The Meaning of 'Accountability', 'Responsibility,' and 'Liability' in the GDPR: Proposal for an Ontology

Nicola Fabiano

Studio Legale Fabiano
Roma, Italy
Email: info@fabiano.law

***Abstract*—The contribution starts from the European Regulation 2016/679 to analyse the terms 'accountability', 'responsibility' and 'liability' and their meaning. Accountability is the key to verify that there is an ethical implication in the GDPR through the evaluation of the related human actions. Every action can qualify the behaviour as 'accountability' and hence confer an ethical connotation. We consider the differences among the meaning of the mentioned terms as a starting point to define an ontology of the GDPR.**

Keywords–Data Protection; Ethics; Accountability; Responsibility; Liability.

I. INTRODUCTION

The present contribution aims to investigate on some terms laid down by the European Regulation 2016/679 (General Data Protection Regulation - GDPR) [1], highlighting how their meaning is not the same in all the official languages of the European Union. We think that the deepening on the sense of the terms 'accountability', 'responsibility' and 'liability' is a relevant focus both to clarify what each term should explain in the data protection context and a good starting point for working on an ontology of the GDPR. We demonstrate that the meaning of the terms above is not the same in all the official languages (especially in Italian), where the true sense belongs to the English languages. Once demonstrating the correct meaning, it is possible to address the ontology that is a complex process anyway. Here, we do not explain the ontology, but we would introduce this topic for the following works.

II. THE EUROPEAN REGULATION N. 2016/679

The European Regulation 2016/679 (General Data Protection Regulation - GDPR) "*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 [18] with effects from 25 May 2018. The GDPR mentions the Charter of Fundamental Rights of the European Union [2] in the first Whereas (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).

One of the primary goals of the European regulator was to harmonise the legislation of each Member State: the GDPR is directly applicable in each European State, to avoid possible confusion among each domestic law. The aim of the European regulator, conscious of the high value of the personal information, was to protect the natural person with regard to the processing of personal data; the GDPR recognises several rights to the 'data subject' (Article 4.1 says: "an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person").

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 (âĂŸright to be forgottenâĂŹ);*
(g) *right to restriction of processing;*
(h) *right to data portability;*

The listed rights show how relevant is the role of the 'data subject' and hence the high value of the personal data.

Regarding the processing of personal data the GDPR lays down specific obligations for the controller (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), and the processor (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), 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" (Article 32).

The GDPR is a milestone because it brings a new approach to the protection of natural persons with regard to the pro-

 ISBN: 978-1-61208-721-4

cessing of personal data, introducing 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.

It is clear that technology and law are not at the same level because the first one (technology) is always ahead than the second one (law). The actions on the part of the legislator always followed the technological solutions, and so the rules have to be able to consider the technology evolution.

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.

III. The terms 'Accountability', 'Responsibility' and 'Liability' in the official languages of the European Union

According to the Treaty on the functioning of the European Union [3] and the Treaty on European Union, the official European languages are those mentioned in the Treaties and hence all those of the States member of the Union. Unfortunately, due to the language localisation, in some versions of the GDPR, we cannot see the same terms mentioned above.

In the English version of the GDPR we find three terms:

1) 'Accountability' (Article 5);
2) 'Responsibility';
3) 'Liability'.

In the Italian version of the GDPR, for example, we see only the term 'responsibility'. In fact, the before mentioned words are typical only of the common law systems, and each one of them has different meanings from the other. In civil law systems, the only used word is 'responsibility', and hence it is quite difficult to translate in other languages, different from English, the words 'accountability', 'responsibility' and 'liability' each one with its specific meaning. Hence, the meaning of the terms above might depend on the context, the legislation, the jurisdiction and also from the geographic area.

On the one hand, applying the GDPR in Europe, and especially in civil law systems, it is hard due to the identification of the correct word to adapt in a specific case of responsibility. On the other hand, the GDPR applies in Europe but also all over the world according to the territorial scope laid down by Article 3, under the conditions set out in paragraph 2. Therefore, to understand the meaning of the three terms 'accountability', 'responsibility' and 'liability' it is necessary to consider, also in the national context, only the English version of the EU Regulation 2016/679.

This approach could be the first step for the best qualification of an ontology of the GDPR.

What does the term '**accountability**' mean? The GDPR uses the term 'accountability' referring to the controller and especially to the principle laid down by the Article 5, paragraph 2, where we read *The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (âĂŸaccountabilityâĂŹ)*. The topic is complex. The first reference we used to understand the correct meaning of the term 'accountability' in Europe is the Interactive Terminology for Europe (IATE) that is the EU's terminology database [4]. The IATE contains several definitions for specific domains or area, and we chose the meanings closer to the data protection field. Checking the word 'accountability' into the IATE database, we found some results, among which the European Data Protection Supervisor (EDPS) vocabulary, with the following definitions that seem more relevant, even if they are taken from different fields:

Data protection: *principle intended to ensure that controllers are more generally in control and in the position to ensure and demonstrate compliance with data protection principles in practice. Accountability requires that controllers put in place internal mechanisms and control systems that ensure compliance and provide evidence âĂŞ such as audit reports âĂŞ to demonstrate compliance to external stakeholders, including supervisory authorities*.

Public sector: *the obligations of persons or entities, including public enterprises and corporations, entrusted with public resources to be answerable for the fiscal, managerial and program responsibilities that have been conferred on them, and to report to those that have conferred these responsibilities on them* [7]. The above definitions show that, depending on the area, the meaning of the term 'accountability' might be different. Nevertheless, apart from the sector or area, the definitions have something in common. In fact, among the most important dictionaries, we found the same definitions or the same concept of 'accountability' always derived by the root 'accountable' (The term 'accountability' is defined: a) the quality or state of being accountable, especially: an obligation or willingness to accept responsibility or to account for one's actions: Merriam-Webster Dictionary online [6], or b) the the fact or condition of being accountable: English Oxford Living Dictionary [7], or c) the fact of being responsible for what you do and able to give a satisfactory reason for it, or the degree to which this happens: Cambridge Dictionary online [8]. Analysing the term accountable we see that the word 'accountability' is strictly related to an action by a person (these are the definitions of the term accountable: a) subject to giving an account (subject to giving an account) [9], or b) required or expected to justify actions or decisions; responsible (ministers are accountable to Parliament) [10], or c) someone who is accountable is completely responsible for what they do and must be able to give a satisfactory reason for it (In settings where responsibility for policy making is most clear, incumbent politicians are held accountable for macroeconomic performances) [11], or d) responsible to someone or for some action; answerable (The council that represents them is funded by the public to serve the public - and must be accountable to the public) [12]. In common law systems, the term "accountability" is closely related to the "responsibility", and the distinction is a thin line of demarcation. The characteristic of "responsibility" is autonomy, that is, a person - in his function - can act without external pressures or interference and therefore be free to make motivated decisions associated with his / her role while being bound to duties or obligations. A person "responsible" can make choices according to his intentions and is not under the control of others, and he or she is free to decide also about moral or social choices. The connection between role or function and the effects of the subject's actions or omissions characterise precisely the "responsibility").

 ISBN: 978-1-61208-721-4

We believe that it is possible to attribute to the term "responsibility" an ethical connotation on the basis of the the decisions that a "responsible actor" can freely assume. Someone [13] describes the "responsible actor" as «[...] one whose job involves a predetermined set of obligations that must be met in order for the job to be accomplished. [...] In many cases, simply discharging this primary obligation (the function associated with the role) may be sufficient unto itself; however, responsibility can also include moral obligations that are in addition and usually related to the functional obligations of the role. Thus, responsibility assumes that the actor becomes also a moral agent possessed of a certain level of moral maturity and an ability to reason».

An "accountable" subject, hence, is obliged to respect external conditions for which he does not have a power of self-determination and lacks the autonomy of the "responsible" subject but he or she is accountable for the consequences of his work anyway. Thus, an "accountable" subject is obliged to maintain a behaviour bound by sources external to himself, which are beyond his control and the power of self-determination. An "accountable" subject is also "responsible". The data controller, therefore, is "accountable" and hence conditioned by factors external to himself (the regulation to be respected), although he is capable of self-determination and has autonomy of action. Similarly, the controller is also "responsible" as he is free to evaluate the actions to be taken to comply with the GDPR rules.

Coming back on accountability, according to Thomas Bivins [13] "*The simplest formula is that a person can be held accountable if (1) the person is functionally and/or morally responsible for an action, (2) some harm occurred due to that action, and (3) the responsible person had no legitimate excuse for the action. Ideally, the assumption would then be to hold a person who is responsible for an action also accountable for the results of that action*". Bivins [13] continues with the following statement: "*In other words, accountability is a response to the human acts that one has performed. If it is a good act, the person deserves praise and if it is a bad act a person deserves blame. The idea of responsibility and accountability are closely linked, however are they slightly different by definition or moral implication*". According to T. Bivins [13] "*accountability might be defined as "blaming or crediting someone for an action" âĂŤ normally an action associated with a recognized responsibility*". **The term 'accountability', hence, is related to the effects of an action for which a person is not able to excuse**. The characteristic of accountability is the autonomy, and namely, a person can act without pressures or interferences hence being free to make decisions associated with his or her role. Furthermore, 'accountability' is linked to a behaviour typified by a moral or social connotation. Considering the moral and social connotation of accountability, we think that it is possible to evaluate implications in the ethical field.

Paragraph 2 of the article 5, in the English version, uses different terms as compared to the Italian translation, where we read: "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ("accountability ")". We read, instead, in the English version of the GDPR two ontologically and legally different terms: on the one hand, the controller shall be: "**responsible** for ... (paragraph 1)" and on the other hand "able to demonstrate compliance with ... (paragraph 1)", qualifying this behaviour as "**accountability**".

In light of what has been said, the data controller, is "responsible" (for the power of self-determination to demonstrate compliance with the regulation) and free to act and take decisions of moral importance, that is to say, respect or not the norms. The controller is also "accountable" and bound by the principle expressed in paragraph 2 of article 5 and responds, under article 83 for the violation of this principle.

"Accountability" has been translated into Italian with "responsibility", and the term "responsible" in the first part of paragraph 2 of article 5, is translated as "competent". The Italian jurist could remain disoriented and confused, having to qualify juridically "competence" and "responsibility".

In the Italian juridical system, indeed, there is only a concept: "responsibility". The important aspect is related to the identification of the juridical nature of the behaviour, related to the role of a subject (the data controller), against the law (mainly action or omission - The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')). The data controller could act (poorly, and therefore not respect the principles set out in paragraph 1) or not act (omit to comply).

The burden of being "able to demonstrate compliance with" (respect for principles) finds other references in the GDPR and specifically in article 24, Paragraph 3 where we read "*Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller*". The legislator, in the English version, used the term "responsibility" precisely to indicate the status of the 'responsible actor' who is free to decide whether to use the certification mechanisms to be able to demonstrate compliance with the obligations laid down by the GDPR. According to the common law systems approach, here we are not faced with a hypothesis of "accountability" for the reasons explained above on the qualification of the two different roles "responsible actor" and "accountable actor".

Moreover, there are differences between the English version and the Italian one of Article 82 of the GDPR titled "Right to compensation and liability". The European legislator used in the English version the term "liability" to highlight a situation where, in case of damages, there are different consequences instead of the administrative fees. Liability, instead, is a legal obligation. In the Italian juridical system, instead, we qualify the "liability" always as responsibility.

According to the article 83 paragraph 5, infringements of the principles laid down by Article 5 "shall be subject to to administrative fines up to 20 000 000 EUR or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher". Therefore, the sanction explains how the GDPR, considers 'accountability' as a high-value principle, layding down 'responsibility' and 'liability' for its infringement. Responsibility, thus, is related to a person and it refers to the outcomes of actions and it is strictly related to accountability.

In light of this, it is clear the choice of the term 'accountability' adopted by the European legislator in the GDPR because, despite being typical of the common law systems, has the aim to highlight and stress exactly the actions (or

 ISBN: 978-1-61208-721-4

omissions) of the controller in respecting of the EU Regulation 2016/679.

IV. Ethics and Data Protection

The European Data Protection Supervisor (EDPS), during the 40th International Conference [14] said [15]:
"*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".

The mentioned statement was perfectly aligned with the theme of the conference (Debating Ethics: dignity and respect in data driven life). Ethics is the new challenge in the field of the protection of personal data, where the primary goal is to guarantee the data subject's rights paying attention, particularly to human dignity.

The attention of the Data Protection and Privacy Commissioners, the stakeholders and the civil society, is 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 a natural person becomes pure data, debasing and losing so the exemplary aspects belonging to a human. Ethics is the correct path to preserve the ontological nature of human.

In light of this, the question is: What is ethics? There are no easy answers because we have several definitions. We want to refer to a way of thinking that can help us 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. Accountability is an element related to ethics on the basis of the behaviour of a person and his or her choice to take action or not.

We must investigate ethical specific aspects to allow us having an efficient approach discovering the correct pathway towards a balance between Data Protection and Ethics. Robert Goodin [16] talks about the 'Vulnerability Principle' which he thus defined: "Moral agents acquire special responsibilities to protect the interests of others to the extent that those others are specially vulnerable or in some way dependent on their choices and actions". The Goodin's definition of 'vulnerability principle' mentions terms (moral agents, responsibilities, vulnerable, choices and actions) that are very close to the accountability definition as explained in the previous paragraph. Hence, in ethical behaviour, people should pay attention to avoiding to make choices and action that could be a vulnerability cause for others. In the data protection field, it is mandatory to avoid any detriment to the data subject.

The GDPR does not 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.

V. Ethics and practical applications in the data protection domain

The main question is "How is it possible in practice to respect Ethics in the Data Protection?" Also, in this case, the answer is not simple, but we can indeed refer to the 'Data protection by design and by default' principle laid down in article 25 of the GDPR. In fact, according to the article 25, paragraph 1, of the GDPR "the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures".

Accountability is the main reference in this case because any infringement of the mentioned principle entails administrative fee "up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher". The controller have to respect the GDPR accountably. In a case, for example, where developers work on a project to carry out an algorithm, they respect the 'data protection by design' principle paying attention during the design phase to norms and rules on the protection of personal data.

Nowadays, we assist in an increase in the technical resources that use Artificial Intelligence (AI). Ethics is much important especially where - through the AI - software works getting data, often not either provided directly by the data subject, processing so massive amount of personal information. Ethics entails the respect of the principles 'Data protection by design and by default' and hence, also here, the controller has to be accountable.

Each natural person, giving his or her personal data, trust the 'controller' who must adopt the appropriate technical and organisational measures and respect the data protection laws. The misuse of personal data, due to the inappropriate use of personal information belonging to a natural person, is a data breach. Any misuse is a breach of trust, and it entails an ethical violation and, above all, the infringement of the data protection laws. The AI Now Report 2018 [17] from AI Now Institute, New York University shows ten points on the Artificial Intelligence and in point 5 and point 10 we find reference to Ethics (AI Now Report 2018, New York, 2018 - Point 5. "Technology companies should provide protections for conscientious objectors, employee organizing, and ethical whistleblowers. 10. University AI programs should expand beyond computer science and engineering disciplines").

VI. Conclusion

In conclusion, we demonstrated how the meaning of the terms 'accountability', 'responsibility' and 'liability' are related to a common law system and their translation in other languages does not find useful to explain the appropriate sense. Thus, our research describes how and why in the GDPR, we read three different terms related to responsibility, and this is the reason to refer to the English version to better understand the sense. We also highlighted the ethical characters that connotate 'accountability' in choices taken by a natural person. Dealing with data protection and privacy should always suggest to people considering the ethical approach in every single case, analysing human behaviour - actions (or omission) - as a part of the 'accountability'. Furthermore, this research, at the same time, shows how we can consider the terms mentioned above as a part of the ontology of the GDPR. We are carrying out a full analysis of the terms laid down by the EU Regulation 2016/679 hoping to publish soon specific research on the GDPR ontology.

 ISBN: 978-1-61208-721-4

REFERENCES

[1] 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: June, 2019]

[2] 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: June, 2019]

[3] 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: June, 2019]

[4] European Union Terminology. IATE (Interactive Terminology for Europe) is the EU's terminology database. https://iate.europa.eu/home [retrieved: June, 2019]

[5] From: the Oxford Handbook of Public Management, Edited by E. Ferlie, L. E. Lynn Jr., and C. Pollitt, Oxford Handbooks Online

[6] Merriam-Webster Dictionary online https://www.merriam-webster.com/dictionary/accountability [retrieved: June, 2019];

[7] English Oxford Living Dictionary https://en.oxforddictionaries.com/definition/accountability [retrieved: June, 2019];

[8] Cambridge Dictionary online https://dictionary.cambridge.org/dictionary/english/accountability [retrieved: June, 2019].

[9] Merriam-Webster Dictionary online https://www.merriam-webster.com/dictionary/accountable [retrieved: June, 2019]

[10] English Oxford Living Dictionary https://en.oxforddictionaries.com/definition/accountable [retrieved: June, 2019]

[11] Cambridge Dictionary online https://dictionary.cambridge.org/dictionary/english/accountable [retrieved: June, 2019]

[12] Collins English Dictionary online *https://www.collinsdictionary.com/dictionary/english/accountable* [retrieved: June, 2019]

[13] T. H. Bivins, Responsibility and Accountability, in Ethics in Public Relations: Responsible Advocacy, chapter 2, Edited by: K. Fitzpatrick - C. Bronstein, SAGE Publications Inc., 2006 http://homepages.se.edu/cvonbergen/files/2012/12/Resonsibility-and-Accountability1.pdf [retrieved: June, 2019]

[14] 40th International Conference of Data Protection and Privacy Commissioners - Brussels, 2018 www.privacyconference2018.org [retrieved: June, 2019]

[15] 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: June, 2019]

[16] R. Goodin, Protecting the Vulnerable: A Reanalysis of Our Social Responsibilities, Chicago, University of Chicago Press, 1985

[17] AI Now Report 2018, New York, 2018 https://ainowinstitute.org/AI_Now_2018_Report.pdf [retrieved: June, 2019]

[18] 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: June, 2019]

[19] 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: June, 2019]

[20] 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: June, 2019]

[21] 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: June, 2019]

[22] 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: June, 2019]

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

[24] 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: June, 2019]

[25] 32nd International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy by Design. 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem, 2010. https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf [retrieved: June, 2019]

 ISBN: 978-1-61208-721-4