

Towards a Digital Ecosystem of Trust: Ethical, Legal and Societal Implications

Jeroen van de Hoven, Giovanni Comandè, Salvatore Ruggieri, Josep Domingo-Ferrer, Francesca Musiani, Fosca Giannotti, Francesca Pratesi, Marc Stauch

▶ **To cite this version:**

Jeroen van de Hoven, Giovanni Comandè, Salvatore Ruggieri, Josep Domingo-Ferrer, Francesca Musiani, et al.. Towards a Digital Ecosystem of Trust: Ethical, Legal and Societal Implications. Opinio Juris In Comparatione, 2021, pp.131-156. halshs-03510761

HAL Id: halshs-03510761

https://halshs.archives-ouvertes.fr/halshs-03510761

Submitted on 4 Jan 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution| 4.0 International License

ISSN 2281-5147

OPINIO JURIS inComparatione

Studies in Comparative and National Law

Vol. 1, n. 1/2021

Towards a Digital Ecosystem of Trust: Ethical, Legal and Societal Implications

Jeroen van den Hoven,

Giovanni Comandé,

Salvatore Ruggieri,

Josep Domingo-Ferrer,

Francesca Musiani, Fosca Giannotti and Francesca Pratesi,

Marc Stauch and Iryna Lishchuk

Pacini Giuridica

Online First ISSN 2281-5147

Towards a Digital Ecosystem of Trust: Ethical, Legal and Societal Implications

Jeroen van den Hoven,[i] Giovanni Comandé,[ii] Salvatore Ruggieri,[iii] Josep Domingo-Ferrer,[iv] Francesca Musiani,[v] Fosca Giannotti and Francesca Pratesi,[vi] Marc Stauch and Iryna Lishchuk.[vii]

Abstract

The European vision of a digital ecosystem of trust rests on innovation, powerful technological solutions, a comprehensive regulatory framework and respect for the core values and principles of ethics. Innovation in the digital domain strongly relies on data, as has become obvious during the current pandemic. Successful data science, especially where health data are concerned, necessitates establishing a framework where data subjects can feel safe to share their data. In this paper, methods for facilitating data sharing, privacy-preserving technologies, decentralization, data altruism, as well as the interplay between the Data Governance Act and the GDPR, are presented and discussed by reference to use cases from the largest pan-European social science data research project, SoBigData++. In doing so, we argue that

[i] Delft University of Technology.

[ii] Scuola Superiore Sant'Anna di Pisa.

[iii] Università di Pisa.

[iv] Universitat Rovira i Virgili.

[v] Centre national de la recherche scientifique.

[vi] Institute of Information Science and Technologies (ISTI), National Research Council of Italy (CNR).

[vii] Gottfried Wilhelm Leibniz Universität Hannover.

Online First ISSN 2281-5147

innovation can be turned into *responsible* innovation and Europe can make its ethics work in digital practice.

Table of Contents

Abstract 131

Keywords 132

1. Introduction 133

2. New privacy-respecting technologies 135

2.1 Ethics-integrating approaches proposed by the SoBigData++ project 138

3. Data Sovereignty and data altruism fostered by the DGA 143

3.1. From data monopolies to data commons 144

3.2 Decentralized architectures and self-sovereign identities 146

3.3 Sovereignty on a geo-political level 148

4. Interplay between the DGA and the GDPR 150

4.1 General interconnection points 151

4.2 Truly enabling personal data altruism 152

4.3 Secondary use of health data for research – a legal perspective 153

5. Conclusion and steps forward 155

Acknowledgment: This work was supported by the European Commission through the H2020-INFRAIA-2018-2020 / H2020-INFRAIA-2019-1 European project "SoBigData++: European Integrated Infrastructure for Social Mining and Big Data Analytics" (Grant Agreement 871042). The funders had no role in developing the research and writing the manuscript. 156

Keywords

Online First ISSN 2281-5147

Digital ecosystem of trust – responsible data science – data altruism – decentralization.

1. Introduction

Europe has developed ambitious plans for its digital leadership in the remainder of the 21th century. With the 2016 EU 'General Data Protection Regulation' (GDPR) and new plans for a Data Governance Act (DGA) and new Regulation for Artificial Intelligence (AI Regulation), the European Union hopes to set global standards for the Digital Age on the basis of its law. The EU has introduced the new model of trustworthy digital environment in an attempt to create an adequate alternative to the existing developments, characterized by a data-centric approach, exclusive IP schemes and data commercialization practiced by large technological companies. The DGA, meant as a centerpiece to the European data sharing framework, promises to foster the availability of data for use, but also promote trust in data intermediaries, technology and strengthening data-sharing mechanisms across the EU. A trustworthy environment requires instruments able to ensure that data from the public sector, industry and citizens is available for use in the most effective and responsible manner, while citizens retain a reasonable degree of control over the processing of data they generate, and businesses can rely on adequate protection of their investments in data economy.[1] The EU has rightly foregrounded ethical principles and fundamental rights, since they are enshrined in its constitutive and binding treaties. On this basis, it aims at building a European digital ecosystem of trust and excellence that will allow the EU to make the best possible use of the potential of Digital Innovations to help solve grand societal challenges. There is however a recurrent concern in Europe itself and a point of surprise, or even disbelief, outside Europe: how can one prosper in a digital economy, how can one lead digital innovation and spearhead data-driven research and AI development while being firmly committed to the highest ethical standards, especially when others are not.

This paper seeks solutions to this challenge. In doing so, it draws upon the findings, results and experience in the SoBigData++ research environment, comprising over

[1] DGA, Explanatory Memorandum.

thirty research institutions, spread across thirteen countries, united by the goal of establishing a pan-European research infrastructure (RI) for social science big data. An important part of the response to the above concern has to do with the fact that this approach fosters trust and augments the quality of relevant institutions. Trust and the quality of institutions are a key determinant in the success of nations[2] and therefore a key to successful digital societies. Trust is at the same time an elusive moral concept. With regard to trust in the context of state power, law and trust cannot be separated and both serve as mechanisms to reduce complexity and risk.[3] Trust implies the belief that the trusted are well-intentioned and are taking a moral view. Like friendship, trust cannot be produced at will and those who set out to 'manage' our trust in relations may find their attempts to be counterproductive. Trust usually does not appear in one's Excel sheets, but when there is no trust, the costs associated with (re-)establishing it become evident. Trust in the digital economy requires infrastructures, institutions, mechanisms and habits to be in place that allow people to receive reliable signals of the moral quality of intentions and plans of others, so that they can determine whether trust or distrust is the appropriate attitude in their interactions. All the above requires a continuous nurturing of awareness about the issues for which trust is needed and embedding this in the culture of organizations.

We define a digital ecosystem of trust as a system of interacting organisms and their environment,[4] in which appropriate norms are clear to parties, and responsibilities are well defined and adequately and fairly allocated to actors and agents. Trust needs to be horizontal between citizens and parties and also vertical between citizens and governments. The SoBigData++ project provides examples of designing for trust in big data ecosystems by furthering (i) data altruism and generosity, (ii) practices of responsible data science, (iii) responsible innovations for privacy-respecting technologies, (iv) research integrity review boards in AI and data-driven research, (v) adequate governance schemes. In this way, both primary and

[2] D. Acemoglu, J. A. Robinson, *Why Nations Fail* (Profile Books 2012).

[3] N. Luhmann, *Trust and Power* (John Wiley and Sons 1979).

[4] The Oxford English Dictionary (Oxford University Press 2003, 5th ed).

secondary use of data can be responsibly geared towards big data and data analytics for the general good of all.

The core aim of this paper is to discuss Europe's plans to profile itself as promoter of ethics and values with the aim to create a digital ecosystem of trust where, on the one hand, people feel safe to share their data and, data science and analytics (either primary or secondary) are conducted with due respect for the subjects' rights while on the other hand the digital functionality can be deployed when and where it can be deployed productively to solve our problems. This is connected to the central questions: *What conditions need to be fulfilled for people to trust an ecosystem in which they would feel safe to share their data? How may one build an appropriate research infrastructure for data science - a prototype of an ecosystem of trust?*

In principle, trust in digital ecosystems is formed from a variety of aspects, not only of legal or technical nature, but also addressing data governance, such as who uses the technology and how the technology is used. Each instrument may reveal benefits and disadvantages depending on the perspective of the actor: citizens, governments, science or businesses. Each solution can be supported by diverse arguments. This paper does not offer an objective analysis of suggested solutions, rather it presents a broad overview of many aspects related to trust in digital ecosystems. The instruments introduced by the European legislative initiatives are tested in their efficiency to counteract the tendencies of centralization and exclusive IP arrangements. The work is based on technical legal and normative analysis.

In order to address this central question in an innovative way, the paper adopts the following structure. Next, we look at privacy-preserving technologies in their pros and contras with respect to data control (Section 2), supplemented with use cases from the SoBigData++ project. We continue with novelties of data sovereignty, data altruism, decentralization and data intermediaries introduced by the Data Governance Act (DGA) (Section 3). This is followed by a consideration of the interplay between the DGA and the GDPR, as well as the GDPR's intricacies for research (Section 4). The paper then concludes by considering some desirable steps for the future (Section 5).

2. New privacy-respecting technologies

Online First ISSN 2281-5147

It is sometimes argued that Europe's strong regulations on privacy hamper the scientific and economic progress that could ensue from massive data collection and processing.[5] While eliminating all barriers would no doubt facilitate progress in certain directions, the issue deserves more careful consideration.

On the one hand, unlimited collection and processing of personal data conflicts with fundamental rights and ethical values such as privacy, autonomy, fairness and security.[6] On the other hand, the need to reconcile progress with the aforementioned rights and values spurs technology research, innovation and development.[7]

Privacy-preserving technologies are the workhorse that enforces the protection of digital assets, whether they are personal or corporate.[8] In particular, such technologies are instrumental to implement privacy and data protection by design. Due to its legal framework and its expertise in information technologies, Europe is very well placed to take the lead in innovation on privacy-preserving technologies and establish a common understanding of digital society notions across disciplines.[9] We next sketch directions that hold promise.

Right now, a very common setting in privacy preservation is to rely on trusted third parties (certification authorities, data controllers that take care of anonymizing or encrypting data, etc.). The trend of future information technologies is to follow the

---

[5] R. Eiss 'Confusion over Europe's data-protection law is stalling scientific progress' (2020) Nature 484; contra, see G. Schneider, G. Comandè 'Differential Data Protection Regimes in Data-driven Research: Why the GDPR is More Research-friendly Than You Think' (2021, forthcoming) German Law Journal.

[6] J. Domingo-Ferrer, A. Blanco-Justicia 'Ethical value-centric cybersecurity: a methodology based on a value graph' (2020) 26 3 Science and Engineering Ethics 1267.

[7] G Schneider, G Comandè, 'Can the GDPR Make Data Flow for Research Easier? Yes it Can! By Differentiating!', (2021) 41 Computer Law & Security Review 105539.

[8] G Danezis, J Domingo-Ferrer, M Hansen, J. H. Hoepman, D. Le Métayer, R. Tirtea, S. Schiffner, 'Privacy and Data Protection by Design – from Policy to Engineering' (2015) European Union Agency for Network and Information Security (ENISA).

[9] G. Comandé (ed.), *Elgar Encyclopedia of Law and Data Science* (Edward Elgar 2022).

ethics-by-design approach, which inherently reduces the need for trust by empowering individual users. This is substantiated by the following design principles:

- *Decentralization*. Most individuals currently have powerful personal computing devices (smartphones, tablets, etc.). Hence, it is possible for them to carry out a fair amount of computation. This has resulted in new paradigms for decentralized machine learning (federated learning,[10] fully decentralized learning,[11] etc.), for decentralized, local anonymization,[12] for decentralized COVID-19 contact tracing, etc.

- *Incentivization*. Decentralized computing relies on the willingness of individual participants to play their respective roles as specified in the computation protocols. But this cannot be taken for granted. Without proper incentives, a rational participant might be better off by not joining the protocol, or by deviating from it, free-riding it or dropping it. The poor uptake of COVID-19 contact tracing apps in spite of most of them being privacy-preserving is a recent example of what can happen when incentives are lacking:[13] people do not feel very motivated to install and run an app that can only give them negative (and maybe false) news. Offering additional services might be a better way to follow.[14]

---

[10] H. B. McMahan, E. Moore, D. Ramage, D. Hampson, B. Aguëra 'Communication-efficient learning of deep networks from decentralized data' (2017) Proc. of the 20th Intl. Conf. on Artificial Intelligence and Statistics – AISTATS'2017 1273.

[11] A. Koloskova, S. Stich, M. Jaggi 'Decentralized stochastic optimization and gossip algorithms with compressed communication' (2019) Proc. Of the 36rd International Conference on Machine Learning – ICML 2019 3478.

[12] J Domingo-Ferrer, J Soria-Comas 'Multi-dimensional randomized response' (2021, forthcoming) *IEEE Transactions on Knowledge and Data Engineering*.

[13] S. Toussaert 'Upping uptake of COVID contact tracing apps' (2021) 5 Nature Human Behaviour 183.

[14] M. Nanni, G. Andrienko, AL. Barabási, et al. 'Give more data, awareness and control to individual citizens, and they will help COVID-19 containment' (2021) Ethics Inf Technol.

In behavioral economics, it has long been known that moral behavior can be encouraged and incentivized.[15] In decentralized computing, the co-utility approach[16] follows this idea by designing protocols in such a way that adhering to them is the best option for all participants: in game-theoretic terms, following a co-utile protocol as specified is an equilibrium for all participants.

Crafting decentralized, co-utile protocols allows embedding not only privacy preservation, but virtually any ethical values by design. This is open ground for European academia and industry to conquer and cultivate. If this opportunity is properly seized, an "*IT made in Europe*" seal might become synonymous with ethics-compliant technology. Ethics by design, as discussed in the AI Regulation, should signal that the development and use of technology (in particular AI) are guided by certain essential value-oriented principles. The core principles of data protection are embedded into technology by virtue of data protection by design (Article 25 GDPR). Alike, transparency and protection against unfair commercial practices may find reflection in ethics-oriented technology (as envisaged by the AI Regulation). Software can be viewed as set of rules whereby machines act. And these rules can embed ethical principles. For example, as follows from the literature on anti-discrimination: artificial intelligence can be trained with more or less biases. A downside is that amid the flourishing field of data analytics, the implementation of the said principles on the level of the law may encounter opposition from the data industry. However, beyond a pay-off in moral and legal terms, this could also give a new purpose and competitive strength to the European IT industry.

2.1 Ethics-integrating approaches proposed by the SoBigData++ project

The focal point of this paper is on building trust, mainly focusing on privacy, data protection, and data management. We will briefly review the various solutions, which are currently in different progress statuses, i.e., in the developing phase or near to

[15] B. S. Frey, F. Oberholzer-Gee 'The cost of price incentives: an empirical analysis of motivation crowding-out' (1997) 87 4 The American Economic Review 746.

[16] J. Domingo-Ferrer, A. Blanco-Justicia, D. Sánchez, N. Jebreel 'Co-utile peer-to-peer decentralized computing' (2020) 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing – CCGrid 31.

being published in the SoBigData++ Catalogue. A detailed study on these topics will be provided in the following White Papers.

Firstly, an analytical platform cannot be considered ethical without non-discrimination guarantees. Indeed, AI models can amplify existing biases coded in data or introduce new forms of bias,[17] resulting in discriminatory or unfair decisions. Approaches to tackle the problem of algorithmic fairness have been proposed within different fields. In the SoBigData++ consortium, we rely on auditing AI-based systems for discrimination discovery[18], through published libraries such as "dd: a Java library for discrimination discovery and sanitization". The final desirable objective is to embed the fairness value in the design of AI models (fairness-by-design).

A second, essential aspect to be tackled concerns the use of social media and social media analysis. Here, the issues of misinformation, fake news, and polarization have become more and more central. In SoBigData++, we dealt with the problems of bot detection,[19] useful to detect automatically a new generation of increasingly technologically advanced spambots, and polarization and echo chambers,[20] which drive debates and increase discords and conflicts. A possible countermeasure to these

[17] A. Olteanu, C. Castillo, F. Diaz, E. Kiciman 'Social Data: Biases, Methodological Pitfalls, and Ethical Boundaries' (2019) Frontiers Big Data 2.

[18] A. Romei, S. Ruggieri 'A multidisciplinary survey on discrimination analysis' (2014) 29 5 Knowledge Eng Review 582; S. Ruggieri 'Using t-closeness anonymity to control for non-discrimination' (2014) 7 2 Transactions on Data Privacy 99.

[19] S. Cresci, R. Di Pietro, M. Petrocchi, A. Spognardi, M. Tesconi 'The paradigm-shift of social spambots: Evidence, theories, and tools for the arms race' (2017) Proceedings of the 26th international conference on world wide web companion; S. Cresci, R. Di Pietro, M. Petrocchi,A. Spognardi, M. Tesconi 'DNA-inspired online behavioral modeling and its application to spambot detection' (2016) 5 31 IEEE Intelligent Systems 58.

[20] V Morini, L. Pollacci, G. Rossetti 'Toward a Standard Approach for Echo Chamber Detection: Reddit Case Study' (2021) 11 12 Applied Sciences 5390; V. Morini, L. Pollacci, G. Rossetti 'Capturing political polarization of Reddit submissions in the Trump Era' (2020) 28th Symposium on Advanced Database Systems; A. Sîrbu, D. Pedreschi, F. Giannotti, J. Kertész 'Algorithmic bias amplifies opinion fragmentation and polarization: A bounded confidence model' (2019) 14 3 PloS one.

problems is to deeply analyze the phenomena of misinformation and disinformation[21] and understand diffusion mechanisms over complex networks.[22]

Finally, another ethical dimension is explainability, which is useful at the development level since it permits to understand and possibly discover undesired behavior within the reasoning of AI methods. Even if full transparency and interpretability are the most powerful solutions,[23] they can also be challenging to reach. Thus, we believe that also meaningful explanations of black-box decision systems can be useful in many cases.[24] These explanations can be related to the whole AI model or to specific instances, and also the kinds of the given explanations depend on several variables, such as the kind of data, the context, and the person to whom the explanation is delivered.[25] A collection of explainability methods will be provided within the SoBigData++ Catalogue.[26]

---

[21] K. Bontcheva, J. Posetti, D. Teyssou, T. Meyer, S. Gregory, C. Hanot, D. Maynard 'Balancing act: Countering digital disinformation while respecting freedom of expression' (2020) United Nations Educational, Scientific and Cultural Organization; X. Song, J. Petrak, Y. Jiang, I. Singh, D. Maynard, K. Bontcheva 'Classification aware neural topic model for COVID-19 disinformation categorisation' (2021) 16 2 PloS one.

[22] See http://data.d4science.org/ctlg/ResourceCatalogue/ndlib. L. Milli 'Opinion Dynamic Modeling of News Perception' (2021) 6 1 Applied Network Science 1; G. Rossetti, L. Milli, S. Rinzivillo, A. Sîrbu, D. Pedreschi, F. Giannotti 'NDlib: a python library to model and analyze diffusion processes over complex networks' (2018) 5 1 International Journal of Data Science and Analytics.

[23] C. Rudin 'Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead' (2019) 1 5 Nature Machine Intelligence 206.

[24] F. Bodria, F. Giannotti, R. Guidotti, F. Naretto, D. Pedreschi, S. Rinzivilli 'Benchmarking and Survey of Explanation Methods for Black Box Models' (2021) CoRR abs/2102.13076; R. Guidotti, A. Monreale, F. Giannotti, D. Pedreschi, S. Ruggieri, F. Turini 'Factual and counterfactual explanations for black box decision' (2019) 34 6 making IEEE Intelligent Systems 14.

[25] R. Guidotti, A. Monreale, S. Ruggieri, F. Turini, F. Giannotti, D. Pedreschi 'A survey of methods for explaining black box models' (2018)51 5 ACM computing surveys 1.

[26] See <https://data.d4science.org/ctlg/ResourceCatalogue/xai_method_for_explaining_time-series>. Accessed 21 Dec 2021.

Online First ISSN 2281-5147

Drawing upon concrete cases and examples within the SoBigData++ project - namely mechanisms in play to address data-related issues – helps to show how the above-mentioned aims may be realized in practice.

The SoBigData and SoBigData++ projects[27] have developed a few vertical, thematic environments, called *exploratories*, focused on specific contexts and research questions. They are intended to test the effectiveness of the cross-disciplinary social mining research conducted on top of the SoBigData research infrastructure. The core exploratories are as follows:

- *Sustainable Cities for Citizens*: models and patterns extracted from data about cities and people living in them serve to generate knowledge about urban mobility, of potential use for local administrators to improve their services and the overall quality of living.

- *Societal Debates and Misinformation Analysis*: the analysis of discussions on social media allows understanding public debates and opinion, tracking them through time and space, and investigating the widespread phenomena of misinformation and bias.

- *Demography, Economy & Finance 2.0*: data of supermarket purchases, of people's mobility, and of financial transactions, allow the investigation of the changes in the well-being of people and in the network structure of companies due to the economic crisis.

- *Migration Studies*: the phenomenon of international migration is studied with models extracted from big data (mobile phone data, social media, surveys, official statistics, etc.), including economic models of migration, visualizing migration flows and stocks, identifying perception of migration, understanding cultural diversity and integration.

- *Sports Data Science*: starting from massive data describing several sports (especially soccer, cycling and rugby) interpretable and easy-to-use models of player performances are offered to practitioners, fans, coaches, and managers.

[27] See <https://plusplus.sobigdata.eu/>. Accessed 21 Dec 2021.

Online First ISSN 2281-5147

Let us focus on *Sustainable Cities for Citizens* as a representative example challenging the digital ecosystem of trust offered by the research infrastructure. Data about people's mobility[28] can be collected from mobile phones, vehicle trajectories, geolocated content uploaded to social media, travel tickets and cards, vehicle sharing services (bikes, scooters, cars, etc.), traffic volumes road sensors, video and photograph streams of security cameras, satellite images, credit card transaction data, shopping records, wi-fi connection, etc. Several useful initiatives and services for citizens and the public-policy decision makers can be designed using models of human behavior extracted from such big data: optimizing mobility and location-based services (car sharing, tour recommendation, public transportation scheduling); supporting urban sustainability through the understanding of urban social activities highlighted by extracted models; planning for different profiles of city users (residents, commuters, visitors, disabled, poor) whose behavior is characterized by those models; optimizing resource distribution (residential energy management, load balancing of shared bikes) based on data-driven analyses and simulations.

The downside is that data collection and models/services may put the privacy of people at risk, e.g., they may disclose the sensitive position of an individual.[29] The trade-off here is to balance the utility of the discovered mobility patterns against the necessary privacy safeguards.[30] Methods offered by the SoBigData platform are applicable at different stages of the data analysis process. Data can be perturbed or

[28] G. L. Andrienko, N. V. Andrienko, C. Boldrini, G. Caldarelli, P. Cintia, S. Cresci, A. Facchini, F. Giannotti, A. Gionis, R. Guidotti, M. Mathioudakis, C. I. Muntean, L. Pappalardo, D. Pedreschi, E. Pournaras, F. Pratesi, M. Tesconi, R. Trasarti '(So) Big Data and the transformation of the city' (2021) 11 4 Int. J. Data Sci. Anal. 311.

[29] A. Bonavita, G. Comandé, 'Mobility Data (Knowledge Discovery from)', in G. Comandé (ed.) *Elgar Encyclopedia of Law and Data Science* (Edward Elgar 2022), 227 ff.

[30] T Asikis, E. Pournaras 'Optimization of privacy-utility trade-offs under informational self-determination' (2020) 109 Future Generation Computer Systems 488; F. Pratesi, A. Monreale, R. Trasarti, F. Giannotti, D. Pedreschi, T. Yanagihara 'PRUDEnce: a System for Assessing Privacy Risk vs Utility in Data Sharing Ecosystems' (2018) 11 2 Trans Data Priv 139.

aggregated to obfuscate individual information.[31] Private-by-design methods[32] are offered to account for privacy risks when disclosing discovered patterns and models. Finally, privacy risk estimators support the data analyst to quantify and monitor the risk of re-identification from individual mobility patterns[33] and from mobility profiles.[34] The platform also offers general mechanisms to tag data with meta-information for ease of search, to control access to data and methods, and to run methods on the cloud.

In summary, the maturity of tools from the literature on privacy-preservation is a prerequisite for the ethics-oriented technology to be accepted and trusted. The *Sustainable Cities for Citizens* exploratory is a significant example showing how the privacy of data subjects and the utility of models extracted from those data can be dealt with at the same level of importance in the design of individual and society-wide data-driven services. Adequate implementation of such tools relies on expert knowledge and skills, requiring investments. While thus not necessarily an immediate advantage (from economic perspective). However, besides being justified by considerations of compliance, data citizens share under conditions of trust may be expected to have greater accuracy and utility in the long term.

3. Data Sovereignty and data altruism fostered by the DGA

A significant step towards decentralization of the web and de-monopolization of data is expected to be achieved under the Data Governance Act. The DGA's aim is to

[31] M. Fiore, P. Katsikouli, E. Zavou, M. Cunche, F. Fessant, D. Le Hello, U. Matchi Aïvodji, B. Olivier, T. Quertier, R. Stanica 'Privacy in trajectory micro-data publishing: a survey' (2020) 13 2 Trans. Data Priv. 91.

[32] N. V. Andrienko, G. L. Andrienko, G. Fuchs, P. Jankowski (2016). Scalable and privacy-respectful interactive discovery of place semantics from human mobility traces. Inf. Vis. 15(2): 117-153.

[33] R. Pellungrini, L. Pappalardo, F. Pratesi, A. Monreale 'A Data Mining Approach to Assess Privacy Risk in Human Mobility Data' (2018) 9 3 31 ACM Trans. Intell. Syst. Technol. 1.

[34] F. Pratesi, L. Gabrielli, P. Cintia, A. Monreale, F. Giannotti 'PRIMULE: Privacy risk mitigation for user profiles' (2020) 125 Data Knowl. Eng. 101786.

create a regulatory framework to facilitate data sharing, *inter alia* in support of data science and open innovation, and to foster altruistic uses of personal and non-personal data. This approach suggests an attempt by the legislator to react to the situation that society requires protection in the context of who uses technology and how technology is used.

The proposed DGA introduces information intermediaries to replace big tech players, encourages 'data altruism' with citizens to facilitate data sharing, and opens avenues for self-sovereign identities.

3.1. From data monopolies to data commons

As our societies are dealing with the social and economic implications of the Covid-19 pandemic and the reconfigurations they entail, the opportunity seems to present itself to "reclaim" digital services and data from centralized monopolies, and for practices of "data altruism". This underscores the importance and potential of initiatives with the objective of building a digital environment that encourages trust. We will provide a brief overview of some of these initiatives, which are also addressed by Dulong de Rosnay and Musiani:[35]

- In a number of contexts where AI dynamics are present, such as "smart cities" and "algorithmic governance", citizen data can either be managed in a top-down fashion,a nd controlled by centralized "control points";[36] or, alternatively, as a commons. This alternative is about the amount and quality of control and opportunities for citizen re-appropriation of data, as well as the ability to promote data commons governance models, opposed to exclusive intellectual property arrangements.

[35] M. Dulong de Rosnay, F. Musiani, 2020, "Alternatives for the Internet: A Journey into Decentralised Network Architectures and Information Commons", tripleC: communication, capitalism & critique, vol. 18, no 2, p. 622-629.

[36] L. De Nardis *The Global War for Internet Governance* (2014 Yale University Press).

- Citizens co-produce and release, intentionally or not, several types and sets of data on a daily basis, for example, by using municipal digital services. These data can be governed in a democratic, consensus-based or collegial manner, as urban or data commons, which might avert or at least mitigate the risk to turn smart cities into dystopian 'safe cities', having surveillance capitalism dynamics at their core.

- A number of other projects generate what has been defined as "big data": e.g. open data on public transportation,[37] P2P energy production by means of decentralized networks,[38] Internet of Things captors that measure street pollution rates in the frame of participatory science initiatives, or smart devices aimed at monitoring our health signs in the frame of what Andrea Matwyshyn has called the "Internet of Bodies".[39] These big data-fuelled dynamics are at a crossroads: if kept open, they can be useful and directly re-usable as a basis for policy decisions and scientific research.

- We should however keep in mind that these data include sensitive personal information in need of safeguards, such as location or health data. As we have argued elsewhere[40] privacy and commons may at first glance appear as incompatible or only partially interoperable. However, proposals do exist to apply the analytical framework of knowledge commons to private data. In these models, personal data are understood as contextualized personal information flow.[41]

---

[37] M. Teli, S. Bordin, M. Menéndez Blanco, G. Orabona, A. De Angeli 'Public Design of Digital Commons in Urban Places: A Case Study' (2015)81 International Journal of Human-Computer Studies 17.

[38] C. Giotitsas, A. Pazaitis, V. Kostakis 'A peer-to-peer approach to energy production' (2015) 42 Technology in Society 28.

[39] A. Matwyshyn 'The Internet of Bodies' (2019) 61 1 William & Mary Law Review 77.

[40] M. Dulong de Rosnay, F. Musiani 2021*supra* notes at 35.

[41] M. Sanfilippo, B. Frischmann, K. Standburg 'Privacy as commons: Case evaluation through the governing knowledge commons framework' (2018) 8 Journal of Information Policy 116.

- Proposals have also been made to link privacy to labor law negotiation mechanisms and social protection, so as to develop a legal framework for the recognition of digital labor collective rights in the data employees generate. This would allow to more easily treat them as a commons.

- G. Comandé and G. Schneider[42] advocate for a dynamic interpretation of the regulatory flexibilities provided by the General Data Protection Regulation leading to 'differential' data protection regimes for research within the European data protection framework with a different impact on contractual freedom to share and aggregate personal data, which is the primary pillar of the creation of "common data spaces" under the latest European strategy for data and under the proposed Data Governance Act.

Overall, there is a worldwide recognition of the need to conceptualize innovative theoretical frameworks to govern systems based on algorithmic decision-making, and the sets of data these systems collect, produce and process in a "closed box" or "black box" approach. These theoretical frameworks can and should inform proper legal and licensing frameworks, that would best fit urban and AI data flows, and governance models based on privacy-friendly commons, decentralized and P2P infrastructure, and on post-capitalist, non-proprietary values having sharing dynamics at their core.[43]

3.2 Decentralized architectures and self-sovereign identities

Another aspect that can be worked on in order to encourage trust in digital ecosystems is the relation between choices of particular types of technical architectures and the establishment of self-sovereign identities. In Europe there have been experiments with self-sovereign identity and application of technology to re-

[42] G. Comandé, G. Schneider 'It's time. Leveraging the gdpr to shift the balance towards research-friendly EU data spaces' (2022) Common Market Law Review.

[43] G. Priora, C. Sganga 'Smart urban mobility: a positive or negative IP space? A case study to test the role of IP in fostering data-driven innovation', in M. Finck, M. Lamping, V. Moscon, H. Richter (cur), *Smart Urban Mobility. Law, Regulation and Policy* (Springer 2020).

decentralize the web. One example is Sir Tim Berners Lee's SOLID. Another example is Ernst Hafen's data cooperation MIDATA. MIDATA contributed to the creation of an ecosystem of trust by way of giving patients the control of their own data. Drawing upon functional equivalent initiatives goes in the same direction.

These data practices are likely to be best supported by experiments with decentralized network architectures, i.e. networks that at the technical level are based on peers/equals that collaborate spontaneously and, in most cases, without requiring a central coordinating entity.[44] These networks are informed by a few core technical principles, i.e. each node of the network can act both as a supplier and as a consumer of resources, there is no central authority to which coordination is entirely delegated, and there is no entity that has a global vision (and thus a global control) of the network. This technical vision has inspired philosophers and social scientists to explore decentralized organizational forms as alternative ways not only to distribute software, files and cultural works among peers (which was the primary purposes to which peer-to-peer networks were destined in the early 2000s), but also to manage the Internet or parts of it. In a perspective of "sustainable digital development",[45] this vision can be the key to develop alternative services, applications or platforms – and at the content level, alternative knowledge or creations. Practical examples of these experimentations with decentralized architectures, which have originated in Europe, include the aforementioned SOLID Web decentralization project, or the PeerTube video platform.

Individual citizens' data stores, as proposed by Nanni et al,[46] for tracking the dynamics of COVID-19, also rely on a decentralized approach. They have been developed to collect contact and location data of persons tested positive for COVID-19. The idea behind them is to enable tracking of virus transmission chains and early detection of outbreaks in a privacy-preserving manner. The conceptual advantage of

---

[44] R. Schollmeier 'A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer architectures and applications' (2001) Proceedings of the First International Conference on Peer-to-Peer Computing 27.

[45] I. Linkov, B. D. Trump, K. Poinsatte-Jones, M. V. Florin 'Governance strategies for a sustainable digital world' (2018) 10 2 Sustainability' 440.

[46] Nanni et al (14).

the decentralized approach lies in enabling sensitive categories of data to be shared separately and selectively - either with a back-end system or the other citizens - voluntarily and with a privacy-preserving level of granularity. It allows for detailed information gathering on infected people, it enables contact tracing, and it is also scalable to large populations.[47]

Decentralized data governance schemes strongly interrelate with self-sovereignty of the networks. The vision of self-sovereignty is highly attractive, not only for decentralized schemes, but also for big tech companies in control of data. However, noin the contexts of global (e.g. COVID-19 pandemic) or pan-European actions (e.g. UEFA EURO) individual self-sovereignty can be counter-productive, unless supported by sovereignty on a geo-political level. Europe is ideally positioned to push innovation forward because of its data quality and diversity. Prominent examples are healthcare and life sciences.

3.3 Sovereignty on a geo-political level

Sovereignty on a geo-political level can work both towards and against trust in digitization, depending on the actor's political motivation. The European legislative initiatives towards fostering data sharing and control with approaches of digitization signal willingness to protect against misuse (of technology and data) by the big technological players.

The COVID-19 pandemic has arguably fueled a crisis of sovereignty. It showed "the limits of national policy, politics and borders," according to anthropologist Arjun Appadurai.[48] By suggesting that "all national sovereigns are weak" it "knocks on the door of the Westphalian model of sovereignty in a way that Ebola, SARS, and even HIV did not." Recently, the sovereignty discourse has been mobilized in reference to the digital, acknowledging that digital infrastructure puts (national and individual)

[47] Ibid.

[48] A. Appadurai 'The COVID exception' (2020) Social Anthropology.

sovereignty under strain.[49] Ongoing EU efforts to reclaim digital sovereignty are a case in point, such as, indeed, the plans for a Digital Services Act and a Digital Markets Act, as well as the GAIA-X project, tasked with developing EU data infrastructures to counter the dominance of global tech giants. Digital infrastructure is the "battlefield" of numerous attempts to exercise sovereignty, such as Russia's "*sovereign Internet*" and "anti-Apple" laws[50] or what has been defined as the "comeback" of the state in the governance of the internet.[51]

More work is needed to establish a systemic view on the distinct levels at which sovereignty dynamics unfold: these include citizens, government institutions and the private sector, and "hybrids" of these groups and entities as they evolve and interact with each other. The current data infrastructure, especially all the regulatory devices based on the treatment of data that have been deployed during the pandemic, alter "the social conditions under which information on the social world is produced",[52] managed and acted upon.[53] Further, this data infrastructure contributes to enact what Isin and Ruppert[54] called "sensory power" — a type of power based on "the accumulation of subject peoples" by means of sensors, involving "technologies of

---

[49] See, for instance, K. Irion 'Government cloud computing and national data sovereignty' (2012) 4 3-4 Policy & Internet 40; L. Amoore, R. Raley 'Securing with algorithms: Knowledge, decision, sovereignty' (2017) 48 1 Security Dialogue 3; S. Couture, S. Toupin 'What does the notion of "sovereignty" mean when referring to the digital?' (2019) 21 10 New media & society 2305; P. Hummel, M. Braun, M. Tretter, P. Dabrock 'Data sovereignty: A review' (2021) 8 1 Big Data & Society.

[50] F. Daucé, F. Musiani 'Infrastructure-embedded control, circumvention and sovereignty in the Russian Internet: An introduction' (2021) 26 5 First Monday.

[51] B. Haggart, N. Tusikov, J. A. Scholte (eds) *Power and Authority in Internet Governance: Return of the State?* (Routledge 2021).

[52] A. Desrosières *The politics of large numbers: A history of statistical reasoning* (Harvard University Press 1998).

[53] I. Hacking 'Between Michel Foucault and Erving Goffman: between discourse in the abstract and face-to-face interaction' (2004) 33 3 Economy and society 277.

[54] E. Isin, E. Ruppert 'The birth of sensory power: How a pandemic made it visible?' (2020) 7 2 Big Data & Society.

detecting, identifying and making people sense-able through various forms of digitized data (…) about their conduct".[55] While Europe is ideally positioned to push innovation forward in this regard, because of data quality and diversity (e.g., in healthcare and life science), it also faces unique challenges due to the particular configurations of sovereignty and data sovereignty it supports. In particular, when personal data, and especially health data - a special data category under Article 9 (1) GDPR) - are at stake, harmonization with the data protection framework is required. The task becomes even more complicated when the data critically required for pan-European actions *a priori* rests in the hands of individual entities. The matter merits attention in view of the highly fragmented and regulated data landscape in healthcare (bound by regulatory constraints, the obligations of professional secrecy, highly divergent data formats and encoding systems, languages, strict legitimation requirements, et cetera). What follows is that apart from potential benefits, the most recent developments in data analysis and infrastructure-building pose concrete challenges to (digital) sovereignty. At the same time, the above developments demonstrate various ways how citizens can keep full sovereignty on their privacy (rather in factual than in legal terms) and data.

A certain degree of synchronization established between the DGA and the GDPR lays a foundation for pan-European data research initiatives, as we consider next.

4. Interplay between the DGA and the GDPR

The DGA can become a centerpiece in the EU strategy for unleashing data sharing and fostering altruistic use of personal and non-personal data. In itself, it builds upon the established frameworks for research, in general, and on the avenues opened for research in support of public good (such as medical research) by the GDPR, in particular.[56]

[55] Ibid, 2.

[56] G. Schneider, G. Comandè 'Differentiating' (7).

Online First ISSN 2281-5147

4.1 General interconnection points

By adding a clear missing infrastructural and normative link, a trustworthy setting for intermediaries should be created, allowing personal data to be used with the help of a "*personal data-sharing intermediary*". This setting should be centered on allowing data use on altruistic grounds. From a technical point of view, the DGA's nature as a proposed EU Regulation (in contrast to a Directive) permits uniform and direct application of the many elements requiring a clear common framework. Chiefly, it would introduce a uniform system and interpretation of the notification for data sharing service providers, including the mechanisms for data altruism, the basic principles that apply to the reuse of public sector data that cannot be made available as open data or are not subject to sector-specific EU legislation, and the set-up of coordination structures at the European level.

The DGA exemplifies and provides content to the so-called FAIR principles limiting the conditions for reuse "*to what is necessary to preserve the rights and interests of others in the data and the integrity of the information technology and communication systems of the public sector bodies*".[57] Such a FAIR approach is made possible precisely by the GDPR regulatory background. Indeed, the very same recital 11 echoes article 89 of the GDPR in its call for transmission (and thus reuse) of anonymous data as a default approach, while also recognizing that "provision of *anonymised or modified data"* might *"not respond to the needs of the re-user"* and, for cases of continued personal data use, suggesting alternative safeguards, such as *"on-premise or remote re-use of the data within a secure processing environment*".[58] A strikingly similar approach has already been tried within the SoBigData++ project (practiced as transnational access and/or virtual access).

In the same line of deference to the GDPR, the DGA leverages the principle of lawfulness of the processing to establish trust, reasserting that "personal data should only be transmitted for re-use to a third party where a legal basis allows such

[57] Recital 11 DGA; see also articles 5 and 11(4) DGA.

[58] Recital 11 DGA.

transmission" ."[59] The evident preference for general interest research and data sharing of the DGA emerges in various instances. Among them is worth mentioning the possibility for public sector bodies "*to allow re-use at lower or no cost, for example for certain categories of reuses such as non-commercial re-use or scientific research purposes, or re-use by SMEs and start-ups, civil society and educational establishments, so as to incentivise such re-use in order to stimulate research and innovation*".[60]

As a possible response to criticisms that the GDPR might excessively limit reuse and personal data sharing, one may consider the notion of "*data cooperatives",* a specific category of data intermediaries including providers of data sharing services that offer their services to data subjects in the sense of Regulation (EU) 2016/679 "*to enhance individual agency and the individuals' control over the data pertaining to them.*"[61] By way of the intermediaries regulated in the DGA, data subjects would, for instance, be enabled to exercise their autonomy not only through the mechanism of wider consent[62] but also to make their personal data "manifestly public"[63] for specific purposes of general interest.[64]

4.2 Truly enabling personal data altruism

An element of data altruism introduced by the DGA is not insignificant for the dimension of trust in digital ecosystems. Indeed, data altruism is a landmark for reuse of data that needs to be encouraged and leveraged within the framework of the GDPR. It is recital 35 that states "*There is a strong potential in the use of data made available*

[59] Recital 11 DGA.

[60] Recital 20 DGA.

[61] Recital 23 DGA.

[62] Artt 6(1)(a) and 9(2)(a) GDPR.

[63] Art 9(2)(e) GDPR.

[64] G. Schneider, G. Comandè 'Differentiating' (7); G. Schneider, G. Comandè 'Differential Data Protection' (5); G. Schneider, G. Comandè 'It's time' (43).

voluntarily by data subjects based on their consent or, where it concerns non-personal data, made available by legal persons, for purposes of general interest."[65] At the same time, it stresses that *"Support to scientific research, including for example technological development and demonstration, fundamental research, applied research and privately funded research, should be considered as well as purposes of general interest"*.[66]

The interplay between data altruism and the GDPR in the prism of fostering research is clearly highlighted in the DGA by stressing the intermediary tools it institutes and regulates: "*In accordance with Regulation (EU) 2016/679, scientific research purposes can be supported by consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research or only to certain areas of research or parts of research projects*".[67] A highly important overlap between big data science and the data protection legal framework has been achieved with regard to data (re-)processing for medical research, essentially due to the value of health as an objective of public interest.[68]

4.3 Secondary use of health data for research – a legal perspective

The comprehensive legal framework created by the GDPR and the DGA in support of science provides a strong foundation for people to trust in the digital ecosystem and an ethically-compliant research environment. A key area of overlap exists between research ethics, the science of big data mining, and legally imposed constraints under the European data protection law: the secondary use of health data for medical research. In this context, where data originally collected for one purpose (e.g. individual diagnosis or treatment), are used for another purpose (e.g. to allow a detailed comparison between the particular patient and others, to draw wider conclusions about the origins of the disease), a number of fairly stringent conditions need to be satisfied of both legal and ethical nature. Thus, both the GDPR and

[65] Recital 35 DGA.

[66] Ibid.

[67] Recital 38 DGA.

[68] Recital 53 DGA.

normative codes of research ethics (such as the Declaration of Helsinki) often insist on the need for fresh consent from the patient to the research use. In addition, under the GDPR strict safeguards must be observed to ensure the fairness and security of the processing, including the principle of 'data minimisation', under which the data must be "*adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed*".[69]

In this regard, it appears the GDPR may contribute rather well to the building of trust relations as a key component, as mentioned earlier, to research involving the use of data, especially sensitive data of a medical kind. The patient subject retains control – the ability to veto the data processing (by refusing consent) as well as knowing that the researcher (data controller) owes an ongoing obligation to use the data in a fair and careful manner. The GDPR also equips the subject with a series of additional rights (under articles 12-20) including the right to withdraw their data from the research at any time. Under these circumstances, it is suggested that researchers working with relatively few subjects and taking the trouble to build up ties and to involve these in the overall research aim (e.g. better treatment for a given disease, from which the subject or a relative may themselves suffer) have a good chance of being able to acquire and use relevant data in an effective (as well as legally compatible) manner.

At the same time, it may be wondered how far this legal framework is favorable to larger scale research, particularly when the researcher has little (or perhaps no) direct contact with the subjects, and receives instead the data via a third-party intermediary. Here the hurdles, including the need for re-consent to different research uses and the guarantee of the subject's rights under the GDPR, may pose considerable logistical and organizational challenges. In this kind of situation, it appears that data privacy and autonomy concerns could lead to suboptimal research outcomes, though this is admittedly difficult to quantify.

A further interesting question, in the specific context of 'big data'-analytic medical research is whether the risk-based approach to data processing found in the GDPR may inhibit such research, even where, in line with normative codes of ethics, the interests and concerns of the research participants are safeguarded to the letter. This

[69] Art 5(1)(c) GDPR.

arises in view of the need, under article 35 of the GDPR, for data processing operations "*likely to result in a high risk to the rights and freedoms of natural persons*" to be subject to a rigorous prior 'data protection impact assessment', potentially including the need for approval by the relevant supervisory authorities. Arguably, this would apply if proposed data research is likely to generate knowledge that would create a dilemma not adequately addressed by the research plan. This is certainly a risk with unsupervised data analytic processes of the kind used to make sense of large volumes of data, which discern probabilistic correlations rather than causal relations. In particular, it may lead to cases where science can predict, on the basis of a person's data, that the person has a high probability of contracting a given disease, but (lacking firm causal knowledge) not do much to stop it: here, the dilemma would be what to tell the person.

In summary, it can fairly be said that, while the GDPR contains important provisions, contributing to safe and ethical use of medical data for research, it has the potential to make both the approval and execution of such research quite complicated. While this may result in Europe lagging behind other parts of the world, where such legal restrictions do not operate, it is not clear that it will (or to what extent the legal constraints will be enforced with regard to research). For example, in the last scenario, a rule requiring data researchers to privilege data analytical processes that generate actionable causally-grounded knowledge could also provide a (scientifically) useful steer. Careful, ongoing analysis, which takes account of diverse data analytical research methods, as well as their respective strengths and weaknesses (including risks to the data subjects and wider society), will be required in order to progress towards a balanced legal and ethical solution.

5. Conclusion and steps forward

From the above discussion, it follows that the initiatives towards creating a European digital ecosystem of trust, including trustful research environments, are quite a few, spreading across regulatory, societal, technological, geo-political, and legal fields. Such initiatives encompass mechanisms integrating ethics-by-design, privacy-preserving technologies, the phenomena of data altruism, data intermediaries, self-sovereign identities and instruments for web decentralization. An important

infrastructural and normative link has been established, thus enabling the creation of trustworthy settings facilitating safe data sharing. The avenues already opened for research, both by the FAIR principles and the legal grounds provided by the GDPR, have found due reflection and productive adoption. A remarkable sign is that such initiatives mainly pay tribute to the core values of the European society, namely fundamental rights and ethics.

The further the story goes, the more challenges emerge. In particular, it becomes evident against the background of integrating the stringent GDPR requirements into research settings, especially when health data are concerned - an important asset for individuals, healthcare and associated industries, the public and the state. The attempts to address such challenges are quite prominent, such as solutions around explainable AI, innovative data control mechanisms, and efforts to address data biases and discriminatory capacity hidden in data and algorithms. Such aspects are critical and merit ongoing reflection and an interdisciplinary approach, which goes beyond the realm of this paper but bears rich potential for further exploration.

Acknowledgment: This work was supported by the European Commission through the H2020-INFRAIA-2018-2020 / H2020-INFRAIA-2019-1 European project "SoBigData++: European Integrated Infrastructure for Social Mining and Big Data Analytics" (Grant Agreement 871042). The funders had no role in developing the research and writing the manuscript.