Feedback for the EU Commission

"Public Consultation on a Set of European Digital Principles"

Giulia Schneider – Denise Amram –Caterina Sganga and Giovanni Comandé[1]

*LIDER Lab, DIRPOLIS Institute, Scuola Superiore Sant'Anna (Pisa- Italy)

Table of contents: 1. Introduction. 2. Digital Education. 3. Data-Driven Research. 4. Digital Health and Health Data Space. 5. Data Sharing. 6. Children. 7. Businesses' Digital Responsibility: a New Framework?

1. Introduction

This feedback is provided considering the ongoing studies undertaken within the LIDER Lab research activities (www.lider-lab.it) at Scuola Superiore Sant'Anna (SSSA; www.santannapisa.it).

[1] Giulia Schneider, PhD (Bocconi University), is currently postdoc Researcher at Scuola Superiore Sant'Anna (giulia.schneider@santannapisa.it); Denise Amram, PhD (SSSA), is currently Affiliate Researcher at Scuola Superiore Sant'Anna and Data Protection Officer (denise.amram@santannapisa.it); Giovanni Comandé, PhD (SSSA) LLM (Harvard), is Full Professor of Private Comparative Law at Scuola Superiore Sant'Anna and Director of LIDER – Lab (giovanni.comande@santannapisa.it); Caterina Sganga, PhD (SSSA) LLM Yale, is Associate Professor of Private Comparative Law at Scuola Superiore Sant'Anna (caterina.sganga@santannapisa.it). The feedback is provided under the H2020 projects *ReCreating Europe: Rethinking Digital Copyright law for a culturally diverse, accessible and creative Europe* (GA 870626); *SoBigData ++: European Integrated Infrastructure for Social Mining and Big Data Analytics* (GA 871042); *LeADS: Legally Attentive Data Scientists* (GA 956562).

Our remarks focus on six specific sectors in which the envisaged European digital principles should be effectively operationalised: i) digital education; ii) data-driven research and the GDPR; iii) digital health and health data space; iv) data sharing; v) children needs in the digital space; vi) businesses' digital responsibility.

2. Digital Education

The principles of **universal access to internet service**; of students' **active participation in society and in democratic processes**; as well as of an **open, secure and trusted online environment** become key aspects of the consolidating digital education system as stirred by the Covid-19 pandemic.

A fair governance of copyrighted content and a full actionability of the fundamental right to data protection in its various substantial and procedural dimensions are two fundamental safeguards needed to address the deeper – and perhaps more worrisome – implications of the ongoing 'platformisation' of the postpandemic education system[2].

Among these implications, one has to think, for example, about the digital divides possibly affecting learning activities. In this respect, digital literacy problems may also impede access to education to minority groups who not only may not have the means to attend online learning courses, but also may not have the relevant technical knowledge to use needed devices and software. Lack of digital literacy and skills to deploy digital services may impair also childrens' digital education and training activities. Specific lines of intervention are thus needed assuring that **children and young people are equipped with the competences needed to navigate safely and responsibly online from an early age throughout their education and training.** Education institutions should take charge of these problems, assuring equal access to remote education experiences though the provision to vulnerable student groups of the relevant digital resources as well as the training required to maximize the online learning experience[3]. Obviously, this comes with substantial costs that education institutions will have to face in addition to the costs needed to access the digital services provided by third parties.

Furthermore, with big data companies entering the education sector and becoming relevant parties in the new digital education system, the risk that digital education will be increasingly shaped and

---

[2] R. Ducato, C. Angiolini, A. Giannopoulou, G. Schneider, (2020). Remote Teaching During the Pandemic and Beyond: Data Protection and Privacy of EdTech. *Opinio Juris in Comparatione*, 1, 43-72.

[3] S. Vincent-Lancrin, R. Van der Vlies, (6 April 2020). Trustworthy Artificial Intelligence (AI) in Education: Promises and Challenges. *OECD Working Papers n. 218* https://www.oecd-ilibrary.org/education/trustworthy-artificial-intelligence-ai-in-education_a6c90fa9-en.

determined by the technological infrastructure these companies offer need to be taken into consideration: in the sensitive education setting, the private code of digital services may well come to govern not only the law, but also the substance of our digitized education patterns. The underlying concern is thus that of an increasing standardization of learning programs across the globe, with the resulting compression on the one hand of education establishments' institutional autonomy, and on the other hand of the diverse and multicultural characterization of education system across different countries[4]. In the background, but not to be overlooked, there is also the risk of further exacerbation of the already ongoing process of privatization of education systems, now occurring in the form of an outright 'googlization' of learning environments.

Possible remedies to the creeping of these distortive implications of digital education systems may be found in collective contractual solutions, by means of education institutions' associations, which could come to counterbalance the contractual power of technology providers. In particular, these associations could support the negotiations with third parties though guidelines and legal technical support. Moreover, the adoption of certification and trust marks regarding chosen digital services could be a means of signaling a greater attention by education institutions regarding the selection of right-preserving technologies. These solutions are being currently explored by the European Parliament in the realm of consumer contracts for digital services[5] but could well be applied also in the context of contracts regarding digital education services. Ultimately, a last- and maybe most effective- way to overcome envisaged hazards of online education models would be that of investing in public digital learning infrastructures, through in-house development of the needed technological means. In this way, third party providers would be left out of the design of remote teaching spaces and the contractual imbalances these come to enact would be structurally nullified. This option would reassure full control by education institutions over the regulation of their education programs conducted online, to be defined in strict collaboration with relevant independent authorities, first of all data protection authorities and in case children are involved also the authorities in charge of **child protection**. While requiring a great amount of public funding, there's no certainty that the in-house development of online learning services by education institutions would be more expensive than charging- at an increasingly higher price- the access to online education spaces owned and controlled by third parties. The proposed solutions could largely advance the implementation within the digital

[4] L. Pascault, B.J. Jütte, G. Noto La Diega, G. Priora, (2020). Copyright and Remote Teaching in the Time of COVID-19: A Study of Contractual Terms and Conditions of Online Services. *European Intellectual Property Review,* 42(9), 548-555.

[5] European Parliament (February 2021). Update the Unfair Contract Terms Directive for Digital Services- Study Requested by the JURI Committee. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/676006/IPOL_STU(2021)676006_EN.pdf.

education space of the principles regarding the **protection and empowerment of children**, while promoting the employment of **human-centric algorithms** for education purposes.

3. Data-Driven Research and the GDPR

For the purposes of the development of an **open, secure and trusted online environment**, which relies on **human-centric algorithms fostering individual and societal wellbeing,** the identification of a clear regulatory framework regarding data-driven research proves essential**.** The more research over digital data is fostered and enabled at regulatory level, the greater amount of digital services is developed, thus **increasing access to the full benefits of digitisation**, for example in the **health or public sector**.

In this respect, the GDPR's regime for research-based processing activities entails fundamental standards, which are of paradigmatic relevance for the development of future data sharing policies within the EU Strategy for Data as well as for the orientation of forthcoming legislative interventions, as the proposed Data Governance Act and the announced European Health Data Space Regulation.

Indeed, the GDPR's special framework for research activities lays the grounds for a distinction between public interest- and commercially oriented- research. Up to now, these elements have not been adequately considered at policy level. As a result, public institutions and public research institutions are experiencing more troubles than private entities in their data sharing. We claim that this contradicts the very policy of the GDPR entangled in its research exceptions.

The complex framework provided by the GDPR for processing activities conducted for research purposes reveals how European data protection law entails the grounds for a solid development of fundamental rights-sound research policies, which take into account the specificities of the types of research pursued with the processing.

First of all, the GDPR lists a number of normative bases that legitimize the processing of special categories of data for the pursuing of research objectives. This framework is particularly relevant for research-based data sharing operations: in order to be lawful pursuant to art. 9(2) GDPR, these must be grounded in data subjects' "explicit consent to the processing of those personal data for one or more specified purposes" (art. 9(2)a GDPR); alternatively, they shall be functional to address serious cross-border threats to health or the safeguards of high standards of quality and safety of health care and of medicinal products or medical devices (art. 9(2)i GDPR); or serve research activities (art. 9(2)j GDPR).

However, the covid-19 experience has revealed the weaknesses of a system that is unable to take due account of both the link between existing databases and new databases, and the benefits of sharing with and by the public. Indeed, art. 9(2)a, and art. 9(2)i GDPR see their limits when we try to apply them to "regular" research, and outside instances statutorily envisaged in a legislation.

Nevertheless, the mentioned legal bases describe a scale of different data protection regimes ranging from data subject-controlled to data controller-oriented ones. These data protection regimes are given by the combination between the lawful bases under art. 9(2) GDPR and the GDPR's normative standards specifically regarding research. The most relevant of the current data protection law's rules concerning data processing (thus, also data sharing) activities conducted for research purposes is given by the so-called default compatibility under arts. 5(1) lett. b) and 6(4) GDPR: the combined reading of these two provisions sets a presumption of compatibility with the original purposes of the processing for those further data processing activities that target research purposes (a test expressly used by the EDPB in setting the safeguards for extra-EU data transfer[6]). Moreover, when it comes to research over personal data, the GDPR enables data controllers (and thus, parties to a data sharing operation) to derogate to fundamental data protection principles, as the storage limitation principle under 5(1) lett. e) GDPR, and to specific data protection rights, as the right to erasure (Art. 17(3) lett. c) GDPR) or or the right to access information regarding the performed research activities (Art. 14(5) lett. b) GDPR). However, these derogations come along with the obligation for controllers, established under art. 89(1) GDPR, to implement adequate safeguards in the form of technical and organisational measures for the protection of the rights and freedoms of the interested data subjects. At a deeper consideration, the traced framework appears to entail sufficient flexibilities in order to modulate the set data protection regime for research on the basis of the different types of research the enacted data processing activity- and thus the correspondent data sharing operation- targets. Accordingly, we envisage a finetuning of the mentioned data protection rules for research, requiring greater control of data subjects- possibly through consent- for research enquiries over personal data oriented towards for profit purposes and, conversely, allowing for greater loss of control for data subjects but triggering greater responsibilities onto controllers in case research is conducted for the public interest[7]. The set framework could be relevant to orient **fair dealing practices** regarding the

[6] European Data Protection Board, 'Recommendations 1/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (10 November 2020) https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransfertools_en.pdf.

[7] G. Comandè- G. Schneider, Can the GDPR Make Data Flow for Research Easier? Yes it Can, by Differentiating! A Careful Reading of the GDPR Shows how EU Data Protection Law Leaves Open Some Significant Flexibilities for Data Protection-sound Research Activities, in Computer Law & Security Review, 2021, 41, 105539; G. Comandè- G. Schneider, Differential Data Protection Regimes in Data-driven Research: Why the GDPR is More Research-friendly than You Think, in German Law Journal, 2021, forthcoming, online available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3897258.

transfer and re-use of personal data among businesses, and in particular **in the relationships with online platforms**.

4. Digital Health and Health Data Space

The implications of the proposed finetuning of the data protection derogations and safeguards for research enquiries based on personal data appear to be particularly promising in respect to the **digital health sector** and in particular in respect to the upcoming **health data space**. In particular, an effective implementation of relevant data protection principles and safeguards in research enquiries over health data- as finetinued in respect to the public interest or commercial orientation of the conducted research- is essential **for the design of digital health and care services that are inclusive, accessible, equitable and designed to meet peoples' needs.** The design of digital health research projects largely reflects itself on the design of digital health services, **as personalised medicine and telemedicine services**: this means that **a secure, non-discriminatory and confidential design of research patterns in digital health** will benefit the digital health services finally marketed, in terms of higher protection assured to users, **including the most vulnerable and with disability or at risk of exclusion**.

Under these premises and in respect to mixed private-public health datasets employed for research purposes, the data protection research regime should be calibrated based on the influence that commercial undertakings have within established research partnerships or organisations. The degree of influence of these entities indeed determines the risk of commercial "capture" of research results (when for-profit interests weight in).

The involvement of for-profit organisations and thus their influence in the governance of research projects and results can be derived from specific parameters. In this respect, the Copyright Directive mentions some parameters that can be relevant also for the purposes of data protection. In particular, recital 12 of the Directive refers the influence by commercial-oriented organisations in research activities to "structural situations" as a qualified shareholder control or the presence of specific members of for-profit organisations in the management of research projects. These structural situations may engender a direct control by these organisations over research infrastructures and thus over initiated research patterns. As the recital suggests, these structural situations may in turn favour a preferential access to the results of the research by for profit organisations. Note also that such preferential access would be dealt with in separate agreements.

In case a "decisive influence" of for-profit organisations over the established research partnership or organisation exists, safeguards should be as strict as in the case of a fully for-profit conducted research. Conversely, in case the control of the research endeavours over mixed private-public datasets primarily resides onto the public entity, the identified mentioned data protection flexibilities could be exploited to the maximum.

However, under the GDPR it is not who funds the research that matters, but its scope. The reason why it is so and why it is a better solution can be clarified by an example. Using the dichotomy under the Copyright Directive could prove to be difficult in respect to private-public partnerships established for grounds of public health protection, as is occurring in the fight against the Coronavirus pandemic. For instance, in the collaboration between private and public actors, as in the "Innovative Medicines Initiative", based on a public-private partnership between the European Commission and the pharmaceutical industry, it might trigger the enactment of higher data protection safeguards and lower derogations from the ordinary regime, merely because of the presence of commercial-oriented stakeholders. Nonetheless, purposes of public health protection, and the need of immediate research actions, could conversely suggest a relaxation of data protection checkpoints. In the specific cases where mixed health data pools are employed for research purposes in the public interest in the area of public health, such as for the protection against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, the higher level of restrictions on the processing of special categories of personal data can be relaxed, in accordance with what is required for the processing for public interest purposes under art. 9(2) j) GDPR, disregarding the public or private nature of the subjects involved.

5. Data Sharing

The proposed analytical framework is of great practical relevance for the purposes of determining how "open" valuable research datasets are in the market: the lighter data protection regime applicable to public interest-related research facilitates sharing practices regarding personal data and creates less interference with the application of those European regulations establishing access regimes over data, such as the Regulation on the free flow of non-personal data, the Open Data Directive, and also the announced Data Governance and Digital Single Market Acts that will further address data sharing practices among platforms.

All these regulations appear to reflect the emergence of a new principle regarding the free movement of research data in the European internal market[8]. The said principle encompasses four data sharing types:

1) public data employed for public interest-related research and innovation purposes also with private partners;

2) private data employed for public-interest related research and innovation purposes;

3) public data employed for commercial-related research and innovation purposes;

4) private data employed for commercial-related research and innovation purposes;

A closer look at the emerging regulations regarding data sharing shows how this principle is differently substantiated at European regulatory level in respect to these different data sharing types, echoing the above illustrated distinctions among data protection regimes for research.

The data protection regimes applicable to a sharing operation encompassing personal data differently influence the simplicity of such sharing. The interference between data protection law and established access and sharing regimes needs to be assessed in consistency with differential data protection regimes: the highlighted flexibilities under the GDPR enable the compression of data protection principles and rights in favour of greater data accessibility and sharing when the resulting processing of personal data is conducted for public interest-oriented (research) purposes. Conversely, a greater interference with the considered access regimes by data protection requirements, should occur when the processing of personal data is related to for profit-oriented (research) operations.

From the very opposite perspective, it cannot be denied how also the regulatory framework provided by the Data Governance Act is destined to have an impact on the shaping of the different data protection regimes. In its present form the DGA reaches an important milestone in the definition of a more structured data sharing environment, characterised by clearer procedural and substantial rules and allocation of responsibilities of involved players. In doing so, it aims at increasing trust in the evolving European sharing ecosystem. Nonetheless, it creates also a natural spillover effect over applicable data protection regimes: the registration requirements of data altruism organisations; the notification regime for data intermediaries; as well as the conditions set for the re-use of public sector information are normative requirements that, once the proposed Regulation comes into force, will have to be taken into consideration also in reference to the applicable data protection regimes. More precisely, the requirements under the proposed Data Governance Act will have to be considered when defining the "appropriate safeguards" to which the GDPR often refers to, for example under art. 89 GDPR. In this light, the provisions of the DGA may play out as normative elements supporting the

[8] OECD Report, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD PUBLISHING, PARIS (2019), https://doi.org/10.1787/276aaca8-en

data protection framework, under the common objective of establishing a fundamental rights-sound data sharing environment.

The consideration of the **multilevel interaction** between data protection rules under the GDPR and the envisaged regulations regarding data sharing under the proposed Data Governance Act is key for the design of **participatory digital education models; inclusive digital health services as well as accessible and human-centric digital public services and administration**.

6. Children Needs in the Digital Space

The Digital Compass Communication[9] proposes to include "the right to Protecting and empowering children and young people in the online space" to shape the concept of EU digital citizenship. In this vein, the envisaged **European digital identity system** could become a means not only to protect **children and young people wellbeing**, but to effectively empower them through the opportunities deployed in the digital space and t**o promote their participation as digital citizens in the online environment**.

In this regard, we underline as follows.

- The digital environment is a new scenario where children's rights shall be promoted and protected. Current debates on Artificial Intelligence (AI), Robotics and Internet of Things (IoT) regulations are not addressing specific technical and organizational measures for a child-friendly paradigm to comply with by design and by default[10]: policy and law-making efforts are mainly driven towards common requirements and standards for developers, intermediaries, service providers, etc. without highlighting the vulnerabilities emerging whereas children are the data subjects / end-users.
- The role of parents, caregivers, educators, facilitators is the main driver to ensure case-by-case the pursuing of the best interests of the child in the use of AI-based technologies / IoT services. This approach could be necessary to protect children's rights. However, it is not sufficient to empower children's rights.

[9] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions- 2030 Digital Compas: the European Way to the Digital Decade, 9 March 2021, COM(2021)118 final, https://ec.europa.eu/info/sites/default/files/communication-digital-compass-2030_en.pdf.

[10] High Leve Expert Group on AI of the European Commission, Ethics guidelines for trustworthy AI, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

- Considering risks and opportunities that the Research & Innovation & Development (R&I&D) solutions are bringing in the children's everyday life, a risk-based approach shall be adopted, identifying roles and responsibilities upon all the agents, including parents and caregivers.
- In this regard, nine requirements have been identified within the UNICEF Policy Guidance on AI for Children[11]. Their implementation into a EU Commission strategy need to also to address the following legal challenges:
    1. to regulate the concepts of responsibility, liability and accountability in adults-child relationships in the digital environment.
    2. to identify a multi-level system of roles and responsibilities aimed at protecting and promoting children's rights according to their age, maturity, skills and competence.
    3. to promote specific educational paths for children, parents/caregivers, teachers/facilitators to develop awareness on risks and opportunities of the digital environment.

7. Businesses' Digital Responsibility: a New Framework?

Companies' use of data and digital technologies entails substantial risks in terms of exploitation and misuse of data, breach of privacy, and discrimination. In light of these threats, the way in which businesses shape and oversee their data collection and retention practices go well beyond mere regulatory compliance concerns and determine, to a broad extent, the role of companies in promoting or undermining human rights, social values and fundamental principles[12]. In this perspective, while digitalisation patterns are starting to be regarded as an outright driver for businesses' transition to sustainable business models directly advocated by the recent European policy developments[13], they also bring about new responsibilities for businesses. In relation to digital technologies, the same general notion of "good governance", often recurring in the recent European Parliament's Resolutions

[11] UNICEF, Policy Guidance on AI for Children, https://www.unicef.org/globalinsight/reports/policy-guidance-ai-children.
[12] Iris H-Y Chiu & Ernest Lim, *Managing Corporations' Risk in Adopting Artificial Intelligence: A Corporate Responsibility Paradigm*, 19 Wash U Global Stud L Rev (2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3780586.
[13] See art. 3 of the Regulation EU 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility, 18 February 2021. David Salb & Hershey Friedman & Linda Friedman, *The Role of Information Technology in Fulfilling the Promise of Corporate Social Responsibility*, 4 Computer and Information Science 2 (2011) http://www.ccsenet.org/journal/index.php/cis/article/view/10661David Salb & Hershey Friedman & Linda Friedman, *The Role of Information Technology in Fulfilling the Promise of Corporate Social Responsibility*, 4 Computer and Information Science 2 (2011) http://www.ccsenet.org/journal/index.php/cis/article/view/10661.

as well in the Draft for a Directive on corporate due diligence and corporate accountability[14], appears to imply the prescription of implementing good governance policies regarding employed data management models and produced digital technologies.

In this respect, exactly for their social risk implications, businesses' data governance practices are to be ascribed to the realm of corporate social responsibility, as interpreted in the light of businesses' current digitalisation trends.

The relevance of corporations' technologies *vis à vis* social justice and common good objectives is at the roots of current reflections regarding "public interest-technologies", which evolve around the identification of legal tools relevant for orienting corporations to design and orient their data processes and resulting technologies in consistency with the public interest[15].

Against this backdrop, the general corporate social responsibility paradigm offers a fruitful ally for orienting businesses to address the risks arising from their data processing models, **also in respect to environmental protection**, and to disclose efforts in this regard to society. In this regard, it offers an operational tool relevant for achieving the general European policy objectives regarding **the creation of a sustainable data economy**, which structurally relies on building trust of external stakeholders regarding economic operators' data processing practices. This could be also achieved through the release of **information on the environmental footprint of digital services and technologies**. The notion of corporate digital responsibility is being increasingly enquired in business studies[16], where it has been defined as "a set of practices and behaviours that help an organization use data and digital technologies in a way that is socially, economically, technologically, and environmentally responsible". It is also currently considered at political national level by two initiatives of the French and German governments[17]. These initiatives aim at permeating corporate social responsibility with the governance of corporations' digital risks, along the lines of a newly emerging notion of corporate digital responsibility.

---

[14] European Parliament resolution of 10 March 2021 with recommendations to the Commission on corporate due diligence and corporate accountability, (2020/2129(INL)) https://www.europarl.europa.eu/doceo/document/TA-9-2021-0073_EN.html. See also European Parliament, Report with recommendations to the Commission on corporate due diligence and corporate accountability, (2020/2129(INL) https://www.europarl.europa.eu/doceo/document/A-9-2021-0018_EN.html.

[15] E. Lu, *Public Interest Corporations in the US and the Promotion of Public-Interest Technology*, STLR (28 December 2020) https://journals.library.columbia.edu/index.php/stlr/blog/view/291.

[16] M. Wade, *Corporate Responsibility in the Digital Era*, MIT Sloan Management Review (28 April 2020) https://sloanreview.mit.edu/article/corporate-responsibility-in-the-digital-era/.

[17] Bundesministerium für Justiz und Verbraucherschutz, *Corporate Digital Responsibility Initiative: Shaping the Digitalization Process Responsibly: A joint platform*, https://www.bmjv.de/SharedDocs/Downloads/DE/News/Artikel/100818_CDR-Initiative_EN.pdf?__blob=publicationFile&v=3. France Stratégie, *Corporate Digital Responsibility- 1. Data Key Isuues Synthesis*, https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-2020-corporate-digital-responsibility-juillet.pdf.

Referring the governance of digital technologies to the realm of businesses' social responsibility could- even more in case a directive regarding corporate due diligence and corporate accountability would enter in force- push businesses beyond formal compliance requirements, making them more proactive **in the responsible shaping of their market practices regarding their digital products and services also in respect to their environmental impact.**