Ethics and the Protection of Personal Data

Nicola FABIANO
Studio Legale Fabiano
Rome, 00179, (Italy)
Affiliation: *International Institute of Informatics and Systemics (IIIS)* - USA
email: *info@fabiano.law*

Abstract

The contribution provides some possible key points in the relationship among robotics, intelligent systems, Artificial Intelligence, Ethics, data protection and privacy. The starting point is the value of personal data belonging to a natural person. Ethics is one of the aspects that should be considered by everyone to have an excellent approach to the processing of personal data. The contribute of this paper presents some possible solutions to read the GDPR considering ethics and proposing other approaches to avoid misuses of personal information.

Keywords: Data Protection, Privacy, Ethics, Robotics, Artificial Intelligence

1. THE VALUE OF PERSONAL DATA: THE STARTING-POINT

The protection of personal data is a topic entirely relevant and very current.
In Europe both the right to respect for his or her private and family life, home and communications (privacy) and the right to the protection of personal data constitute fundamental rights, as provided for respectively by Articles 7[1] and 8[2] of the Charter of Fundamental Rights of the European Union (2016/C 202/02) [1]. Apart from the Charter of Fundamental Rights, also the Treaty on the Functioning of the European Union (TFEU - 2016/C 202/01) [2] lays down the right to the protection of personal data (Article 16, paragraph 1)[3].

The main question is: "Why the protection of personal data is a fundamental right?"

The answer is related to the intrinsic meaning of "personal data" because its qualification entails an evaluation of the term "personal" because it is strictly related to a natural person. We cannot dismiss the primary role of a natural person precisely for its ontology. Hence, any personal information means that it belongs to a natural person, realising such a strict relationship between them. Therefore, precisely due to the relationship that intrinsically binds information to each natural person generates a value.

What is the value we are referring to?

The meaning of the value can be both economic or financial and high ethical relevance. In fact, the protection of personal data means, generally speaking, to preserve a natural person from the misuse of his or her personal information.

Each person deserves respect.

Every opportunity to take advantage of something brings out its economic value. Unfortunately, personal data are not exempt because, in the last times, we see a trend towards their commodifying, every time someone, although not apparently, profits through personal information belonging to a natural person. In this way it realises is the warped economic value of personal data.

People often are not aware of the possible risks related to the full use of their personal data, especially when they are not informed about the purposes of processing.

Due to the change of the communication systems, people use several resources from the email to the most disparate messaging apps. Unfortunately, people very often do not care about the security risks because it is prevalent the final goal that is "communicating any-

[1] Article 7 - Respect for private and family life. Everyone has the right to respect for his or her private and family life, home and communications.

[2] Article 8 - Protection of personal data. 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.

[3] Article 16(1) says: "Everyone has the right to the protection of personal data concerning them".

way".

Human beings need to communicate (this is the first axiom of the School of Palo Alto) and the advantage offered by the Internet of being able to interact with other people even from a distance has been successful.

Paradoxically, the "new" mode of communication favours communication between individuals exponentially, and the speed of interaction has given rise to the custom (which has become the model) of the rapid (and convenient) consultation of the contents present on the web (without no discernment of the sources) also with the aim, unfortunately, of learning. The sources that can be consulted (not always correct) are basically on the web, and the contents are not very articulated because they must be easily readable and in a short time.

Accessing (comfortably and quickly) the sources on the web can distort the self-training process (or self-directed learning or self-learning - self-learning) because people must have a specific competence on how it is possible to self-learn and it is necessary to develop in advance competences to self-learn that cannot be taken for granted. The generalised self-learning process can lead to a lowering of the cultural level.

In essence, the need for ever-faster communication very often requires as much speed in acquiring notions and increasing the cultural profile that, on the other hand, may suffer a decrease both because of the multitude of sources present on the web which are accessed without selecting those that are certain and accredited regarding the necessary competence for self-learning.

Economic value can arise through wrong processing of personal data, due to the indiscriminate use of personal data without any information provided to the data subject by the controller about the purposes stated or for different ones not declared. In the same way, a data breach can entail economic value of personal data with consequent commercial exploitation.

Understanding the value of personal data helps to respect and pay attention to the person.

2. ETHICS AND THE EUROPEAN REGULATION ON DATA PROTECTION

The European legislation on data protection has changed modifying the approach to this topic.

The European Regulation 2016/679 (General Data Protection Regulation - GDPR) [3] "*on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*" has been published on 4 May 2016 in the Official Journal of the European Union and entered into force on 25 May 2016, but it applies from 25 May 2018. According to the Article 94, this Regulation repeals the Directive 95/46/EC [4] with effects from 25 May 2018.

The GDPR obviously mentions the Charter of Fundamental Rights of the European Union in the first Whereas[4].

The main rights of the 'data subject' laid down by the GDPR are:

(a) *right to request from the controller access to and rectification or erasure of personal data;*

(b) *right to withdraw consent at any time;*

(c) *right to lodge a complaint with a supervisory authority;*

(d) *right of access;*

(e) *right to rectification;*

(f) *right to erasure ('right to be forgotten');*

(g) *right to restriction of processing;*

(h) *right to data portability;*

It is clear how it is relevant the role of the 'data subject'[5] and hence the high value of the personal data.

Regarding the processing of personal data the GDPR lays down specific obligations for the controller[6] and the processor[7], mainly observing the principles according to the articles 5 and 6 and implementing "appropriate technical and organisational measures to ensure a level of security appropriate to the risk"[8].

The GDPR is a milestone because brings a new approach to the protection of natural persons with regard to the processing of personal data, introducing

[4] The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

[5] According to the Article 4(1) number (1) of the GDPR 'data subject' is 'an identified or identifiable natural person'.

[6] The Article 4(1) number (7) says: 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

[7] The Article 4(1) number (8) says: 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

[8] Article 32.

numerous changes, such as, inter alia, the accountability principle, the Data Protection Impact Assessment (DPIA), the Data Protection by Design and by Default principle, the data breach notification, the Data Protection Officer (DPO), the very high administrative fines in respect of infringements of the Regulation, and so on.

Apart from the law, there is also the "soft-law" that consists of opinions issued by Data Protection Supervisory Authorities and the European Data Protection Board (former Article 29 Working Party). The opinions are not binding but provides clarification contributing to interpret the data protection law.

3. ROBOTICS, ARTIFICIAL INTELLIGENCE, ETHICS AND DATA PROTECTION: THE EUROPEAN OVERVIEW

The legislation about the protection of natural persons with regard to the processing of personal data applies to all over the sectors, including robotics, artificial intelligence and others intelligent systems.

Public Bodies paid attention to these topics over the last few years [9].

In 2018 the European Group on Ethics in Science and New Technologies of the European Commission on 9 March 2018 issued the "*Statement on Artificial Intelligence, Robotics and Autonomous Systems*" [5] that addresses the following questions: about safety, security, the prevention of harm and the mitigation of risks; about human moral responsibility; about governance, regulation, design, development, inspection, monitoring, testing and certification; regarding democratic decision making, including decision making about institutions, policies and values that underpin all of the questions above; about the explainability and transparency of AI and autonomous systems. This document addresses also ethical aspects and states the following ethical principles and democratic prerequisites:

(a) *Human dignity;*

(b) *Autonomy;*

(c) *Responsibility;*

(d) *Justice, equity, and solidarity;*

(e) *Democracy;*

(f) *Rule of law and accountability;*

(g) *Security, safety, bodily and mental integrity;*

(h) *Data protection and privacy;*

(i) *Sustainability.*

On 25 April 2018 the European Commission issued the "*Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Artificial Intelligence for Europe - COM(2018) 237 final*" [6]. This Communication contains the Europe strategies for AI, and in the paragraph 3.3., titled "Ensuring an appropriate ethical and legal framework", we read the intent to "*draft AI ethics guidelines will be developed by the end of the year, with due regard to the Charter of Fundamental Rights of the European Union*".

Recently, the 40th International Conference of Data Protection and Privacy Commissioners, held in Brussels, 22-26 October 2018, issued a document titled "*Declaration on Ethics and Data Protection in Artificial Intelligence*" [7] where we read "*The 40th International Conference of Data Protection and Privacy Commissioners considers that any creation, development and use of artificial intelligence systems shall fully respect human rights, particularly the rights to the protection of personal data and to privacy, as well as human dignity, non-discrimination and fundamental values, and shall provide solutions to allow individuals to maintain control and understanding of artificial intelligence systems*".

The before-mentioned collection of documents shows as the attention are moving from purely technical aspects towards more high-level ones, focusing, hence, on concepts strictly related to human values: human dignity. The risk is that natural person becomes pure data, debasing and losing so the typical aspects belonging to a human. Ethics is the correct path to preserve the ontological nature of human.

What is ethics?

[9] In 2015 the European Data Protection Supervisor (EDPS) carried out the Opinion 4/2015 [11]. In 2016 the Robotics and Artificial Intelligence Session at the 38th International Conference of Data Protection and Privacy Commissioners carried off and published the document titled "*Informal reflections on policy questions*" [12] and also a "Room document" titled "*Artificial Intelligence, Robotics, Privacy and Data Protection*" [13]. In 2017 the Information Commissioner's Office (ICO) carried out a discussion paper titled "*Big data, artificial intelligence, machine learning and data protection*" [14]. The European Parliament adopted the "*Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))*" [?] by which, after proposing several statements, requests the European Commission to submit a proposal for a directive on civil law rules on robotics, following the recommendations set out in the Annex hereto.

There are no easy answers because we have several definitions. We want to refer to a thinking way helpful to distinguish, generally speaking, what is wrong from what is right, finding the right key to conferring a natural person the exact value belonging to him or her.

The GDPR doesn't lay down any specific rules on Ethics. Nevertheless, we think that it is possible to start applying the GDPR principles thinking ethical: it is a matter of approach even without any norm.

The EDPS, during the 40th International Conference [10] said [8]:
"*What then is the relationship of ethics and the law? From my perspective, ethics come before, during and after the law.*
It informs how laws are drafted, interpreted and revised.
It fills the gaps where the law appears to be silent.
Ethics is the basis for challenging laws".

4. A POSSIBLE STARTING PATHWAY TO BALANCE ETHICS AND DATA PROTECTION LAW

According to the scenario described in the previous paragraph, the primary goal is to have a balancing approach between ethics and data protection law.

We think that it is possible to evaluate a balancing pathway starting from some articles of the GDPR.

The Article 5 states the principles relating to the processing of personal data [11] that are: 'lawfulness, fairness and transparency', 'purpose limitation', 'data minimisation', 'accuracy', 'storage limitation', 'integrity and confidentiality' and 'accountability'.

The mentioned article should be balanced with an ethical approach protecting personal data guaranteeing the dignity of each natural person. The ethical approach should be not only theoretical but practical and adopted mainly by the private sector.

The principles provided for in Article 5 of the GDPR should be used as the primary references for Ethics, but we cannot dismiss the other rules of the same Regulation. Data protection and privacy are, indeed, "processes" and their assessment to comply with the law is the right way to address them. Furthermore, applying an ethical approach, the others principles ('lawfulness, fairness and transparency', 'purpose limitation', 'data minimisation', 'accuracy', 'storage limitation', 'integrity and confidentiality' and 'accountability'), could be considered a pathway to ethics even if the GDPR does not contain any specific reference to it. Interpreting and applying the GDPR norms it is possible to consider a valid ethical approach though the mentioned principles.

In practice, each controller should evaluate the processing of personal data based on the mentioned principles and considering them also from an ethical perspective.

Apart from the laws, in the processing of personal data, each controller should consider ethics anyway also even does not exist any obligation provided by the law. The following two cases could be useful to explain our opinion:

Case 1: The head office of a bank asks engineers to develop software to share clients' personal information with a financial company of the same group. The bank correctly informs the 'data subjects' about the recipients or categories of recipients of the personal data. Engineers develop an intelligent system to automate some processes. The developed algorithm works but, unfortunately, someone in the head office of the

[10] 40th International Conference of Data Protection and Privacy Commissioners - Brussels, 2018 - www.privacyconference2018.org

[11] Article 5 - Principles relating to processing of personal data
1. Personal data shall be:

(a) *processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');*

(b) *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');*

(c) *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*

(d) *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');*

(e) *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');*

(f) *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

bank misuses personal information for purposes not declared to the 'data subjects'. Beyond possible illegal aspects, the mentioned case shows no attention to ethics, probably because there is not any consciousness about it. A consciousness of ethics entails the comply with the law (data protection law - GDPR), but it could not true the contrary (respecting the law does not mean to have always consciousness of ethics).

Case 2: A technical staff develops a robot to manage industries processes consisting of four steps. After years of testing the robot is implemented in the industrial production. Unfortunately, from step two to third, there is an issue related to a possible personal data breach, but the developers consider the production priority firstly instead of managing the risk correctly and adopting the adequate implementation. The developers, evaluating the risk as very low and irrelevant, decide that the implementation entails a high effort not balanced by the possible data breach. Also, in this case, there could be illegal aspects, but an ethics approach certainly would have avoided the final decision. Even if the risk is qualified as low, it does not mean to be authorised to bypass it.

It would be desirable to consider a business ethics approach to process personal data correctly, according to the GDPR (or, in general, the laws). In certain cases, where it is not possible to refer to the data protection law the ethical aspects might be addressed by policies or agreements. We know that the GDPR concerns the protection of personal data in Europe and one issue is related to the processing outside Europe.

On the technical side, one of the relevant points is the development of applications for robots or intelligent systems. An excellent approach should be to develop the applications guaranteeing a high-security level to avoid any alteration od disclosure of personal data. Developing an algorithm for an intelligent system should avoid the misuse of personal data considering also ethics. As technology improves, the attacks on the systems grow as well. However, we cannot dismiss the several threats on these systems.

The GDPR jurisdiction could be a limit for any business especially outside Europe; in this case, it is possible to compensate for this lack of laws through policies or agreements.

Furthermore, beyond the legal norms, it exists for several sectors a technical regulatory framework, governed in Italy by the Italian Unification Body (UNI)[12], in Europe by the European Committee for Standardization (CEN) and worldwide by International Organization for Standardization (ISO).

Regarding data protection, in Italy UNI has issued the 'Guideline for personal data management within ICT according to Regulation (EU) 679/2016 (GDPR) - Management and monitoring of personal data within ICT' - UNI PdR 43:2018. The guideline consists of two sections. Section one (UNI/PdR 43.1:2018)[13] provides the guidelines for the definition and implementation of processes related to the processing of ICT personal data according to the European regulation 679/2016 (GDPR) and the relevant normative requirements. Section two (UNI/PdR 43.2:2018) [14] provides an adequate summary of the requirements enabling an organisation, in particular small and medium enterprises, to conform effectively with the European and national normative framework, demonstrating the conformity and effectiveness also by means of certification. Section 2 also provides indications for the conformity assessment to the requirements defined by this UNI/PdR.

provides an adequate summary of the requirements enabling an organisation, in particular small and medium enterprises, to conform effectively with the European and national normative framework, demonstrating the conformity and effectiveness also by means of certification. The present document also provides indications for the conformity assessment to the requirements defined by this UNI/PdR

, composed of two parts, that represent an interesting and appreciable initiative.

carried out by the Italian Association for technical standards (UNI), composed of two parts, that represent an interesting and appreciable initiative.

[15]

It is clear that standards or technical norms can be helpful to achieve and manage an ethical approach,

[12] UNI is the Italian National Body for technical standards, an association, recognised by the State and the European Union - http://uni.com/

[13] http://store.uni.com/catalogo/index.php/uni-pdr-43-1-2018.html)

[14] http://store.uni.com/catalogo/index.php/uni-pdr-43-2-2018.html

[15] Guideline for personal data management within ICT according to Regulation (EU) 679/2016 (GDPR) - Management and monitoring of personal data within ICT - The UNI/PdR 43 consists of two sections. Section 1 (UNI/PdR 43.1:2018) provides the guidelines for the definition and implementation of processes related to the processing of ICT personal data according to the European regulation 679/2016 (GDPR) and the relevant normative requirements (http://store.uni.com/catalogo/index.php/uni-pdr-43-1-2018.html).Section 2 (UNI/PdR 43.2:2018) provides an adequate summary of the requirements enabling an organisation, in particular small and medium enterprises, to conform effectively with the European and national normative framework, demonstrating the conformity and effectiveness also by means of certification. The present document also provides indications for the conformity assessment to the requirements defined by this UNI/PdR (http://store.uni.com/catalogo/index.php/uni-pdr-43-2-2018.html).

without excluding the GDPR or others data protection laws.

5. CONCLUSIONS

Ethics is a new challenge.

People should pay attention even more and more to high values such as human dignity, especially in the sector of personal data and privacy.

How is it possible to achieve an excellent ethical approach?

Firstly, every single subject involved in the processing of personal data must have a significant awareness of the high value belonging to a natural person such as human dignity. Knowing only the legal framework often does not is synonymous of professionalism, because there is the needing to had to acquire other skills like pragmatism and especially knowledge of more high-value aspects. Laws are necessary to regulate the life of people but the operators have to apply them considering essential principles often not written like ethics. Often it is not possible to balance laws and ethics and it is necessary only to apply the law. In any case, the operator should consider ethics, until it is possible, during the approach to data protection and privacy. It is essential to acquire the consciousness of ethics because it certainly can drive any activity correctly.

Secondly, the GDPR lay down the principle "Data Protection by design and by default" (article 25) that entails the needing to consider primarily the protection of personal data during the design phase and to implement technical and organisational measures to ensure 'by default' the processing of personal information necessary for each specific purpose. It is relevant to organise continuous training courses to growth the personal knowledge on the protection of personal data for anyone involved in a work activity.

Last but not least, do not forget that ethics is a relevant part of the entire knowledge that people who deal with data protection should acquire anyway. Each natural person - as 'data subject' - should know him or her rights laid down by the data protection law.

REFERENCES

[1] Charter of Fundamental Rights of the European Union, 2016 https://www.ecb.europa.eu/ecb/legal/pdf/oj_c_2016_202_full_en_txt.pdf [retrieved: July, 2019]

[2] The Treaty on the functioning of the European Union (2016/C 202/01), 2016. https://www.ecb.europa.eu/ecb/legal/pdf/oj_c_2016_202_full_en_txt.pdf [retrieved: July, 2019]

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN [retrieved: July, 2019]

[4] 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. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN [retrieved: July, 2019]

[5] European Group on Ethics in Science and New Technologies, Statement on Artificial Intelligence, Robotics and Autonomous Systems, 2018 https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf#view=fit&pagemode=none [retrieved: July, 2019]

[6] European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Artificial Intelligence for Europe - COM(2018) 237 final, 2018 https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe [retrieved: July, 2019]

[7] 40th International Conference of Data Protection and Privacy Commissioners, Declaration on Ethics and Data Protection in Artificial Intelligence, 2018 https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf [retrieved: July, 2019]

[8] G. Buttarelli - European Data Protection Supervisor, Choose Humanity: Putting Dignity back into Digital, 2018 https://www.privacyconference2018.org/system/files/2018-10/Choose%20Humanity%20speech_0.pdf [retrieved: July, 2019]

[9] European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices, 2019. https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-32019-processing-personal-data-through-video_en [retrieved: July, 2019]

[10] N. Fabiano, "Privacy and Security in the Internet of Things", in Cutter IT Journal, Vol. 26, No. 8, August 2013

[11] European Data Protection Supervisor (EDPS), Opinion 4/2015 - Towards a new digital ethics. Data dignity and technology, 2015 https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf [retrieved: July, 2019]

[12] 38th International Conference of Data Protection and Privacy Commissioners, Informal reflections on policy questions, 2016 https://icdppc.org/wp-content/uploads/2015/03/Robotics-and-artificial-intelligence-session-Informal-reflections-on-policy-questions.pdf [retrieved: July, 2019]

[13] European Data Protection Supervisor - EDPS, Artificial Intelligence, Robotics, Privacy and Data Protection, 2016, https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf [retrieved: July, 2019]

[14] Information Commissioner's Office, Big data, artificial intelligence, machine learning and data protection, 2017 https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf [retrieved: July, 2019]

[15] European Parliament, European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)),2017 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0051+0+DOC+PDF+V0//EN [retrieved: July, 2019]

[16] T. Karras et alt., A Style-Based Generator Architecture for Generative Adversarial Networks, 2018-2019 https://arxiv.org/pdf/1812.04948.pdf [retrieved: July, 2019]

[17] N. Fabiano, Internet of Things, Blockchain and Intelligent Systems: The Primary Role of Data Protection, APPIS Conference 2018, book chapter, DOI: 10.3233/978-1-61499-929-4-266 http://ebooks.iospress.nl/volumearticle/50886 [retrieved: July, 2019]

[18] N. Fabiano, The Internet of Things ecosystem: the blockchain and data protection issues, ASTES Journal, Volume 3, Issue 2, Page No 01-07, 2018, DOI: 10.25046/aj030201 https://astesj.com/v03/i02/p01/ [retrieved: July, 2019]

[19] N. Fabiano, Blockchain and data protection: The value of personal data, IMCIC 2018 - 9th International Multi-Conference on Complexity, Informatics and Cybernetics, Proceedings, 2018, vol. 2, pages 112-115 https://www.scopus.com/record/display.uri?eid=2-s2.0-85050251219&origin=inward&txGid=cfe1f0ad79ff4bd05fd884e4b3100b92 [retrieved: July, 2019]

[20] N. Fabiano, Internet of things and blockchain: legal issues and privacy. The challenge for a privacy standard, Proceedings, 2017, IEEE International Conference on Internet of Things, DOI: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.112

[21] J. Pandya, Is The Future Of Artificial Intelligence Tied To The Future Of Blockchain? https://www.forbes.com/sites/cognitiveworld/2019/03/29/is-the-future-of-artificial-intelligence-tied-to-the-future-of-blockchain/