with the idea of informed consent since the latter directly ensures that the first is being respected. Informed consent in the context of ICT products and services means that the user has the possibility to make an informed decision about activities regarding her personal data. This includes being informed about what data is collected and in what ways, for what reasons, for how long it is stored, who has access to it,[4] as well as whether there is the possibility to voluntarily opt-in/opt-out from data activities and withdraw previously given consent.

Ethical issues and challenges may arise in several cases. First, cases where the silence or inaction of the user is interpreted as a sign of consent can be ethically problematic. Such implied consent has in itself inherent

[2] Spiekermann 2016, p. 49.

[3] Rössler 2005, p. 126.

[4] European Group on Ethics in Science and New Technologies 2012, pp. 46–47.

ambiguity.[5] It is not voluntary, informed and it lacks the explicit agreement of the user. Second, there are also cases where the user is offered no alternative at all to opt-in/opt-out from data collection activities, but merely informed about data collection activities. Another ethically problematic example includes cases where «consenting» seems to be the only option that the user has in order to participate in modern life.[6] In the context of ICT products and services, this would imply the existence of «either-or» circumstances where the user is faced with a dilemma whether to use a particular product or service at the cost of her privacy.

When talking about informed consent, there is one important aspect that ought to be brought up. To what extent can it be argued that the possibility for an informed consent truly empowers users to make decisions regarding their privacy if users have the tendency to accept almost anything while placing little or no effort to understand the implications this might have on their privacy?[7] This is an aspect that calls for a stronger consideration since it shows that in order for the user to be empowered she has to have the possibility to control and make choices over aspects that may affect her life, and she also has to be aware of the possibility to do so. Furthermore, it also suggests that informed consent is not a one-sided thing that ought to be provided and respected solely by providers of ICT products and services, but a shared responsibility. Informed consent also requires the awareness of and certain contributions from the user.

2.3. Security

Apart from privacy issues, security of data and security of systems and networks where data is circulated or stored present an additional challenge. Given the vast space the digital realm presents, the enormous number of users participating as well as the unprecedented quantities of data being exchanged, there are myriad of risks and threats that may occur such as data breaches, identity thefts, unauthorised access etc. These may affect the confidentiality, integrity and availability of data[8], but can also cause much graver consequences such as impeding the work of organisations, shutting down entire computer networks or even disrupting major parts of the Internet.[9] In that context, it is the job of providers of ICT product and services to provide and guarantee secure networks and systems to the users who are using their products and services. However, as was the case of informed consent, this also depends on the security awareness of the users and the efforts they make to protect themselves against any security threats.

2.4. Justice and its Principles

Justice principles including fairness, equality and impartiality, also find their place in the ethical discourse around ICT. For example, the increased automation of the decision-making process and the use of algorithms in the e-commerce sector may cause concerns over data-based discrimination and biased decision-making. This happens when collected data is analysed and used to create profiles which enables to differentiate among users and eventually make decisions based on that data.[10] Such practices are especially problematic when some of the decisions suggest to unjustifiably and unfairly exclude particular individuals from certain benefits or opportunities, be it in the form of a product or service offered. In that sense, issues related to justice can be analysed, for example, in terms of informational injustice, information-based harm, informational inequality, data-based discrimination.

Despite a wide-spread belief that algorithms allegedly operate with less or no bias, many experts disagree and argue that the development and design of algorithms is everything but value-neutral. Namely, the designer's

[5] Ibid.

[6] European Group on Ethics in Science and New Technologies 2014, p. 73.

[7] Cf. Zuiderveen Borgeswius 2015, pp. 103–107.

[8] These three components are also known to comprise the CIA triangle which is considered to be the industry standard regarding information security.

[9] Tavani 2011, pp. 177–178.

[10] Cf. Amicelle 2015, p. 275; Lyon 2003, p. 20.

values or the values of the author of an algorithm are always embedded into the algorithm itself.[11] This brings up the point that the design process of ICT is as important as the way ICT products and services are being used.

2.5. Transparency

All the issues previously mentioned are closely connected to the issue of transparency. In this context, transparency relates to two main aspects: (a) providing information about ICT products and services in terms of their quality and functionality, and (b) providing information about users' data that are exchanged within the purchase relationship or as a result of using a service. With that in mind, very often users do not seem to have the possibility to directly ensure the quality of the products and services they purchase/use or do not have specific information as to what happens to the data they enclose within the purchasing process or by using a service and how secure that data is.[12] Therefore, transparency demands greater openness, honesty, responsibility and communication with the users. Transparency helps uncover and provide answers to questions as to *what* is being done, *how* it is being done and *by whom* it is done.[13] In this way, the information asymmetry that exists between providers of ICT products and services and users could be narrowed down too. In addition, greater transparency would at the same time encourage ethical behaviour and a culture of trust.

Privacy policies are an important tool that can contribute to greater privacy compliance and transparency, and thus can shift the control more towards the user. Privacy policies have the aim to inform users about what data is collected, where and for how long it is stored, how it is used, among whom it is disseminated etc. However, there are also some criticisms and weaknesses identified around privacy policies and their effectiveness. The mere existence of a privacy policy does not directly imply that a business has fulfilled its duties concerning privacy towards users. The issue runs deeper and concerns the content of a privacy policy. In reality, privacy policies are generally regarded as too long, time-consuming, user-unfriendly and complex to be understood for which they prove to be ineffective and fail to serve their purpose.[14] In order to change this, privacy policies should be made easily accessible, comprehensive and understandable to the user and also be compliant with legal requirements. This would suggest that apart from information on activities with users' data, users should also be acquainted with the rights they have in relation to their data in terms of access, modification and deletion. A further relevant aspect is the security of the collected data. The user should also be informed about the level of protection of her data against unauthorised access, or in the case of e-commerce, the security of the payment process. To sum up, in order for a user to be able to make an informed decision regarding her personal data, she has to understand any activities regarding her data, she has to be informed about the options she has at hand and she also has to know her rights. It is based on the level of transparency that the possibility for an informed choice depends.

2.6. The Issue of Responsibility

This brings us to the last issue that will be elaborated in this contribution, namely, the issue of responsibility and accountability. In order to better pinpoint where ethical challenges exist, an example from everyday life will be presented. Let us assume that there is a user X who is interested in buying a certain product at company Y and as part of that purchase, the user X has to disclose some sensitive information. However, X has also noticed that the company Y does not seem to pay much attention to the protection and security of users' data. Moreover, Y seems to be pretty non-transparent in dealing with users' data. So, it appears it is in the hands of the user X to decide either to buy the product at the risk of the misuse of her data or to try and find another company, service or product which may appear to be more privacy-friendly. Such «take-it-or-leave-it»

[11] Mittelstadt et al. 2016, p. 7.

[12] Grabner-Kräuter/Kaluscha 2008, pp. 7–8.

[13] European Group on Ethics in Science and New Technologies 2014, p. 75.

[14] Balboni/Dragan 2017, pp. 9–10.

approach is problematic because it entirely shifts the burden towards the user. The burden, or in this context the responsibility regarding activities with users' data, lies predominantly on the side of the company. It is the company that needs to make sure that all the activities with the users' data in terms of collection, storage, processing, use and dissemination, are legitimate and carried out within the bounds of the legal framework.[15] It is an ethical and legal obligation of every company.

2.7. Ethical Attributes of Trustworthy ICT Products and Services

Having sketched out the main ethical issues and challenges that arise in the context of ICT products and services, we can now use these insights as guidelines to identify the main concepts that can contribute to building trustworthiness of ICT products and services and hence to building greater trust among users/consumers. These concepts can also be considered as attributes of trustworthiness since they show what is relevant from an ethical perspective when designing and using ICT. The list is not exhaustive since depending on the type of ICT products and services, the need for including additional ones may arise. The following attributes, however, may be considered as the basic ones: privacy, autonomy, informed consent, security, transparency, justice, responsibility and accountability.

3. Conclusion

ICT products and services are becoming more and more indispensable part of our lives, workplace and homes. In order to continue enjoying the numerous benefits they bring and at the same time to ensure the protection and respect of European values and fundamental rights, it is important to identify the main ethical concerns and challenges that may arise in the process of developing and using ICT. As the contribution has already showed, the main ethical issues revolve around concepts such as privacy, autonomy, informed consent, security, transparency, justice, responsibility and accountability. Including normative considerations and ethics as a discipline in the efforts to make ICT products and services more trustworthy is a necessary and inevitable step. These findings will pave the way for developing the ethical criteria that will be included in the TRUESSEC.eu Multidisciplinary Criteria Catalogue for Trustworthy ICT Products and Services.

4. References

Amicelle, Anthony, Surveillance, freedom of movement and discrimination. In: Wright, David/Kreissl, Reinhard (Eds.), Surveillance in Europe, Routledge, London and New York 2015, p. 271–277.

Balboni, Paolo/Dragan, Theodora, Big Data: Legal Compliance and Quality Management. In: Li, Kuan-Ching /Jiang, Hai/Zomaya, Albert Y. (Eds.), Big Data Management and Processing, CRC Press, Boca Raton 2017, pp. 1–16.

Griesbacher, Martin/Staudegger, Elisabeth/Stelzer, Harald, SSH in ICT Using the Example of TRUESSEC.EU. In: Schweighofer, Erich/ Kummer, Franz/ Hötzendorfer, Walter/Sorge, Christoph (Eds.), Trends and Communities of Legal Informatics. Proceedings of the 20th International Legal Informatics Symposium IRIS 2017, books@ocg.at, Vienna 2017, pp. 469–474.

European Group on Ethics in Science and New Technologies, Opinion No.26, Ethics of Information and Communication Technologies, Brussels 22 February 2012.

European Group on Ethics in Science and New Technologies, Opinion No.28, Ethics of Security and Surveillance Technologies, Brussels 20 May 2014.

Grabner-Kräuter, Sonja/Kaluscha, Ewald A., Consumer trust in electronic commerce: conceptualization and classification of trust building measures. In: Kautonen, Teemu/Karjaluoto, Heikki (Eds.), Trust and New Technologies: Marketing and Management on the Internet and Mobile Media, Edward Elgar Publishing, Cheltenham, Northampton 2008, pp. 3–22.

Lyon, David, Surveillance as social sorting: computer codes and mobile bodies. In: Lyon, David (Ed.), Surveillance as Social Sorting: Privacy, risk, and digital discrimination, Routledge, London and New York 2003, pp. 13–30.

[15] Cf. Martin 2016, pp. 51–56.

Martin, Kirsten, Data Aggregators, Consumer Data, and Responsibility Online: Who is Tracking Consumers Online and Should They Stop?, The Information Society Volume 32, No.1 (2016), pp. 51–63.

Mittelstadt, Brent Daniel/Allo, Patrick/Taddeo, Mariarosaria/Wachter, Sandra/Floridi, Luciano, The ethics of algorithms: Mapping the debate, Big Data & Society 3 2016, pp. 1–21.

Rössler, Beate, The Value of Privacy, Polity Press, Cambridge, Malden 2005.

Spiekermann, Sarah, Ethical IT Innovation: A Value-Based System Design Approach, CRC Press, Boca Raton, London, New York 2016.

Tavani, Herman, Ethics and Technology, Controversies, Questions, and Strategies for Ethical Computing – 3rd ed., John Wiley & Sons Inc., New Jersey 2011.

Zuiderveen Borgeswius, Frederik J., Informed Consent: We Can Do Better to Defend Privacy, Security & Privacy IEEE Vol. 13 Issue 2 2015, pp. 103–107.