ISSN 2281-5147

COMPARING EU INITIATIVES ON DATA: ADDRESSING RISKS AND ENHANCING HARMONISATION OPPORTUNITIES.

Denise Amram*

Abstract

The Author provides a mapping of the recent EU legislative initiatives on data, identifying common interpretative issues and gaps emerging from the fragmented evolution of the legal framework. In order to give a systematic interpretation of the different provisions, two sectorial initiatives impacting on completely different scenarios are compared: the European Health Data Space proposal and the Digital Service Act. This cross-sector exercise allows the Author to identify those common principles able to shape effective implementations strategies aiming to protect fundamental rights and democratic values in the information society.

Indice Contributo

* Assistant Professor of Comparative Private Law, Scuola Superiore Sant'Anna, Pisa. The research has been financially supported by VALKYRIES project Harmonization and Pre-Standardization of Equipment, Training and Tactical Coordinated procedures for First Aid Vehicles deployment on European multi-victim Disasters H2020 GA 101020676 and the Programma Operativo Nazionale Ricerca e Innovazione 2014-2020, PON "Il danno alla persona e la giustizia predittiva". The author is grateful to the anonymous referees for their fruitful comments.

ISSN 2281-5147

Keywords

Personal and non-personal data, data governance, health data space, digital services, impact assessments.

1. The EU Data Strategy: common features and tailored specifications.

The increasing datafication of the society required a new legislative approach aiming to regulate the consequences of digitalisation of services and products and to adapt the current applicable framework to the new risks and opportunities emerging within the information society dimensions. Data, in fact, have become essential either in business (B2B) or business to consumers contractual relationships (B2C) or among private organisations and public institutions (B2G)[1].

[1] B. Martens et al., Business-to-Business data sharing: An economic and legal analysis, JRC, Seville, 2020; A. Acquisti, C. Taylor and L. Wagman (2017) Economics of privacy, Journal of Economic

ISSN 2281-5147

The EU approach in dealing with information society consists of shaping a strategy for single market for data where information can be shared across sectors in a transparent and fair manner, in compliance with the needs of confidentiality emerging from privacy and data protection rules and competition law[2].

To this end, a series of legislative initiatives have been promoted in order to boost data economy growth both in commercial and industrial sectors. In particular, the EU Reg. n. 2016/679 on General Data Protection Regulation (GDPR) and the EU Reg. n. 2018/1807 on Free Flow of non-personal data are defining how to process personal and non-personal data in EU, identifying conditions to ensure the free circulation of information. Moreover, the Data Governance Act (DGA) together with the EU Dir. n. 2019/1024 on Open Data Directive aim to facilitate the data sharing and their re-use, by reinforcing trust in data sharing intermediaries and in the public sector, in alignment with the purposes of openness in the digital market. These mentioned initiatives shall be read in a perspective of fostering innovation and competitiveness in several sectors, as specified by the Data Act (*i.e.* the Proposal for a Regulation of harmonised rules on fair access to and use of data, that has been published in 2022), setting rules for data exploitation to create value from them. These initiatives can be considered as the general framework on data-driven matters, functional to be "accommodated" and adapted for specific purposes and means. To regulate consistent applications of data processing in different sectors, indeed, is one of the EU challenges to boost data economy and innovation[3].

Literature 54(2), 442-492; OECD (2019) Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing.

[2] M. Burri (ed), Big Data and Global Trade Law, Cambridge, 2021; A. Kuenzler, What competition law can do for data privacy (and vice versa), Computer Law & Security Review, Volume 47, 2022, 105757, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2022.105757; A. Davola; G. Malgieri, Data, power and competition law: the (im)possible mission of the DMA?, Research in Law and Economics, forthcoming, 2023.

[3] M. Leistner, The Commission's vision for Europe's digital future: proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act—a critical primer, Journal of Intellectual Property Law & Practice, Volume 16, Issue 8, August 2021, Pages 778–784,

ISSN 2281-5147

To this end, it is essential to understand what is meant for data[4]. According to article 2 DGA, it is a "digital representation of acts, facts, or information", considered as a general asset. In this regard, further initiatives are focusing on defining sectorial boundaries and rules in terms of digital spaces where general provisions and specific ones find application. As complementary actions, indeed, we may focus on both the Digital Service Act (DSA), empowering users' rights among digital platforms, and the European Health Data Space Proposal of Regulation (EHDS), laying down rules and mechanisms to boost the secondary use of electronic health data, by creating common safe spaces to share personal and non-personal data of patients. These two examples of sectorial legislative initiatives are particularly significant for our analysis as they allow to assess the current general legal landscape under a plurality of grounds, impacting on different categories of vulnerable subjects. If we identify common principles to cover gaps and lacks, their role of enablers will find validation in terms of model to be able to circulate among sectors.

Firstly, we will deal with the necessity to cover possible gaps emerging from the different initiatives on data strategy. From the analysis, we will identify common notions to verify room for sectorial accommodations and possible evolutions of concepts between different regulatory frameworks. Then, we will focus on two sectorial initiatives impacting on different sectors, like health data spaces and digital platforms, in order verify whether or not a common methodology based on

https://doi.org/10.1093/jiplp/jpab054; C. Sganga, Ventisei anni di Direttiva Database alla prova della nuova Strategia europea per i dati: evoluzioni giurisprudenziali e percorsi di riforma, Il diritto dell'informazione e dell'informatica, 2022, p. 657 ff; V. Zeno-Zencovich, Data protection[ism], Rivista di diritto dei media, 2/2022, 1 ff; G. Malgieri, Bart Custers, Pricing Privacy – The Right to Know The Value of Your Personal Data (2017) Computer Law & Security Review <doi: 10.1016/j.clsr.2017.08.006>. Trix Mulder, Nynke E Vellinga, Exploring data protection challenges of automated driving, Computer Law & Security Review, Volume 40, 2021, 105530, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2021.105530.

[4] Quinn, P. and Malgieri, G., 2022, The Difficulty of Defining Sensitive Data – The Concept of Sensitive Data in the EU Data Protection Framework, German Law Journal, 2022, 22(8), 1583-1612. doi:10.1017/glj.2021.79.

ISSN 2281-5147

interoperable standards can be identified together with principles able to address the harmonisation process.

Last but not least, we will identify monitoring mechanisms to detect and develop best practices with a bottom-up approach, in order to address existing vulnerabilities and possible new ones in order to suggest content for self-regulatory instruments, like codes of conducts whose development is particularly supported by the EU Commission.

2. Applicable notions to general and sectorial initiatives.

All the mentioned EU legislative initiatives are contributing to the global aim to regulate the data-driven challenges, even if impacting on different topics and profiles. The fact that there isn't a unique text to define all the aspects of the information society arises a series of concerns in terms of possible lacks and overlaps that could constitute a practical barrier against an overall compliant approach for stakeholders.

A first premise for a harmonized interpretation and application of the provisions included in the strategy consists of comparing definitions developed in the legal texts. In particular, it is essential to identify what is meant for the main objects, actors, and actions of each relevant framework in order to shape the interplay of the stated rights and obligations to comply with. Secondly, it is necessary to detect common principles inspiring the law in action whereas applicative lacks are identified in order to align the interpretations[5].

In this regard, if we analyse the definition of "data", we could appreciate a declared alignment between the GDPR and the Free Flow Regulation where the latter recalls the notion given in the first one to identify the opposite field of application. Therefore, the GDPR refers to "any information relating to an identified or identifiable natural person", while Free Flow Regulation covers all other information.

[5] G. Comandé (ed.), Elgar Encyclopedia of Law and Data Science, Elgar Publishing, 2022.

ISSN 2281-5147

This approach seems easy to be addressed under a normative perspective as all possible information could have a regulatory framework of reference. However, in practice, it is not always so clear to establish whether or not a dataset includes only non-personal information. In fact, according to recital 26 GDPR, pseudonymized data are considered as personal data since with additional information persons are identifiable, taking into account the available technologies applied to the data processing. While anonymous information includes data not related to an identified or identifiable natural person or de-identified data, where data subject is not (or no longer) identifiable "by any means reasonably likely to be used"[6]. To distinguish between personal and non-personal data is essential in order to properly apply principles stated in the other legislative initiatives during their processing, however other characteristics of the information are relevant, especially in order to identify roles and responsibilities in the digital environment[7]. To this end, the DGA adds further details for the current analysis. In fact, as anticipated, in the DGA "data" is described as "any digital representation of acts, facts, or information", accessible in several formats including audio and video, specifying that non-personal data are those falling out from the personal data under the GDPR. Conversely, audio and video representing identifiable persons are included in the concept of personal data under GDPR. Such a specification introduced in the DGA finds justification in the Recital 30 of the Open Data Directive, where it refers to the previous Public Sector Information (PSI) Directive that was limited to the concept of document, whose definition "is not intended to cover computer programmes". Therefore, data is not only documents, but it includes information in any format that could be processed by

[6] ICO, Introduction to anonymisation, 2021, 15 https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf.

[7] C. Irti, Personal Data, Non-personal Data, Anonymised Data, Pseudonymised Data, De-identified Data, in R. Senigaglia, C. Irti, A. Bernes (eds), Privacy and Data Protection in Software Services, Springer, 2021, pp 49 ff.

ISSN 2281-5147

a human being, or automated mechanisms, for example those ones based on artificial intelligence. This simple statement becomes essential in the identification of the object of a contractual relationship or a duty/right, not only to establish compliance requirements, but also to identify what can be processed, who can process, who owns a given dataset etc. This is relevant also when data processing brings to develop services and products. For instance, if we analyse the Data Act notions and definitions, we may notice that Recital 6 identifies the designer/manufacturer and the user as main actors of that regulatory framework aiming to establish how users can access and reuse the data generated by a given digital service or product, by empowering their role with the main purpose to ensure that products are developed "in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user". Therefore, according to the Data Act any contractual relationship establishing a purchase, rent or lease of a product or digital service shall include a series of elements in order to allow and facilitate data sharing. In particular, details on how data are generated, stored, and made available to users shall be specified as mandatory content of contractual relationships, taking into account that limits to data access could be applied only in case of trade secrets or if generated data are considered as personal ones.

Under these premises, the EU Health Data Space Proposal recalls all notions included in the GDPR and the ones of data and data access described in DGA, specifying for its purposes that electronic health data refer to both personal and non-personal data concerning health and genetic information and relating determinants[8]. In fact, taking into account that a "residual risk that the capacity to re-identify could be or become available, beyond the means reasonably likely to be used (…) is present in relation to rare diseases (…) where the limited numbers of case reduce the possibility to fully aggregate the published data in order to preserve the privacy of natural persons while also maintaining an appropriate level of granularity in order to remain meaningful", an assessment on the characteristics of the data processed within a EHDS shall be

[8] G. Schneider, Health Data Pools Under European Data Protection and Competition Law, Springer, 2022.

ISSN 2281-5147

always undertaken. To this end, the level of granularity combined with the description of the characteristics of data subjects, and other information, like geolocalisation of patients or reduced number of cases, play a significant role to evaluate the impact on fundamental rights protection of a given access for reuse of collected and stored electronic health data[9]. Therefore, specific policy of reuse, also for non-personal data, and standards of aggregation shall be developed considering the features of datasets and the anonymization or aggregation techniques to protect data subjects' identity. The DSA, instead, does not provide an own notion of data. Considering the field of application, it is reasonably to apply the discussed extension of the concept of data beyond the documental perception of a data flow. Under the DSA, in fact, the main actors are the users-consumers and the intermediary services. The first ones, according to the general consumer law framework, are those acting for purposes which are outside their trade, business, craft, or profession and they can be recipients of a service online provided; while service providers are the ones who can transmit, cache or host information provided in a communication network provided by a recipient of the service. Conditions of liability are established under articles 3, 4, 5 for service providers, shaping the terms of a "responsible and diligent behaviour (…) for a safe, predictable and trusted online environment" (Recital 3 DSA), in order to prevent from sharing "illicit content" or to act against them. This latter notion is thus broadly conceived and referred to all information "irrespective of its form".

Some difficulties are emerging in the analysis of the main actors of the other legislative initiatives where roles may overlap in the interplay of different provisions[10]. As far as the target category whose fundamental rights shall be protected and promoted by the given legislative initiatives is concerned, we may list: the data subject under the GDPR, that is the identifiable natural person, whose notion is included in the DGA,

[9] A. Mantelero, AI and Big Data: a blueprint for a human rights, social and ethical impact assessment, Computer Law & Security R., 34:4(2018), pp. 754-772.

[10] J-S. Bergé - S. Grumbach - V. Zeno-Zencovich, The 'Datasphere', Data Flows beyond Control, and the Challenges for Law and Governance, in European Journal of Comparative Law & Governance, 5, 2018, p. 144.

ISSN 2281-5147

while defining the "data altruism", and that could be the consumer law. In addition, the data holder under the DGA refers to those who have technical and legal control of data, granting the possibility to share or to access to flows. It also remarks at Recital 15 the need to introduce safeguards to protect their commercial interests and intellectual property rights against unlawful or unauthorized access, especially in circumstances involving requests from non-EU countries. In fact, according to article 19 DGA, the right to be informed in case of international access as well as about the conditions of data altruism shall be always ensured[11].

Looking at the adaptations emerging from the EU Health Data Space proposal, it addresses its provisions both to natural and legal persons who are processing personal and non-personal data, specifying that the data holder shall arrange how to ensure the legal and technical interoperability in order to disclose the data to health data access bodies in compliance with GDPR (Recital 37). Three are the main actors: the data holder, who provide data to the data space, the data access body, that are playing the role as intermediaries and guarantor of the data subjects' anonymity, and the data user, who ask access to data for re-using purposes. The data holder could be an entity or a body in the health or care sector, or research institution, or specific organization identified by the EU/national law, processing health-related data that need to demonstrate the GDPR compliance to arrange their re-use. The data access bodies, indeed, are organisations established by the EU Member States, like -at this stage- Findata, French Data Hub, German Forschungsdatenzentren, that centralise the availability of electronic health data for secondary use. Data access bodies are entitled to "verify compliance and give data users and holders the opportunity to reply to any findings and to remedy any infringement" (Recital 48) and to provide the pseudonymization key to data users, who cannot attempt to re-identify data subjects. In fact, also in case of incidental findings or specific benefits that could emerge from the re-use of data, data users shall inform the data access body, that can solely directly

[11] A. Duisberg (2022), Legal Aspects of IDS: Data Sovereignty—What Does It Imply?, in B. Otto, M. ten Hompel, S. Wrobel (eds.) Designing Data Spaces. Springer, Cham. https://doi.org/10.1007/978-3-030-93975-5_5.

ISSN 2281-5147

contact the data subject. Also in case of request concerning statistical data, the processing is provided by the data access body that will then communicate only the results.

Such role of intermediary for the data access body is twofold since it ensures the protection of data subjects' identities from any possible attempt of re-identification, but it also includes technical assistance duties for data users in the selection of suitable datasets according to the approved request of access. For these reasons data access bodies shall be organised as a complex interdisciplinary structure, including, but not limited to a digital library management. Firstly, contractual relationships with data holders shall be developed in order to set conditions for data sharing in the health data space. Therefore, for any dataset a tailored assessment shall be undertaken and translated into contractual clauses for establishing terms and conditions for data sharing. Secondly, considering the role of intermediary body towards data subjects, it is necessary to establish specific procedure to interact with them, including reporting mechanisms to exercise rights, all possible ethical concerns in case of incidental findings communication, smart systems to extract aggregate data considering tailored thresholds depending on the granularity of stored data and requests. Thirdly, common procedure to evaluate data users request shall be developed and mechanisms of enforcement, monitoring, auditing, and reporting established. In the next paragraph we will deep these profiles.

3. Risk based assessments for personal and non-personal data processing.

A common feature of all the initiatives on EU data strategy is the approach based on risk assessment that imposes the main actors to analyse how the data-driven activity could affect fundamental rights of the target groups and therefore which safeguards shall be put in place in order to avoid harms in the given scenario(s) of application[12].

[12] G. Georgiadis, G. Poels, Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: A systematic literature review, Computer Law & Security Review, Volume 44, 2022, 105640, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2021.105640; R. Binns, Data protection impact assessments: a meta-

ISSN 2281-5147

The evaluation shall be put in place before enabling any data processing in order to reach the *by design* standards of compliance, meaning that the ethical legal issues are addressed since the very beginning and risks are consequently mitigated. Monitoring mechanisms of conformity during the development of the data-driven activity may contribute to achieve the by default standard as well, meaning that the solution could be put in the market as a fully compliant one. As known, these standards have been introduced for privacy-preserving techniques and extended to a general concept of ethical-legal assessment on fundamental rights protection. In this paragraph, we will analyse how these assessments are shaped for electronic health data processing in the EHDS and for online service providers in the DSA.

3.1 Risk based approach for health data spaces: comparing the existing experience with the EDHS provisions.

To address the risk-based approach by design and by default within a Health Data Space, the EHDS proposal identifies a procedure of access request addressing the ethical assessment in order to grant the secondary use and implement the proper technical and organisational safeguards. Firstly, in compliance with the principle of minimisation, any access to personal (pseudonymised and encrypted) data shall be justified by the data user (i.e. the natural or legal person who has lawful access to personal or non-personal electronic health data for secondary use), who will not get access to the re-identification key in any case. If no justification is provided, the request is considered for anonymised flows. The request shall include the legal basis, means and purposes envisaged for re-using the requested data (that shall be described) as well as the technical measures identified to protect the datasets during the re-use

regulatory approach, International Data Privacy Law, 2017, pp. 22 ff.; A. Mantelero, AI and Big Data: A blueprint for a human rights, social and ethical impact assessment, Computer Law and Security Review, 2018, 34 (4): pp. 754-772 ; N. van Dijk, R. Gellert, K. Rommetveit, *A Risk to a Right? Beyond Data Protection Risk Assessments*, 32 Computer Law and Security Review, 2017, pp. 286–306, https://doi.org/10.1016/j.clsr.2015.12.017.

ISSN 2281-5147

processing. In this regard, to comply with the highest standards of security, third parties might be involved and therefore appointed as data processors under the article 28 GDPR by the data access body that - according to Recital 54 - "should remain at all time in control of the access to the electronic health data with access granted to the data users determined by the conditions of the issued data permit". Furthermore, arrangements of joint controllership under the article 26 GDPR shall be established with the aim of boosting inclusive and sustainable framework for multi-country secondary use through research infrastructures ensuring legal certainty and interoperability in the re-use processing.

The proposal then identifies a national competence for the ethical assessment to comply with. In this regard, Member States may introduce different obligations for the ethics assessment, including the submission of a self-assessment, or an approval from an independent ethics committee, or an authorization from the competent authority. This may constitute a barrier for accelerating the constitution of cross-border health data spaces as the ethical-legal compliance at national and local levels is fragmented[13]. For example, in France a prior approval from the competent ethical committee and then an authorisation from the data protection authority is required. In fact, according to the article 1462-1 of the Public Health Code a Health Data Hub has been already established and the national authority – the CNIL - has already authorised some projects to be carried out on the technological platform. In particular, each project shall receive an opinion from a committee for the protection of persons (CPP) mentioned in article L. 1123-6 of the Public Health Code for research involving the human person or from the ethics and scientific committee for research, studies and assessments in the field of health (CESREES), for research not involving the human person. Once obtained the approval from the competent ethics committee, the CNIL shall verify the compliance of the data management plan with the GDPR and the national data protection legislation, including legal and technical

[13] See D. Amram, Building up the "Accountable Ulysses" model. The impact of GDPR and national implementations, ethics, and health-data research: Comparative remarks, Computer Law & Security Review, Volume 37, 2020, 105413, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2020.105413.

ISSN 2281-5147

standards recommended in its opinions on the Health Data Hub. The Finnish Findata space has been approved by the Act on the Secondary Use of Health and Social Data n. 552/2019 that specifies that reuse of data stored in the platform can be asked for the purposes of statistics, scientific research, development and innovation activities, teaching, information management, social and healthcare authority guidance and supervision, planning and investigation tasks of the authority. Access to the platform is subject to an authorisation from the Social and Health Information Authorization Authority that operates in connection with the Institute of Health and Welfare, unless the requested data are generated through clinical trials. In fact, in this case another authority is competent to issue permits, so-called Fimea. Other exceptions are illustrated in the Finnish act and summarised by the Findata terms and conditions as well. To the purposes of this essay, it is significant to address that not harmonised and centralised procedures to requests data from the health data space could limit its effective use at local, national, but especially at international level. The German Forshungsdatenzentren is committed to statistics analysis and includes two research data centers the one of the Statistical Offices of the Federation and the one of the Federal States. Access request includes a specific commitment on statistical confidentiality but no reference to specific ethics assessments seems to be required. This simplified procedure could be justified by the nature of data that are classified in the platform as absolute anonymised (those data that are modified "by coarsening or by removing individual variables to a degree that makes an identification of the respondents impossible"), that are available to both individuals and organisations, and factual anonymised ("if de-anonymisation cannot be ruled out completely but the allocation of data to the respective statistical unit is only possible with an unreasonable effort in terms of time, cost and manpower"), that are available only to scientific institutions for research purposes[14]. The two notions aim to distinguish between "sufficiently anonymous" data and pseudonymised data according to the recital 26

[14] R. Becker, D. Chokoshvili, G. Comandé, E.S. Dove, A. Hall, C. Mitchell, F. Molnár-Gábor, é-Nicolàs, S. Tervo, A. Thorogood, Secondary Use of Personal Health Data: When Is It "Further Processing" Under the GDPR, and What Are the Implications for Data Controllers?, European Journal of Health Law, 2022, doi: 10.1163/15718093-bja10094.

ISSN 2281-5147

GDPR. However, once that the EHDS proposal will enter into force, efforts for language alignment would be mandatory.

According to the mentioned experience of data spaces, it is reasonable to affirm the necessity to identify common paths of demonstrating a responsible and accountable approach towards the ethical-legal compliance also in light of the new EU framework and the room of application left to the national implementation. This is particularly relevant to avoid phenomena of forum shopping in the future, ensuring that the reuse of electronic health data would be permitted following simplified and harmonised procedure of ethical legal compliance, especially taking into account the increasing number of cross-border research infrastructure that are going to be implemented under the global and national data strategies.

3.2 Risk based approach for larger online platforms in the DSA.

As anticipated, the risk-based approach drives also the Digital Service Act implementation, even if with a different normative technique, consisting of introducing "asymmetric due diligence obligations" for larger online platforms, that are, according to parameters described by article 26, the ones with more than 45 million recipients each month.

In particular, in order to mitigate the risk of sharing illicit online contents, the DSA establishes obligations to conduct risk assessments on "any significant systemic risks stemming from the functioning and use made of their services in the Union" (Article 26). The grounds of analysis include the general risks of disseminating illicit content, risks to compromise fundamental rights, that are further specified as privacy and confidentiality protection in terms of private and family life rights; freedom of expression and information, especially against fake news but also in terms of ensuring equal access to online resources and contents, without discrimination; and, last but

ISSN 2281-5147

not least, to protect the rights of the child, considered as *per se* vulnerable users[15]. Another ground of risk analysis consists of intentional manipulation that could affect democratic values and groups interests like public health and security, minors, civic discourse, elections[16].

The assessment shall be continuous and addressed on developing tailored content moderation systems, recommender ones also for advertisement able to rapidly detect and avoid dissemination of illegal content, namely in contrast with fundamental rights and terms and conditions adopted by the platform. To this end, a series of measures are suggested by Article 27, including technical and organisational ones aiming to reinforce and adapt decision-making processes for content moderation and recommender systems to identify, detect, and block illicit contents. Therefore, duties of supervision, cooperation with other platforms, reporting measures are explicitly identified to develop common methodologies to be included in codes of conducts for digital service providers.

In fact, large online platforms have specific obligations of due diligence, but such an imposition shall be considered as an opportunity to develop standards of compliance in order to inspire also medium and small enterprises to adapt their systems, procedure, and compliance activities in alignment with them for a safer online environment[17].

As illustrated, there are several grounds of assessment that may require different expertise from an ethical-legal viewpoint and specific skills in cybersecurity and programming both for detecting, reporting, blocking and replacing harmful content. To develop and share common methodologies as well as best practice could

[15] M. Stoilova, S. Livingstone, R. Nandagir Digital by default: children's capacity to understand and manage online data and privacy. Media Commun, 2020, 8(4):197–207.

[16] G. Caggiano, G. Contaldi, P. Manzini (eds), Verso una legislazione europea su mercati e servizi digitali, Cacucci editore, 2021.

[17] G. Resta, Digital platforms and the law: contested issues, MediaLaws–Rivista di diritto dei media, 2018, 1:231–242.

ISSN 2281-5147

harmonise standards of accountability and reduce costs for compliance. This process of harmonisation could start from collecting practices in the context of the external and independent auditing procedure that are mandatory at least once a year under Article 28. Thus, an assessment to extract the most effective solutions could be undertaken to develop codes of ethics and conduct in order to ensure a wider implementation.

In particular, considering the variety of the profiles to be analysed an interplay of different checklists, recommendations, and guidelines[18] could be tested for the purposes of the DSA ethical-legal compliance. In particular, we could verify which ones of the existing tools could be applied in this context.

Firstly, as known, the Assessment List on Trustworthy Artificial Intelligence (ALTAI) elaborated by the High-Level Group on Artificial Intelligence has identified seven requirements to assess a solution based on AI in terms of ethics, lawfulness, and robustness. They could be useful, with some adaptations, to address the level of safety of digital platforms, for example:

i) Human agency and oversight could be developed into sections aiming to identify general safeguards to protect the freedoms of expression, association, and tailored ones to specifically empower users-consumers rights as well as vulnerable ones, like children. In this regard, the service providers could list which technical and organisational measures are implemented not only to protect users from illicit content dissemination and diffusion, but also to empower their fundamental rights in the digital environment.

In particular, it could be useful to list which safeguards are implemented to collect, store, and allow the withdrawal of consent(s) for the different services according to the maturity and age of users. Moreover, a section for each risk identified by article 26 DSA shall be introduced to assess its grade of occurrence and severity in the given

[18] A. Mantelero, Human Rights Impact Assessment and AI. in Beyond Data. Information Technology and Law Series, vol 36. T.M.C. Asser Press, The Hague, 2022, https://doi.org/10.1007/978-94-6265-531-7_2.

ISSN 2281-5147

platform, establishing - as a consequence - proper measures to be implemented for the three possible activities, namely the content moderation (e.g. how illicit content is detected, how content moderation is addressed, how to guarantee the free expression of users, which are the countermeasures in case of illicit content, how equal access to services is granted, how users can report their complaints etc), as well as the functions of the recommender systems (that are the ones suggesting in the online interface specific information to recipients of the service), and advertising ones.

ii) Technical robustness and safety shall include an assessment on the cybersecurity aspects of the platform and the level of accomplishment with existing standards, for example taking into account the evolution of the state of the art by ENISA[19].

iii) Privacy and data governance, including the GDPR compliance according to the data protection impact assessment article 35 GDPR.

iv) Transparency section can be used for analysing the lawfulness of users profiling activities in order to avoid manipulative advertising content, like the so-called "dark patterns"[20]. The DSA, indeed, considers illicit manipulative content. According to article 24, therefore, each specific advertisement displayed shall be user-friendly in terms of being clear and unambiguous manner identified as an advertisement in the interest of a given natural or legal person with "meaningful information about the main parameters used to determine the recipient". In addition, pursuant to Recital 63 public access to repositories of advertisements displayed in the platforms shall be ensured to both facilitate supervision and protect platforms' content integrity. From this perspective, this section of the checklist could be articulated in order to assess platforms' a) Terms and Conditions respect to users (according to Recital 47);

[19] See the reinforced role of ENISA under the NIS Directive, and the dedicated web-page: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/nis-visualtool.

[20] J. Luguri, L. Jacob Strahilevitz, Shining a Light on Dark Patterns, *Journal of Legal Analysis*, Volume 13, Issue 1, 2021, pp. 43–109, https://doi.org/10.1093/jla/laaa006.

ISSN 2281-5147

b) risks emerging during the activities of content moderation (according to Recital 39); c) compliance with specific additional safeguards required for the nature of service provided, including reporting procedure under articles 13 and 23, Recitals 51 and 65.

v) Diversity, non-discrimination and fairness section could replicate the analysis under the ALTAI checklist. However, it is important to extend the concept of fairness in terms of commercial one respect to users-consumers and competitors (B2B). In fact, on the one hand it should be the opportunity to demonstrate the compliance with competition law as well as with the measures aiming to balance the increasing contractual asymmetry in the B2C relationships, determined for example by the digital divide or by unfair profiling activities. Among B2B and B2G relationships, the analysis could be associated to the Digital Market Act obligations as well.

vi) Societal and environmental wellbeing section is the one that could be used to address the risks on democratic values, considering the risks and opportunities emerging in the digital dimension. Therefore, the adaptation of the ground of analysis could be translated into a formula related to "societal and digital wellbeing", stressing that the objective of the assessment is to develop and maintain a safe digital environment. Cross references with section *sub* i) could be developed in order to facilitate the analysis.

vii) Accountability could be maintained as the section to report all the initiatives aiming to detect, mitigate and monitor risks, including the compliance with the auditing obligations under article 28.

The described proposal of requirements to be addressed in compliance checklists could be further adapted to specific needs emerging for specific online services, taking into account, for example, the public or private nature of the provider, the state of the art of the safety standards, and the targeted group(s) of the platform users. The efforts developed for AI-based solution assessment could certainly constitute a starting point towards a more harmonised approach to deal with the compliance activities defined in the new DSA as well.

ISSN 2281-5147

4. Codes of Conducts and standards of compliance

To better address the ethical-legal compliance, the EU Commission promotes the adoption of self-regulatory tools from those organisations that are sharing the same means/purposes of data processing/target groups in order to enable the development of tailored and appropriate safeguards to mitigate common risks. Such a bottom-up approach is justified since all the compliance activities are based on the perception of impacts that a given (personal or non-personal data) processing could have on fundamental rights protection, as well as on the case-by-case identification and implementation of mitigating measures considered as appropriate as effective for the given circumstances.

Thus, to draw up common paths of risk detection and mitigation among stakeholders could help the standardisation process and at the same time it could facilitate the adoption of already designed compliant methodologies, including complementary commitments that can increase the level of accountability, also for those organisations who have not started a conformity plan yet, ensuring monitoring mechanisms to maintain the highest adherence. From this perspective, organisational efforts could be limited to adapt the modalities of implementation of the mechanisms of compliance that have been agreed in the context, for example, of a Code of Conducts.

Currently, the EU Commission has assessed a series of Codes of Conducts aiming to identify convergences in dealing with specific issues. In 2016, for example, a Code of Conduct on countering illegal hate speech online was signed by Commission and Google (YouTube), Facebook, Twitter and Microsoft[21], other companies joined in the following years. It establishes how to report, assess, and remove illicit content, including delays for detecting and replacing content, providing information and

[21]https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination-0/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en.

ISSN 2281-5147

feedback to end-users[22]. In 2021, the European CRO Federation's GDPR Code of Conduct for Service Providers in Clinical Research has been submitted to create a transnational GDPR Code of Conduct for data processors working in the clinical research industry, under the supervision of the French CNIL.

Under the legal framework illustrated in this paper, Codes of conducts are promoted both under article 40 GDPR, and pursuant article 6 to boost data portability within the Free-Flow Regulation, and to strengthen the due diligence activities according to articles 45, 46, 47 DSA.

In particular, the DSA encourages the development of codes of conducts for minors as end-users in order to establish "appropriate and proportionate" measures for their protection (Recital 71) as well as to "support and complement the transparency obligations relating to advertising for providers of online platforms, of very large online platforms and of very large online search engines (…) to provide for flexible and effective mechanisms to facilitate and enhance the compliance" (Recital 107), in order to deal with "the specific challenges of tackling different types of illegal content and systemic risks" (article 45). It also regulates Codes of Conducts dealing with specific matters like the online advertising (article 46) and accessibility (article 47).

The purpose is to make participation and commitment of companies effective. Therefore, mechanisms of internal monitoring shall be introduced and undertaken by the EU Commission and the established European Board for Digital Services. These may include according to the identified objectives, reports on the achieved key performance indicators and auditing to verify the concrete adherence. In fact, proper actions shall be taken in case of default. In this regard, the involvement of stakeholders (from citizens to associations to independent authorities) in the draft and

[22] K. Podstawa, Hybrid Governance or. . . Nothing? The EU Code of Conduct on Combating Illegal Hate Speech Online, in E. Carpanelli, N. Lazzerini (eds.), Use and Misuse of New Technologies, Cham, 2019, p. 167 ff.

ISSN 2281-5147

assessment of the Codes are essential to develop protocols able to satisfy concrete tailored needs of compliance[23].

Articles 46 and 47 identify the specific objectives for the codes of conducts on online advertising, that shall address how to comply with article 26 and 39, including to ensure transparency in the information on data monetisation. The accessibility one instead shall ensure the inclusiveness in the digital environment taking into account specific vulnerabilities, like possible disabilities that could increase the asymmetry of the position of the user[24].

Other self-regulatory mechanisms are encouraged as well. In particular, the DSA regulates the adoption of crisis protocols to manage those situations affecting public security or public health. In parallel to data breach policies addressed in the GDPR, aiming to manage the violations in terms of availability, integrity, confidentiality of data flows, the crisis protocols are encouraged in order to pre-establish procedure to "to coordinate a rapid, collective and cross-border response in the online environment" determined for example by the misuse of the online platforms "for the rapid spread of illegal content or disinformation or where the need arises for rapid dissemination of reliable information" (Recital 108), by enabling response mechanisms under article 36, including the allocation of obligations of publishing information and contacts for crisis management.

As far as the European Health Data Spaces are concerned, a chapter of the proposal refers to the mechanisms of certification of the Electronic Health Records systems, setting common requirements of safety and interoperability in alignment with the CE marking requirements, registration, and conformity obligations.

---

[23] R. Thorburn, F. Paci, V. Sassone and S. Stalla-Bourdillon, Connecting Regulatory Requirements to Audit Outcomes: A Model-driven Approach to Auditable Compliance, ACM/IEEE International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C), 2021, pp. 641-642, doi: 10.1109/MODELS-C53483.2021.00100.

[24] U. Sury, Digital Services Act (DSA). Informatik Spektrum 45, 265–266 (2022). https://doi.org/10.1007/s00287-022-01464-1.

ISSN 2281-5147

Certification mechanisms, codes of conducts, and public protocols are tools aiming to make public the level of conformity that the given company declares respect to general and tailored standards. This would increase the user / data subject awareness and would create competitiveness between companies on the ethical-legal matter ground. The adoption of voluntary monitoring systems, in fact, will increase the trustworthiness and awareness among users towards the "sealed" solution, contributing therefore to develop a cultural process where accountability, fairness, and transparency play a fundamental role in the B2C, B2B, and B2G relationships[25].

5. Towards an effective implementation of the EU Data Strategy between compliance and standardization through accountability, transparency, and fairness principles.

In the previous paragraphs, we illustrated the EU Data Strategy, classifying the legislative initiatives considering the ones aiming to achieve general purposes and the sectorial ones impacting on specific categories of data and data processing.

We identified the main interpretative paths to boost the data-driven economy and innovation balancing the fundamental rights protection and empowerment of individuals and groups with the potentialities of data analysis, sharing, and exploitation. To this end, we illustrated how the notions and definitions included in the normative texts are functional to identify roles and responsibilities in order to allocate duties and obligations, especially the ones to assess the impacts of a given data processing activity to implement mitigation measures and safeguards.

We compared two different and apparently far sectors of application like the health data space regulation and the digital service act in order to highlight the relevance of

[25] G. Amore, Fairness, Transparency e Accountability nella protezione dei dati personali, Studium Iuris, 2020, 4:414–429.

ISSN 2281-5147

developing harmonised mechanisms of compliance starting from the risks assessments.

From our analysis, we may highlight some common principles that could drive further interpretations and implementation strategies even in other sectors than the described ones.

First of all, the principle of accountability that is paramount for the risk-based approach adopted by all the illustrated initiatives. In fact, despite of the nature, those who enable a data processing shall demonstrate to have assessed any possible impacts of their activity against fundamental rights of data subjects / users as well as to have introduced proper measures to mitigate either the occurrence or the severity of possible risks. If, despite the efforts, any harm occurs, an accountable approach could limit consequences against the victims and the sanctions by the competent authority. However, the main characteristic of the accountability is to contribute to a cultural change aiming to include, not only in the annual budget, the ethical-legal dimension in the design process of a digital/technological solution.

This element is particularly significant in terms of standards identification and harmonisation of procedure. In fact, if technical development is a global phenomenon completely interoperable despite of the frame of reference, the legal evolution is not easy to be adapted at national and local level, especially in a domain – like the ethical legal one – where strategies to achieve rights protections and empowerments are sophisticated and truly connected to the shared values at a given moment. To this end, the legal interoperability that could concretely realise common safe environment where to share data and boost innovation needs to be built up step by step through case-by-case and sectorial compliance to general principles as well as to specific provisions and standards.

Other two principles play a fundamental role in the harmonisation of the implementation of the EU data strategy: transparency and fairness, that together with the accountability rule could address all the interpretative issues emerging from the different interplay of the complex data regulatory framework.

ISSN 2281-5147

Transparency[26] embeds legal and technical standards related to both the solution design and the information duties towards data subjects/users. Clear and public procedure can be included in reports made available both on digital platforms and on the health data repositories. This organisational measure is essential to understand how to identify in a transparent manner roles and responsibilities during the all life-cycle of the processing. Transparency is therefore also related to the concept of maintaining the control of the governance of processed data by technical measures (eg traceability) and organisational ones (eg activity reports, records of data processing, terms and conditions to get access to data/services, etc.). It shall be clear – or at least easily to reconstruct - who has which rights on a given (raw / processed) dataset.

Fairness[27] is a principle that finds application both in B2C and B2B relationships. It helps to cover the concept of accountability with meaningful content: to demonstrate to be compliant with the ethical-legal framework is not only a formal obligation to avoid sanctions but a relevant part of the solution development and deployment. To enable fair data processing is in fact a guarantee for the fundamental rights of the involved individuals and groups and it also ensures the robustness of the democratic architecture of values in the digital environment and the maintenance of competitiveness in the relevant market.

---

[26] G. Finocchiaro, Transparency of Digital Providers and Digital Divide, in R. Senigaglia, C. Irti, A. Bernes (eds) Privacy and Data Protection in Software Services, Springer, 2021, p. 3 ff.

[27] G. Malgieri, The Concept of Fairness in the GDPR – A Linguistic and Contextual Interpretation, FAT* '20: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency January 2020 (2020) 154–66, https:// dl.acm.org/doi/pdf/10.1145/3351095.3372868; G. Schneider, Fairness, in G. Comandé (ed), Elgar Encyclopedia of Law and Data Science, cit., p. 168; H. Hoffmann, V. Vogt, M. P. Hauer, K. Zweig, Fairness by awareness? On the inclusion of protected features in algorithmic decisions, Computer Law and Security Review, Volume 44, 2022, 105658, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2022.105658.

ISSN 2281-5147

The interplay between accountability, transparency, and fairness, therefore, seems to be the interpretative key for harmonising the different legislative initiatives on data, as well as to solve applicative issues and standardise procedure.

ISSN 2281-5147