A Regulatory Mariage de Figaro*: Risk Regulation, Data Protection, and Data Ethics*

Alessandro SPINA*

I. Introduction

"*Vien poi l'occasione/che vuolmi il padrone/don, don; in tre salti/lo vado a servir*"[1] sings the innocent Figaro in the first act of Mozart's *Mariage de Figaro*. He is talking to his betrothed, Susanna, with naïve happiness about the future advantages of sleeping in a bedroom close to that of his master, the Count Almaviva. The Count is in love and insidiously pursues Figaro's bride-to-be; the conventional plot of a love triangle. The concepts of risk regulation, data protection, and data ethics seem to be entangled in a similar complicated relationship, with persuasive affinities and ambiguous misunderstandings. This dangerous liaison stems from the fact that the digital economy is fuelled by personal data, quite literally. Its main, and quintessentially defining, commercial applications – such as the Google search engine or a Facebook newsfeed – rely on the collection, use, analysis, and transfer of information concerning individual users. Search engines, apps and digital platforms offer services to users almost at no cost, the commercial transaction being enabled by the exchange of data. Collection and use of the data are agreed upon by consumers by accepting voluntarily "terms of use". We know that the tripartite methodology of risk regulation, i.e. risk assessment, risk management and risk communication, is technology-neutral, and yet its emergence and prominence has come about in the second half of last century. This is why risk regulation has been traditionally associated with the uncertain negative outcomes connected with the products of industrialized manufacturing, such as food, pharmaceuticals, chemicals, or with sources of energy, safety of transport, or general environmental issues. It is now becoming obvious, with the skyrocketing amount of digital data being created and used, that there is a relationship between risks and data. One could, therefore, legitimately wonder what is the role for risk regulation in the emerging economic and social landscape of digital platforms, algorithms and artificial intelligence (AI)? Can risk regulation contribute to the governance of the data-driven digital economy? And if so, what is the role that data ethics will play in the relationship between risk regulation and data protection?

* Data Protection Officer at the European Medicines Agency (EMA) and Visiting Lecturer in Global Risk Regulation at the University of Fribourg. The views expressed in this article are the personal opinions of the author. The author is indebted to Professor Luciano Floridi for the stimulating discussions about data ethics and for the comments received in the course of drafting this paper; email: alessandro.spina@ema.europa.eu.

[1] Wolfgang Amadeus Mozart, *Le Mariage de Figaro*, Libretto by L. Da Ponte, opera buffa in four acts first represented at the Burgtheater, Vienna in 1786. The original text in Italian can be translated into English as follows: "*And then when the time comes/that my master wants me/ dong dong: in three bounds/I am ready to serve him*".

European Journal of Risk Regulation, 8 (2017), pp. 88–94
doi:10.1017/err.2016.15

This brief contribution does not provide a definitive answer to these questions. It rather attempts to lay down some of the theoretical and practical conditions that make not only possible but desirable the development of research to explore the relationships between risk regulation and data governance. The first condition, in our view, is the centre of interest that the new EU data protection legislation, Regulation (EU) No 679/2016 (also known by the acronym, GDPR) assigns to risks. Compared to the current EU legislation on data protection, the GDPR strengthens the rights of individuals vis-à-vis public and private entities ("data controllers"). But one of the most important transformations brought about by the GDPR is the different regulatory model envisaged to ensure that data controllers comply with data protection law, through the principle of accountability. In this new regulatory framework, data controllers are requested to control, in a formal and structured way, the risks to the rights and freedoms of data subjects arising from data processing operations. We are therefore witnessing a progressive "*riskification*" of EU data protection law, which will likely move out from the limited boundaries of formal legality of processing of data and enforcement of individual rights against companies. The shift towards a model of "enforced self-regulation" for managing technological innovation in uncertain scenarios seems to be at play.

Secondly, in a mutually reinforcing relationship, it seems that both the industrial products – the risks of which have been controlled by traditional regulatory frameworks – and the urban settings where risky activities take place, are becoming "smart". Sensors, data-generating micro-devices, connected wearables and more generally the Internet of Things transform our experience of the world and present another layer of risks to consumers that need to be factored in. Driverless cars, for example, create not only risks to the safety of passengers and third parties, but also to their privacy, as these connected cars can function only through the collection, analysis, and integration of large quantity of data.

The final consideration moves the debate about the social and economic disruption of digital innovation back to the core of the structural definition of the risk regulation regime. In fact, the idea of regulation stems originally from the cybernetic perspective of organizing control systems. These systems operate through the function of standard-setting. But this function is paired with intrinsically interconnected functions of information-gathering and behaviour-modification.[2] The complexity of risks created by digital innovation seems to necessitate the creation of a regulatory control system which is focused not only on the formal compliance with formal rules and standards, but also on the technical aspects of the information-gathering and on the ethical aspects of the real impact of those rules (behaviour-modification). Risk regulation, in this sense, should be able to integrate in its tripartite model of risk assessment, risk management and risk communication the profound ethical issues that materialize. The new digital service and products, in fact, present risks that cannot be easily measured or quantified in accordance with a mere technocratic paradigm; they do not only affect the individuals that use them, but transform the collective fabric of our society; they

[2] C Hood, H Rothstein and R Baldwin, *The Government of Risk: Understanding Risk Regulation Regimes* (Oxford University Press 2001) 23.

concern the cognitive rather than the physical integrity of human beings. One could think, for example, of the concerns raised about the echo chambers or filter bubbles created by social media, or the extent of the inadvertent digital manipulation of our behaviour and the invisible and therefore uncontrollable forms of algorithmic discrimination.

Hoping that the new livery of this journal will trigger the interest of risk regulation scholars in exploring new connections between digital data and risks, we will now examine the three conditions presented above and discuss their links.

II. The concept of risk embedded in the GDPR

As we have already seen, the collection and use of personal data will be regulated in the EU by the GDPR, that will apply as of May 2018. In this new legal framework, the concrete operative functioning of which is still not fully developed yet,[3] the concept of risk will play a crucial role. This is not just because the word "risk" is widely used in the text of the GDPR, or at least it is certainly more frequently used than in the previous legislative instrument that will be replaced, i.e. Directive 95/46/EC. In the latter, the concept of risk occurs in relation to data security and for the justification of a separate category of sensitive data. Health information, political opinions or religious beliefs fall into that category on account of being likely, by virtue of their nature, scope or their purposes, to pose specific risks to the rights and freedoms of individuals.[4] It is perhaps important to make a clarification about the role of risk or, better, risk-based model, in data protection law, which still generates some confusion and misunderstanding between experts. In the gestation of the new data protection law, the risk-based model emerged in public debates as a synonym with a more flexible approach to ensure compliance with data protection law. It was opposed by those who wanted rules on data protection to be serious and effective.[5] In reality, the "*riskification*" of data protection legislation in the GDPR has a much more profound underpinning, which goes well beyond considering "risk-based" as a model for enforcement. First, the idea of the control of risks marks the essence of the new regulatory tool that data controllers should use to measure the impact of new technologies, the "Data Protection Impact Assessment" or DPIA – Article 35 of Regulation (EU) 679/2016. Second, whilst Directive 95/46/EC mentioned, but did not describe, what the risks to the rights and freedoms of individuals are, the GDPR presents

[3] For example, the GDPR foresees the creation of a new EU body, the European Data Protection Board (EDPB) composed of the various supervisory authorities with series of important tasks, including issuing guidelines and recommendations, necessary to operationalize the new regulatory framework.

[4] Recital 53 of Directive 95/46/EC. In the GDPR, the special category of sensitive data is maintained.

[5] This claim seems to confuse the application of risk analysis to two different issues: the rules aimed at regulating risks and the processes by which the rules are enforced on the basis of the alleged risk of non-compliance. Although risk plays a role in both, risk regulation and risk-based regulation are completely different concepts. For a overview of risk-based regulatory models *cf*: J Black and R Baldwin, "Really responsive Risk Based Regulation" (2010) 32 *Law and Policy* 181; J Black and R Baldwin, "When risk based regulation aims low: A strategic framework" (2012) 6 (2) *Regulation and Governance* 131. This understanding of risk-based regulation has been the object of a specific statement issued by the Article 29 Working Party, the network of independent national data protection authorities created by Directive 95/46/EC during the adoption of the legislative proposal of the GDPR. *Cf* "Statement on the role of risk-based approach in data protection legal framework", adopted on the 30 May 2014, available at <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf>.

a detailed overview of the criteria for the definition of the risks. Recital 75 informs us that risks to the rights and freedoms:

> "may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects".

This is, then, followed by a reference to the objective assessment needed to evaluate these risks depending on the likelihood and severity and by a reference to the code of conducts and guidelines that could provide best practices "to mitigate the risk". There is a need for more in-depth analysis of the severity of these risks and for a refinement of the language used to describe negative events resulting from unlawful processing of personal data. The severity of risks depends, in the final analysis, on the evaluation of the harmful consequence by size or nature of the unwanted event occurring. It remains to be seen whether the highly individualized set of attitudes to avoid privacy risks could result in a more homogenous baseline of events that could be assessed in an objective manner, depending on the likelihood and severity of risks. Although the GDPR makes reference to risks in other instances,[6] the introduction of the principle of accountability grounds the idea of risk control at the very heart of the new enforced self-regulation model adopted to guarantee compliance with the provisions of the legislation. A set of governance measures to control risks will be available to data controllers, including the performance of DPIAs but also the appointment of data protection officers (DPOs), and the adoption of regulatory strategies to embed data protection principles "by design" and "by default" in new data processing systems.

III. Combination of products, combination of risks

Besides the regulatory approach moulded on the control of risks, which forms the basis of the new EU data protection legislation, risk regulation theory remains relevant in the field of digital technological development essentially because the products that were traditionally in the scope of risk regulation are being transformed and digitally enhanced. This entails the use of connected data-processing sensors and devices that are either integrated with the product or exert an ancillary function. In this way, users' behaviour is

[6] For example, with regard to "the right to be forgotten" it is clarified that the right of the data subject to have his or her data erased and no longer processed is particularly important in those cases where "the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing and later wants to remove such personal data, especially on the Internet" (Recital 65).

monitored, influenced or even enabled by digital technologies. The mass of data created by the products would pose a new risk to be assessed and managed, together with the usual risks to the safety of the users or to the environment. This becomes particularly challenging when the additional smart feature modifies the risk profile of the use of the product, bringing a trade-off between risks of a different nature or, better, between risks to privacy and alleged benefits to individuals. Take, for example, the case of digital pills: the sensor implanted in the pill is meant to guarantee the transmission of data for monitoring the intake of medicines by patients and therefore decrease the risk of non-adherence to the recommended treatment.[7] Or consider the use of "smart" metering in the distribution of energy and the relative problems of balancing the legitimate interest to make efficient decisions on energy distribution, which could result in benefits to consumers, and the risk posed by the mass collection of personal data from the use of electrical appliances and the personal insight into private life of individual households that analysis of consumption patterns could provide.[8] When the new smart version of the product becomes commercially dominant, users will not effectively opt-out from the processing of the data connected to the use of the product that could gradually become the standard commercial practice.[9] The tension between risks of a different nature and between risks and benefits will be an important aspect of development and discussion in risk regulation studies.

IV. Risk regulation and data protection meet the ethical aspects of technology development

In the relationship between risk regulation and data protection, a special place is occupied by the emergent field of data ethics.[10] The ethical considerations which are relevant to the consequences of the emerging digital technologies are connected with the new form of unprecedented informational power. It would probably be over-reductive to refer to this change only as a consequence of extended computational capabilities. "Big Data" is not only a technological artefact, but a much more complex phenomenon of epistemic change that affects the availability of knowledge and the governance of the public and private space.[11] To oversimplify, Big Data is a new form of power and the

[7] A Ward, "US regulator accepts chip in a pill application", *Financial Times*, 10 September 2015, available at: <https://www.ft.com/content/dececе84-57b1-11e5-a28b-50226830d644>. It appears that the regulatory review of the digital pill by the FDA was not as swift as originally thought by the developers and it will require more testing: <http://www.mobihealthnews.com/content/fda-declines-approve-proteus-otsuka-sensor-equipped-pill-asks-more-tests>.

[8] Article 29 Working Party Opinion on smart metering No 12/2011 adopted on 4 April 2011 available at: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf>.

[9] This point is particularly visible when the offer of services implies a transfer of personal data which data subjects are not able to monetize. The difference between a ride in a traditional taxi and in an Uber car is not only about the pricing modalities, but that in the case of Uber, the transaction between the parties is partly monetary and partly based on a voluntary transfer of geolocation and behavioural data. For an in-depth study of the legal issues connected with the competition offered by digital platforms, see A Ezrachi and ME Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Cambridge MA: Harvard University Press 2016).

[10] For a reference on "data ethics" see L Floridi and M Taddeo, "What is Data Ethics?" (2016) 374 *Philosophical Transactions of the Royal Society* Part A. More in general about the impact that new digital technologies are having on knowledge and ethics is L Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality* (Oxford University Press 2014).

[11] Council for Big Data, Ethics and Society, "Perspectives on Big Data, Ethics and Society", report prepared by Jacob Metcalfe, Emily F Keller and danah boyd, May 2016 available at: <http://bdes.datasociety.net/wp-content/uploads/2016/05/Perspectives-on-Big-Data.pdf>, 5.

benefits and risks stemming from the use of this new analytical power are substantial, complex and yet unclear in their scope and nature. We are just starting to realize the full extent of the consequences of the fact that the design of social media generates "echo chambers" and "filter bubbles",[12] problematic social developments undermining profoundly the public space and the common sense of belonging to a social community. Another important development is the erosion of our capacity to choose freely, due to digital manipulation of the information sources framing our decision-making,[13] and, finally, the thorny issues of algorithmic discrimination,[14] whereby mathematical models, which embed the logic of their creators, could determine and shape our life. It is therefore evident that some of the risks posed by Big Data exceed the limited scope of data protection law and present more general ethical challenges.[15] In this context, the rigorous methodology of risk regulation could be essential. First, through an analytical approach, risk regulation can unbundle the set of multiple and heterogeneous risks posed by "Big Data". Second, the tripartite composition of the institutional framework could certainly help to ensure that the review process of these risks is conducted in an objective, transparent, independent, and accountable manner. The risk regulation model has been often associated with a technocratic form of governance, but this is not necessarily true. In fact, there is nothing preventing ethical concerns from being integrated in the decision-making process of risk management, of the decisions that collectively are deemed fair and just. This model would be essential in order to counterbalance new forms of technological power, which aim at programming our cognitive understanding of the world and advancing an idea of human behaviour as "programmed behaviour systems" with a renewed sense of collective *responsibility*. It is, perhaps, timely to recall the lecture of the German philosopher Hans Jonas, who speaking of the technological modalities of behaviour control and social functionalism, wrote in a rather prophetic way: "Somewhere along the line of increasing social manageability at the price of individual autonomy, the question of the worthwhileness of the whole human enterprise must pose itself. Answering it involves the image of man we entertain. We must think it anew in light of the things we can do with it or to it now and could never do before".[16]

V. Conclusion

In the final scenes of Mozart's *Mariage de Figaro*, the vicissitudes of troubled lovers and couples, after a series of encounters and unexpected revelations, come to a happy end and every character finds again its place in the order of things. The category of risk and

[12] E Parisier, *The Filter Bubble: What the Internet is Hiding From You* (New York: Penguin Press 2011); W Quattrociocchi, A Scala and C Sunstein, *Echo Chambers on Facebook* (2016) paper available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2795110>.

[13] F Pasquale, *The Black Box Society: the Secret Algorithms that Control Money and Information* (Cambridge, MA: Harvard University Press 2015).

[14] C O'Neilly, *Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy* (Allen Lane 2016).

[15] B D Mittelstadt, P Allo, M Taddeo, S Wachter and L Floridi, "The Ethics of Algorithms: Mapping the Debate" in (2016) 3(2) *Big Data & Society* 1.

[16] H Jonas, *The Imperative of Responsibility. In search of an Ethics for the Technological Age* (University of Chicago Press 1984) 20.

the methodology of risk regulation offer powerful theoretical instruments and practical solutions to avoid unnecessary, preventable harm and enable the societal benefit accrued by technological innovation. This has resulted in perfectible, yet functioning, models for the control of risks previously considered unimaginable, such as those of nuclear energy and nanotechnology. Likewise, risk regulation will be an essential governance instrument for the control of the risks of the digital "infosphere" we inhabit. It is a complex relationship that pulls, as in a complicated ménage, concepts and models in many different directions. It is fertile territory for the inquisitive mind.