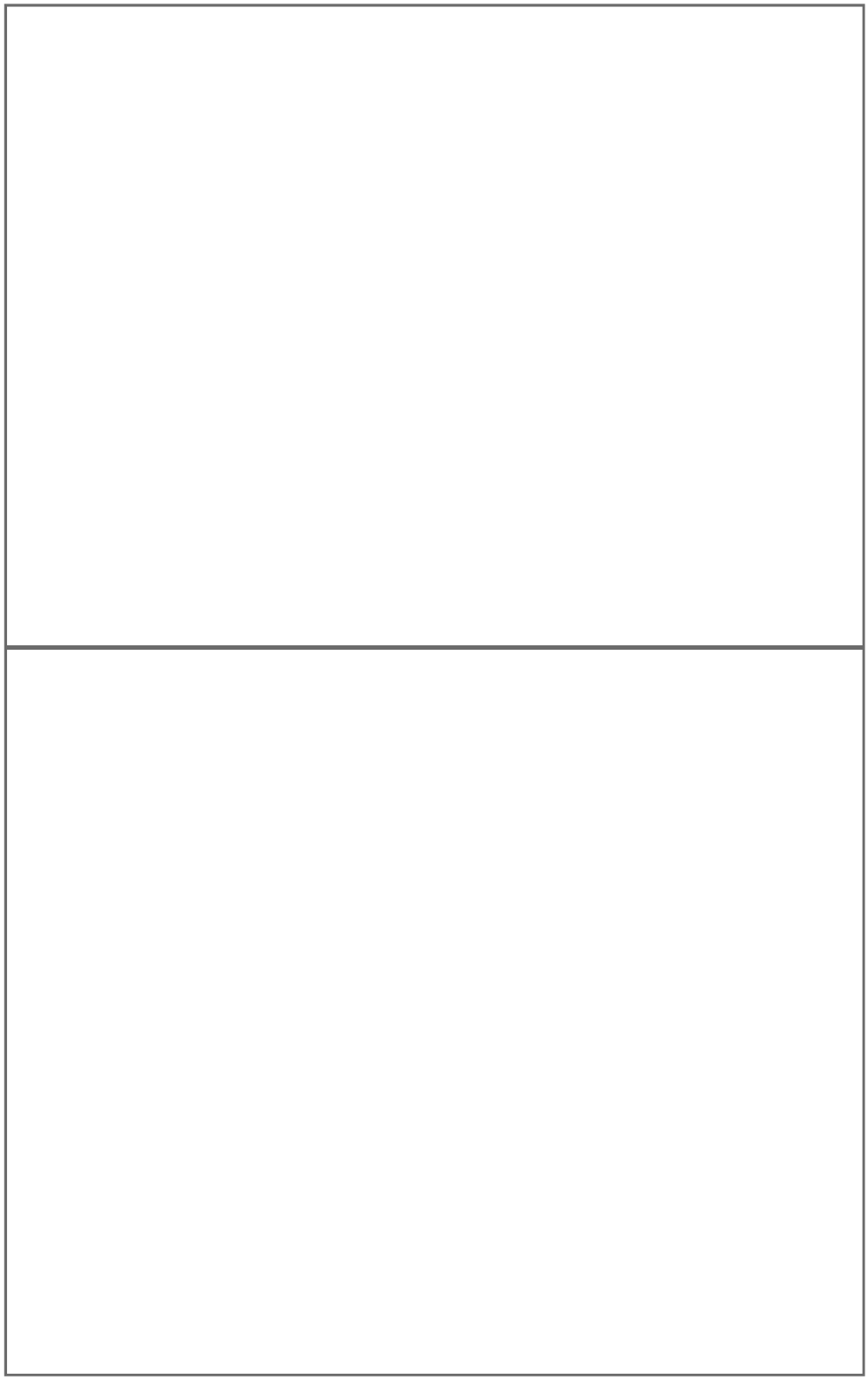
Camilla Crea | Alberto De Franceschi (Eds.)

The New Shapes of Digital Vulnerability in European Private Law

Nomos



Camilla Crea | Alberto De Franceschi (Eds.)

The New Shapes of Digital Vulnerability in European Private Law

Prefaces by
Frank Pasquale and Oreste Pollicino

Nomos

This volume is funded by the Italian Ministry of University and Research as a 'Research Project of National Interest (PRIN) 2020XBFME2'

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.d-nb.de

1st Edition 2024

Published by
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Production of the printed version:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN 978-3-7560-1632-7 (Print)
ISBN 978-3-7489-4091-3 (ePDF)
DOI https://doi.org/10.5771/9783748940913

Online Version
Nomos eLibrary

Table of Contents

PART III Contexts and Images of Digital Vulnerable Subjects

CONCLUSIONS

Authors' profiles

Denise Amram is a senior Assistant Professor of Comparative Private Law at LIDER Lab – DIRPOLIS Institute L'EMbeDS Department of Excellence at Scuola Superiore Sant'Anna of Pisa (Italy). At LIDER Lab, she coordinates the research lines ETHOS (EThics and law witH and fOr reSearch), Children's Rights, and the Permanent Observatory on Personal Injury Damages. Her research interests include fundamental rights enhancement and protection of vulnerable subjects in different context, especially within the digital dimension.

Shabahang Arian holds a PhD in Law from the Dirpolis Institute of the Scuola Superiore Sant'Anna in Pisa. She is currently an adjunct professor and researcher at University of Tehran where she is dedicated to advancing legal education and fostering innovative research in the field of Law and Technology.

Federica Casarosa is a Research Associate at the Scuola Superiore Sant'Anna (Pisa) and part-time professor at the European University Institute. Since her degree in Private Law (University of Pisa, 2001) and her subsequent PhD in Law (European University Institute, 2008), Federica Casarosa has directed her interests towards the intersection of law and technology, analysing the role of information in consumer contracting, the protection of consumer data and internet users, private regulation in the protection of freedom of expression, and the impact of cybersecurity legislation in private law. She has carried out both teaching and research activities on these topics.

Niti Chatterjee is a seasoned commercial and technology lawyer with over a decade of experience advising multinational corporations. Holding an advanced LLM in Digital Technology Law from Leiden University, Niti specializes in the intersection of law and technology, focusing on ethical practices in the digital realm. Currently based in Luxembourg, she is passionate about promoting the responsible use of technology and advocating for regulatory frameworks that ensure fairness and accountability in the digital landscape.

Camilla Crea is Associate Professor of Private Law at the University of Sannio. She is the founder and Editor-in-Chief of The Italian Law Journal, and serves on the editorial boards of several Italian legal journals and book series. She is the author of monographs and essays on contract law, intellectual property and private law theory, analyzed through historical, comparative and critical perspectives. She has held research and teaching positions at many foreign universities, including the University of Berkeley; Beijing Normal University; Sorbonne Université; Université Cadi Ayyad-Marrakech; Edinburgh Centre for Private Law; Florida International University; Université Paris

Nanterre; Université Catholique de Lille; and the École des hautes études en sciences sociales (EHESS).

Alberto De Franceschi is Professor of Private Law, Digital Law and International Trade Law at the University of Ferrara, Ambassador's Chair at the KU Leuven and Distinguished Visiting Professor at the UC Los Angeles. From 2021 to 2023 he was Visiting Professor at the Zhejiang University, Hangzhou. Since 2016 he has been serving as Italian Expert at EU Council, G7 Digital&Technology, UNCITRAL E-Commerce Working Group, Unidroit and the Hague Conference on Private International Law. He is co-editor of the "Journal of European Consumer and Market Law" and of "The Italian Law Journal". He is an Ordinary Member of the Academia Europaea and of the European Academy of Sciences and Art. His research deals with Law of obligations and contracts, with focus on digital economy and sustainability.

Giovanni De Gregorio is the PLMJ Chair in Law and Technology at Católica Global School of Law and Católica Lisbon School of Law. He is also a member of the Católica Research Centre for the Future of Law. His research interests include digital constitutionalism, fundamental rights, technologies and digital policy. Giovanni is the author of the monograph Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society (Cambridge University Press 2022).

Irina Domurath is Adjunct Professor of Law at the University Adolfo Ibañez in Santiago de Chile. Previously, she held positions at the Central University of Chile, the University of Amsterdam, and the University of Copenhagen. She researches the effects of market regulation on horizontal relationships, with case studies concerning consumer credit, access to housing, and data protection.

Mateja Durovic is Professor of Law and Co-Director of the Centre for Technology, Ethics, Law and Society (TELOS) at King's College London, where he first worked as lecturer and then as a reader in law. Previous to this, he was an Assistant Professor (2015-2017) at the School of Law, City University of Hong Kong. Dr. Mateja Durovic holds a PhD and LLM degrees from the European University Institute, Italy, LLM degree from the University of Cambridge, UK, and LLB degree from the University of Belgrade, Serbia. Dr. Durovic was a Post-Doc Research Associate at the EUI, Italy (2014-2015), Visiting Scholar at Stanford Law School, USA (2011), and at the Max Planck Institute of Private International and Comparative Law, Hamburg, Germany (2010). Dr. Durovic worked for the Legal Service of the European Commission, as well as a consultant for the European Commission, World Bank, GIZ, BEUC and the United Nations. The work of Dr. Durovic was published in leading law journals and by most prominent publishers. He is a member of the European Law Institute, Society of Legal Scholars and Society for European Contract Law.

Isabel Laura Ebert is a Senior Research Fellow at the Institute for Business Ethics and Institute for Work and Employment Research, University of St. Gallen, and serves as a Strategic Adviser to the United Nations Office of the High Commissioner for Human Rights B-Tech Project, focusing on Business & Human Rights in the technology

sector. Her research explores regulatory and policy responses to emerging human rights challenges connected with technology company conduct and implications for policy coherence. Isabel received a PhD in Business Ethics from the University of St. Gallen.

Fabrizio Esposito is a Bocconi and EUI alumnus and Associate Professor of Private at the NOVA School of Law (Lisbon). His 40+ publications combine doctrinal analysis, especially of EU consumer and regulatory law, with economics and other disciplines. His monograph, *The Consumer Welfare Hypothesis in Law and Economics,* opens a new path in 'law and economics'. He has co-edited three volumes, including the forthcoming *Cambridge Handbook on Algorithmic Price Personalization and the Law.* Fabrizio sits on the Consulting Board of the *European Review of Contract Law* and acts as class representative in two class actions against Big Tech companies.

Catalina Goanta is Associate Professor in Private Law and Technology and Principal Investigator of the ERC Starting Grant HUMANads, focused on understanding the impact of content monetization on social media and on reinterpreting private law fairness in the context of platform governance. Between 2016-2021 she was Assistant Professor at the Faculty of Law at Maastricht University, and during February 2018 - February 2019, she was a Niels Stensen fellow and visited the University of St. Gallen (The Institute of Work and Employment) and Harvard University (The Berkman Center for Internet and Society). She is also a non-residential fellow of the Stanford Transatlantic Technology Law Forum.

Gérardine Goh Escolar is Deputy Secretary General of the Hague Conference on Private International Law (HCCH), and Head of its International Commercial, Digital and Financial Law Division. Dr Goh Escolar is Full Professor (Adjunct) and Academic Fellow at the Centre for Technology, Robotics, Artificial Intelligence and the Law (TRAIL) at the Faculty of Law of the National University of Singapore.

Jura Golub, LLM, is a Research Assistant at the Faculty of Law Osijek, Croatia, and a PhD Candidate under the Croatian Science Foundation's program "Young Researchers' Career Development Project – Training of New Doctoral Students." He teaches seminar classes in Private International Law at the Faculty of Law Osijek. His research focuses on the digitalization of law, particularly on issues related to digital assets from both substantive and conflict-of-law perspectives. Jura has presented at several international scientific conferences, including those at Radboud University, the University of Milan, the University of Ferrara, the National University of Singapore, and Royal Holloway, University of London. As a recipient of a British Scholarship Trust award, he completed a two-month research stay at Kingßs College London, The Dickson Poon School of Law. He is also the author of several scientific and professional papers.

Mateusz Grochowski is an Associate Professor of Law at Tulane University School of Law and an Affiliated Fellow at the Information Society Project at Yale Law School. His research focuses on the intersections of digital market and contract law theory, the protection of weaker market participants, and the comparative study of US-EU consumer protection and regulation of digital markets. He is a member of the editorial boards of

the "Rabel Journal of Comparative and International Private Law" and the "Journal of European Consumer and Market Law", as well as a member of the consulting board for the "European Review of Contract Law".

Eleni Kaprou is a senior lecturer in Business Law in Queen Mary University of London since 2022. Prior to that she held posts in Brunel University and Cardiff. Eleni has also served as a consultant on EU projects and taught on executive programmes for civil servants. Eleni's research interests lay in European private law with a focus on vulnerable subjects. She has written on consumer vulnerability, aggressive practices and retail financial services among others. Currently she is working on aggressive practices in the digital environment.

Gianclaudio Malgieri is an Associate Professor of Law & Technology at Leiden University (the Netherlands) and a board member of the eLaw Center for Law and Digital Technologies. He serves as the Co-Director of the Brussels Privacy Hub, an Associate Editor of Computer Law and Security Review, and the founder of "VULNERA", the International Observatory of Vulnerable People in Data Protection. He conducts research on and teaches Data Protection Law, AI regulation, Fundamental Rights in the Digital Age, Legal Vulnerability. He is the author of "Vulnerability and Data Protection Law" (Oxford University Press, 2023). Gianclaudio has authored over 70 publications, including articles in leading international academic journals. His works have been cited by, inter alia, top international newspapers (The New York Times, The Washington Post, Le Monde, Politico, La Tribune, France Culture, ilSole24Ore, la Repubblica, il Corriere della Sera, Euractiv).

Hans-W. Micklitz is Part-time Professor of Economic Law, European University Institute, Florence Italy, fullt-time between 2007 and 2019, formerly Professor at the Berlin School of Business and the University of Bamberg (Germany), visiting scholar at the universities of Bologna (Italy), Columbia (USA), Florence (Italy), Helsinki (Finland), Michigan (USA) and Oxford (UK), ERC Grant 2011-2016 on European Regulatory Private Law, Grant Academy of Finland, 2017-2022 on External Dimension of European Private Law, research on European and transnational private law, compulaw, legal theory.

Emilia Mišćenić, Dr. iur. (KFU Graz), LL.M. (Saarland) is a full professor at the Faculty of Law, University of Rijeka. For her academic work in the field of European private law and consumer protection, she has been awarded by the Croatian National Science Award, the Award of the University of Rijeka Foundation, the Award of the Republic of Croatia Ivan Filipović and many others. Her work has contributed to AG's legal opinions in cases such as Pereničová and Perenič, Meta Platforms Ireland and UFC, Que choisir and CLCV AG. She is a co-chair of the award-winning European Law Institute Croatian Hub, and a head of the University of Rijeka project "Transparency and Fairness in the Digital Environment" (uniri-iskusni-drustv-23-101).

Frank Pasquale is Professor of Law at Cornell Law School and Cornell Tech. He is an expert on the law of artificial intelligence (AI), algorithms, and machine learning. His

books include The Black Box Society (Harvard University Press, 2015) and New Laws of Robotics (Harvard University Press, 2020). His work has been translated into over a dozen languages. His present research is focused on affective computing, the political economy of automation, and AI in the public sphere.

Alessandra Pera is PhD in Comparative Law and Full Professor at Palermo University-Department of Political Science and International Relations. Her research focuses on family law, ADR systems and protection of vulnerable individuals and groups. Member of the International Society of Family Law (ISFL), the Italian Association of Comparative Law (AIDC) and Juris Diversitas. She has been visiting at the IALS University of London, the Cape Town University, the Rey Juan Carlos University of Madrid, the Hanu-Hanoi University. Member of the Editorial board of Comparazione e Diritto Civile, Comparative Law Review, International Journal of Law and Society, Cardozo Electronic Law Bulletin.

Oreste Pollicino is Professor of Constitutional Law at Bocconi University. His research interests focus on European and Comparative Constitutional Law, and Digital Constitutional Law. He is the Director of the LLM in Law of Internet Technologies at Bocconi University. He has been appointed by the European Commission for the negotiation on the 'European code of practice on disinformation'. He is also member of the Executive Board, European Union Agency for Fundamental Rights, and of the European Commission Sounding Board of the Multistakeholder in the fight against online disinformation. He is participant to the Council of Europe Ad Hoc Committee on Artificial Intelligence (CAHAI), and Italian member of the OECD Global Partnership on Artificial Intelligence.

Sara Rigazio is PhD in Private Law, holds a LL.M. from the University of Minnesota Law School and is Assistant Professor of Private Law at the department of Political Sciences and International Relations at the University of Palermo. She has been visiting fellow at the Norwegian Center for Computer and Law at the University of Oslo. She has published several articles and a book on family law, national and international child protection, legal design and the relationship with new technologies.

Katarzyna Południak-Gierz Ph.D. (Jagiellonian University in Kraków) is a senior lecturer at the Jagiellonian University's Private Law Department. Her academic interests focus on the interplay between private law and technology. She researches private law reactions towards the use of personalization techniques in consumer contracts and the possibility of using granularity to increase the ecological efficiency of sales law.

Teresa Rodríguez de las Heras Ballell is Full Professor of Commercial Law at University Carlos III of Madrid, Spain. She was Sir Roy Goode Scholar at Unidroit 2021–22. She is the Delegate of Spain at UNCITRAL for WGs VI, IV (on AI in international trade) and I, and an Expert for UNCITRAL and Unidroit on digital economy projects. Arbitrator. Member of the Austrian Academy of Sciences. Member of the European Commission Expert Groups on Liability and New Technologies, for the Observatory

on Online Platform Economy, and on B2B Data Sharing. Member of the ELI Executive Committee and Council, and co-reporter of ELI Algorithmic Contracting Project.

Alain Sandoz holds a MSc in mathematics from Neuchâtel University and a PhD in computer science and distributed information systems engineering from EPFL, Lausanne. His interests are related to distributed information systems design and implementation; the role of scale and complexity in innovation strategy; and information infrastructures. He is lecturer and professor at Neuchâtel University and has been teaching informatics and strategy at higher education institutions in Switzerland since 1995.

Reiner Schulze is Professor Emeritus of German and European Civil Law and Director of the Centre for European Private Law at the University of Münster, Germany. He is a founding member of the European Research Group on Existing EC Private Law and the European Law Institute, as well as foreign member of the Italian Accademia Nazionale dei Lincei and the Spanish Real Academia de Jurisprudencia y Legislación. He has published extensively in the field of European private law, contract and consumer law, and digital law with books including *European Contract Law* (3rd edn, co-written with Fryderyk Zoll), *EU Digital Law* (2nd edn, co-editor with Dirk Staudenmayer), and *Bürgerliches Gesetzbuch Handkommentar* (12th edn).

Gerasimos (Jerry) Spanakis is an assistant professor in machine learning and data mining at Maastricht University. His current work lies in the area of Social Computing and includes computational social media modeling, dialogue systems (conversational agents) and information retrieval. More specifically, he is interested into using Large Language Models (like chatGPT) in a controlled way and build useful applications that have added value for all relevant stakeholders, especially for the legal domain. He is the PI for the VOXReality H2020 project, co-organizes the Natural Legal Language Workshop, and serves as a senior expert for the European Commission's e-enforcement academy project.

Léa Stiefel holds a PhD in Social Sciences in the field of STS and Digital Studies. Her thesis, defended and awarded at the University of Lausanne in 2023, focused on the Politics of digital architectures. She currently works as a research fellow at the Swiss Competency Centre for Penal Sanctions (cscsp.ch) in Fribourg and is also vice-president of IRIN (irin.ch), an independent research institute on digitisation based in Bulle.

Piotr Tereszkiewicz Ph.D. (Jagiellonian University in Kraków), M.Jur (Oxford), is a professor at the Jagiellonian's University Private Law Department, an adjunct professor at Cornell Law School and a senior affiliated researcher at the University of Leuven (KU Leuven). His research interests include private law, law and economics, insurance law and financial services in a comparative and international perspective. He was

Deputy Chair of the Scientific Advisory Committee at the Financial Ombudsman in Poland (2019–2021).

Patryk Walczak is a a PhD Candidate at the Jagiellonian University in Kraków, Poland.

Isabelle Wildhaber, LL.M. (Harvard Law School), is a Full Professor for Private and Business Law at the University of St. Gallen and the Executive Director at the Institute for Work and Employment Research (FAA-HSG) at the University of St. Gallen in Switzerland. Isabelle Wildhaber is admitted to the Bar in Switzerland and to the Bar in New York First Department, having previously worked for Swiss and American law firms in Basel, New York and Frankfurt a.M.

Standards to Face Children and Patients Digital Vulnerabilities

Denise Amram

A. Introduction: digital vulnerabilities and the digitization of vulnerabilities

The advent of the digital era has strongly impacted on the way people lead their daily lives. In fact, novel contexts where diverse cultures, needs, and values intersect with the potential of data-driven economy, where individuals can be exposed to a series of new risks, or be included in minorities due to a combination of factors that affect their life and existence at a particular historical moment. The digital transformation of services, products, and relationships impacts on the mechanisms for fundamental rights protection, enforcement, and empowerment. This is because new risks have emerged (and are still emerging) in the digital environment, leading to what is referred to as "digital vulnerabilities". For example, cybersecurity profiles or issues related to interoperability requirements are proper only of the digital dimension, shaping additional assessments and consequent measures to be implemented exclusively to protect fundamental from specific risks emerging online or from the operations set by new technologies.

In addition to the digital vulnerabilities, within the cyberspace already known risks may require additional safeguards compared to the ones implemented to face the same ones within the physical dimension. For example, in the healthcare sector, the patient is still vulnerable because of the information asymmetry in providing consent to healthcare choices, however, where digital technologies that are supporting diagnosis, treatment, or rehabilitation activities, might change the results of the impact assessment. Therefore, new methodologies and different risk mitigation measures shall be adapted considering the process of "digitalization of vulnerabilities", as a supplementary ground to be properly addressed by the relevant stakeholders to protect and promote fundamental rights also in the digital dimension.[1]

1 D.J. Solove, *The New Vulnerability: Data Security and Personal Information, in Securing Privacy in the Internet Age*, Radin & Chander, eds., Stanford University Press, 2008,

The impact of the digital dimension on fundamental rights generally relates to the analysis of the effects that the potential lack of transparency or awareness has on the individuals, especially as far as the data processing activities (such as profiling of habits or behaviours, or the secondary use of data) are concerned. In fact, the gradual loss of control over the flow of information in the digital environment is the main issue to be addressed in order to avoid negative implications from data sharing. In particular, what should be subjected to assessment is the increasing probability to suffer negative consequences, including unforeseeable ones, from the processing of personal (and non-personal) data in the digital dimension. [2] Among the most common scenarios in this regard, there is the necessity to address possible unauthorized access to information concerning the individual, as well as the unauthorized profiling of the individual habits, resulting in direct (or indirect) exposure to automated content or decisions for purposes not necessarily related to the ones that led to the original data collection. [3]

The interest on this topic arises from the number and relevance of the legislative initiatives promoted within the framework of the European Union's strategy on data and the digital market.[4] They all share a common approach based on risks analysis: in fact, they are all structured to identify roles and responsibilities among the various actors in a specific data flow, in order to better identify and assess the potential impact on users, both

GWU Law School Public Law Research Paper No. 102 <https://ssrn.com/abstract=583483>.

2 A. Mantelero, M.S. Esposito, *An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems*, in *Computer Law & Security Review*, Volume 41, 2021, 105561, ISSN 0267-3649, <https://doi.org/10.1016/j.clsr.2021.105561>.

3 G. Comandé, *Regulating Algorithms' Regulation? First Ethico-Legal Principles, Problems, and Opportunities of Algorithms*, in T. Cerquitelli, D. Quercia, F. Pasquale, *Transparent Data Mining for Big and Small Data*, *Springer*, *2017*, 169 ff.

4 Regulation (EU) 2016/679 of the European Parliament and ft he Council of 27 April 2016 on the protection of natural persons with regard ft he processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), Digital Service Act, Regulation (EU) 2022/2065 of the European Parliament and ft he Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), the Regulation (EU) 2022/868 of the European Parliament and ft he Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance); Proposal for a Regulation ft he EU Parliament and ft he Council on harmonised rules on fair access to and use of data (Data Act) COM/2022/68 final, etc.

as individuals and as categories of vulnerable subjects. As a consequence, diversified compliance levels with specific obligations aim at protecting users (*ie* the recipients of the service or product being marketed, or the data subject of the data processing activities) from different perspectives. Examples of such obligations include the data protection impact assessment under Article 35 of EU Regulation n. 2016/679 (hereinafter GDPR) [5], the evaluation of the reliability of systems based on artificial intelligence techniques under the recently approved EU Regulation 2024/1689[6], or the obligations of due diligence on online content imposed by the EU Regulation n. 2022/2065 on Digital Services Act (hereinafter DSA)[7].

This contribution aims to provide insights into the methodology to be applied for analyzing the risks arising from the digitalization process in different sectors, where technological innovation is integrated into the dynamics of care relationships, that are requiring new balances respect to the physical dimension.[8] This is both to meet the obligations set by regulations addressed to specific sectors and to align with the informative principles in the field, which are themselves enriched with new interpretative content for the necessary adaptations to maintain the effectiveness of the liability paradigm also in the digital dimension.

To this end, two positions are explored in this paper: children, who are vulnerable because of their legal incapacity unless represented, and patients, who are vulnerable due to their limited psycho-physical integrity. Before the digital dimension, in fact, they both become users (and potential consumers), adding a new ground of vulnerability due to the contractual asymmetry with the market players.

---

5 M. E. Kaminski, G. Malgieri, *Algorithmic impact assessments under the GDPR: producing multi-layered explanations*, in *International Data Privacy Law*, 2021, 125 <https://doi.org/10.1093/idpl/ipaa020>.

6 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance).

7 A. Gullo, *Il Digital Services Act e il contrasto alla disinformazione: responsabilità dei provider, obblighi di compliance e modelli di enforcement*, MediaLaws, 2023, 2, <https://www.medialaws.eu/rivista/sezione-monografica-il-digital-services-act-e-il-contrasto-alla-disinformazione-responsabilita-dei-provider-obblighi-di-compliance-e-modelli-di-enforcement-contenuti-scopi-e-traiettoria-della/>.

8 J.A. Sanchez, P. Barach, J.K. Johnson, J.P. Jacobs (eds), *Improving Safety, Quality, and Value*, Springer, 2017.

As a result, common principles are identified and their interplay with technical standards explored in order to achieve a common core of harmonised best practices that could help the *by design* protection of vulnerable groups in the digital dimension.

B. Risks and opportunities for children

The digitalisation of services and products impacted on the growth of children since the earliest stages of their lives[9]: new risks, but also new opportunities, addressed in the cyberspace require tailored approaches towards children's care and education.[10]

Global challenges launched for children and the ongoing initiatives aiming to shape an inclusive future generation of digitalized citizens are highlighting the increasing opportunities of access to culture and education offered by the information society, fostering the need to address fresh forms of free expression, organization, and association[11]. In the cyberspace, ideas and content are disseminated more rapidly and effectively. Furthermore, physical and mental well-being could be enhanced by empowering individual attitudes and skills through tailored paths of learning, experiencing, and playing in the digital dimension. Inclusivity can be promoted by providing broader chances to exchange experiences, knowledge, and values among the world being just connected to internet[12]. In this context, the acquisition of digital skills becomes imperative for the education of children. This is an especially delicate matter, given that UNICEF reports that nearly 65 million young people, approximately 90% of adolescent girls and young women aged between 15-23 years old remain without internet access[13]. Hence,

9 S. Livingstone, G. Lansdown, and A. Third, *The case for a UNCRC general comment on children's rights and digital media*, 2017, LSE Consulting/Children's Commission.

10 E. Marrus and P. Laufer-Ukels, *Global Reflections on Children's Rights and the Law 30 Years After the Convention on the Rights of the Child* (Routledge 2021).

11 See the OHCHR, *Children's rights and the 2030 Agenda for Sustainable Development*, https://www.ohchr.org/en/children/childrens-rights-and-2030-agenda-sustainable-development.

12 Committee on the Rights of the Child 'General comment No. 25 (2021) on children's rights in relation to the digital environment' (2021). <https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en>.

13 The statistics refers to low-income countries, where almost 78% of young men and male adolescents are offline too (57 million persons), UNICEF, Bridging the Gender Digital Divide, Report, 2023, <https://data.unicef.org/resources/ictgenderdivide/>.

the digital divide among young generations concerns as it exacerbates the economic disparities, and it pertains to the cultural shifts affecting the daily routines of every child and their caregivers. The implementation of appropriate measures to ensure inclusivity, non-discrimination, and safety within the IoT shall thus be designed and applied as a standard to be followed in order to avoid the development of harmful mechanisms of access and use of digital services.[14]

The above-illustrated premises need to be balanced considering the different phases of growth and maturity of the given child, rather than solely relying on the formal definition of a minor. According to Article 1 of the UN Convention on the Rights of the Child (hereinafter CRC), adopted in New York in 1989, a minor is defined as "*every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier*". Despite this, in fact, one-third of the IoT users are aged between 11 and 16. Therefore, critical profiles arising from their daily engagement within information society services shall be not only addressed but also solved since risks might daily occur, becoming urgent harms for children's wellbeing[15]. In this regard, the GDPR is the first EU legislative initiative on data relying with children as a specific category of (vulnerable) data subjects. It established that consent to process data by information society services could be autonomously provided at 16 years old, leaving the Members States to identify a lower threshold up to 13 years old, considering that in the data protection impact assessment, the data controller would have addressed the vulnerability of children-users as a ground of specific analysis.

From this perspective, the fact that the new service launched by OpenAI Ldt, the well-known ChatGPT[16], has been limited by the Italian data protection authority because of the lack of safeguards to identify the age of potential users, stresses a lack of an attentive strategy, looking at the possible vulnerable categories of users in the digital environment, as well as the necessity to implement stricter obligations for services providers to

14 Ibid.

15 M. Boomgaard, *Children's Rights in Data Protection: A Comparative Analysis on Ex-Ante and Ex-Post Protection of Children's Data in the EU and the USA* (College of Europe 2016).

16 D. Amram, *Accountability, Transparency, and Fairness to Assess Generative AI Solutions with the Lenses of Data Protection Law*, Diritti Comparati, 2023 <https://www.diritticomparati.it/accountability-transparency-and-fairness-to-assess-generative-ai-solutions-with-the-lenses-of-data-protection-law/>.

specifically develop risks assessment procedures to protect such a vulnerable users category *by design* and *by default*.

While the so called AI Act just refers to children as vulnerable groups in *recitals* 16, 19 and 28, and in articles 5, sub d. i) and article 9 *sub* 8) stating that the risk assessment shall take into "*specific consideration (…) whether the high-risk AI system is likely to be accessed by or have an impact on children*", without providing any instrument to address it, the DSA covers this gap in article 35 *sub* j) where it presents a short list of organisational and technical safeguards, like "*age verification and parental control tools, reporting tools aimed at helping minors signal abuse or obtain support*". The DSA commitment to protect children is expressed also in the recital 71, stating that due-diligence obligations shall be applied to an online platform that can be "*considered to be accessible to minors when its terms and conditions permit minors to use the service, when its service is directed at or predominantly used by minors, or where the provider is otherwise aware that some of the recipients of its service are minors*", for example through personal data processing. In these cases, therefore, "*appropriate and proportionate measures to protect minors*" shall be implemented, including the design online interfaces reaching "*the highest level of privacy, safety and security for minors by default where appropriate or adopting standards for protection of minors, or participating in codes of conduct for protecting minors*". The recital identifies also as best practices and available guidance the ones provided by the communication of the Commission on A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+). In particular, it recommends introducing specific safeguards in case of profiling activities based on personal data processing, in compliance with the principle of data minimisation that shall prohibit the online platform "*to maintain, acquire or process more personal data than it already has in order to assess if the recipient of the service is a minor*".

In this regard, it seems that the protection of children as users of digital services is a technical matter, aiming to firstly verify the age of the user in order to enable or prohibit the exposure to contents, services, and products. However, these technical standards might not be sufficient to address the challenges of an inclusive and safer digital environment as additional measures – including organisational ones – might be required to face specific harms emerging even for services directly targeted to children.

I. Harms in the digital environment

The EU Commission identified six different harms that may occur to children while accessing IoT as users.[17] The first relates to fake news, which authors have identified as falling into six different concepts, including content manipulation, satire, and advertising.[18]

By its misleading nature, fake news can have a negative impact on the development of children's opinions, whose discerning capacity and maturity are still in evolution.[19] In this regard, the DSA expresses the commitment of the EU Commission to address this risk as a general attempt to users' fundamental rights protection and empowerment. In particular, DSA compliance activities include the obligation to publish annual reports on content moderation practices, the one to set users friendly complaints mechanisms to make content removed if illicit or in contrast with inclusiveness, non-discrimination or fundamental rights. Furthermore, Very Large Online Platforms shall formally assess risks also connected to the content manipulation in order to avoid misuses as disinformation spreading, especially in crisis cases.

The second risk concerns exposure to cyberbullying.[20] For the victim, this can be shaped as a series of behaviours including an innocuous attitude to perpetrate moral disengagement as well as harmful exposures to disturbing content. The latter is perceived as a third autonomous risk when it becomes a -so-called- digital challenge/game directly offered to young users. The well-known case of the *Blue Whale*, consisting of proposing a series of tasks to depressed teenagers for a period, increasing time after time the relative level of self-harm until inducing players to suicide, has been followed by other challenges like *Chroming*.[21] Article 6 CRC states that children have

17 European Commission, *EUKidsOnline survey*, IP/11/479. See previous remarks on the topic in the contribution: D. Amram, *Children (in the digital environment)*, in G. Comandé (ed), Elgar Encyclopedia of Law and Data Science, 2022, 64 ff.

18 E.C. Tandoc, Z.W. Lim and R. Ling, *Defining "fake news": A typology of scholarly definitions*, 2017, Digital Journalism, 6, 137ff.

19 Council of Europe, *Challenges to Children's Rights Today: What Do Children Think*? (2015), Ch. 8.

20 S.C. Vestergaard (ed.) *Encyclopedia of Bullying* (Nova 2020).

21 F. Liat and G. Khalid, *The criminalization of cyberbullying among children and youth*, 2019, 17 Santa Clara J Int'l L 1ff. See the recent urgent measures adopted by the Italian Data Protection Authority against the Tik Tok platform following a 10-year-old child's death from an online challenge, <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9524224>; (2019); in May 2020 the Dutch DPA started an

an inherent right to life and, therefore, also within the digital environment they shall be protected from violence and suicide.[22] Such a protection may be compromised even in a technically robust system. Parents' awareness and collaboration with schools become essential to prevent harms for the given child, however at any level, each stakeholder shall contribute to avoid the described phenomena. In this regard, the well-known TikTok platform has been recently sanctioned by the European Data Protection Board for a dossier issued by the Irish data protection authority, because of the illicit data processing activities of underaged users[23].

Furthermore, children can be exposed to grooming and sexting both as users of social networks, platforms, etc., and where someone else shares their pictures, images, videos. To this end, national legal systems are implementing new provisions in order to address the digital dimension of these crimes.

As the digital dimension is based on data processing, it is not surprising that the data protection authorities are those ones that have more sanctioned services providers for exposing children to known risks of the Internet of Things. In fact, all the mitigation measures concern data processing activities. This is true also in case of AI-based solutions, where data processing is undertaken through an automated decision-making system. For example, in case of toys that can monitor and record children's habits, behaviours, voices, without their parents or adults or caregivers having any control over that kind of data processing or means and purposes of processing activities deployed after the data collection, two different risks might be envisaged: firstly, the *boomerang* effect of being target both for specific advertisement and manipulative marketing strategies and, secondly, for even unpredictable uses, since none has the control on that kind of information and safeguards that are applied to the data flows before being shared to third parties.[24] Further vulnerabilities might also be exposed

investigation into the same platform <https://autoriteitpersoonsgegevens.nl/en/news/dutch-data-protection-authority-investigate-tiktok>.

22 Doek, J.E., *Article 6 CRC and the views of the CRC Committee*, 2015, 26 Stellenbosch L. Rev. 254.

23 EDPB, Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR), <https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22023-dispute-submitted_en>.

24 B. Knowles, S. Beck, J. Finney, J. Devine and J. Lindley, *A scenario-based methodology for exploring risks: Children and programmable IoT*, DIS'19 Proceedings (2019) 751 ff.

through the combination of IoT services and AI-based technologies. For example, the increasing use of chatbot systems at home can increasingly affect teenagers' behaviours, becoming a kind of personal assistant to be checked for confirmation on possible outfit, or other daily attitudes that are shaping one's personal identity. [25]

Some of the mentioned risks could be mitigated by technical and organizational measures implemented by services providers and developers, especially if standards and codes of conducts are adopted. However, an essential role is played by adults (family members, teachers, educators, and professionals) that shall develop a digital education and be able to transmit competence and skills to detect and avoid dangerous circumstances.[26] A strong information and awareness campaign promoted by institutions (schools, social services, municipalities, etc.) has become a priority. A long-term commitment towards a cultural change shall be addressed to protect children as *per se* vulnerable users.

To this end, international organisations, like UNICEF, have produced tailored strategies aimed at promoting children's rights in the digital environment as a priority[27]. Other ones are developing specific studies to address these issues, for example the Joint Research Centre of the EU Commission has published a report in order to address future policies for a more ethical approach of AI-based systems for children: some applications have been mapped and classified in terms of risks and opportunities under a series of parameters, including accessibility, engagement for learning, adaptation, social interaction, health, transparency, inclusivity etc[28].

Considering the principles stated in the CRC, to protect children's rights in the digital environment means to develop a setting where they can enhance their freedoms to shape and express their opinion both as individuals and as belonging to groups, and at the same time not being

25 H. Alexa, S. Cortesi, A. Lombana-Bermudez and U.Gasser, *Youth and Artificial Intelligence: Where We Stand*, 2019, Berkman Klein Center for Internet & Society publication.

26 T. Leibur, L. Saks, I.A. Chounta, *Towards Acquiring Teachers' Professional Qualification Based on Professional Standards: Perceptions, Expectations and Needs on the Application Process*, 2021, Education Sciences, 11(8), 391 and I. Tuomi, R. Cachia, D. Villar-Onrubia, *On the Futures of Technology in Education: Emerging Trends and Policy Implications*, JRC Publication, 2023, <file:///C:/Users/denis/Downloads/JRC134308_01.pdf>.

27 UNICEF, *Policy guidance on AI for children*, 2020.

28 JRC, *Artificial Intelligence and the Rights of the Child*, 2022.

exposed to potential harms. Thus, the general principle of the best interests of the child stated under Article 3 CRC requires a specific balance in the digital dimension between rights and situations aimed at identifying case by case which conditions could satisfy the child's well-being.[29] Other principles, like the one of non-discrimination – stated by Article 2 CRC-, become paramount also within the EU regulations to establish a safer digital environment where equal access is guaranteed, despite of the existing digital divide between countries facilities. Socio-geographical-economic conditions shall not affect the possibility to enjoy fundamental rights in the digital dimension.[30] However, the exclusion from online services is an index of contemporary poverty and it is largely impacting on raising the new generation of adults. Therefore, for the most marginalized groups of children proper actions should be implemented to remove these barriers. In particular, it highlights the role of learning initiatives for children as a means to successfully avoiding the risks and exploiting the opportunities offered by the information society.[31] The COVID-19 pandemic emergency has highlighted this aspect, as everywhere – especially primary and secondary – schools moved to e-learning activities: the access to internet facilities was the means to allow children to remotely attend classes and keep pursuing their educational path. Moreover, access should not be denied, and content should be reliable and not harmful under the well-known grounds of inclusiveness assessment based on race, ethnic origins, political opinions, religious/philosophical beliefs, trade union memberships or sexual orientation. Conversely, a digital environment that could admit grounds of discrimination shall be completely prohibited and limited. Further challenges might be launched for the use of generative AI applications.[32]

Under Articles 12 and 13 CRC, children's right to be heard and the right to freedom of expression are promoted in IoT services.[33] In particular, Article 12 enhances participation in decision-making, while Article 13 includes

29 J. Todres and S.M. King, *The Oxford Handbook of Children's Rights Law* (OUP 2021); J. Tobin, *The UN Convention on the Rights of the Child: A Commentary* (OUP 2019).

30 T. O'Neill and D. Zinga, *Children's Rights: Multidisciplinary Approaches to Participation and Protection* (University of Toronto Press 2008).

31 Council of Europe, *Strategy for the Rights of the Child*, 2016–21, <https://edoc.coe.int/en/module/ec_addformat/download?cle=2d45cbe914655ca562553cb81fdfc464&k=43516ccd18e8b8e8d5d68b6fd3b7e4c1>.

32 UNICEF, *Generative AI: Risks and Opportunities for Children* (2023), <https://www.unicef.org/globalinsight/media/3061/file>.

33 S. Lee, *A child's voice VS. A parent's control: Resolving tension between the Convention on the Rights of the Child*, U.S. LAW' (2017) 117(3) Columbia Law Review, 687–727.

"*the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice*".

These rights could be empowered at different levels according to the maturity of the child. However, everyday online educational, training, or ludic activities mark the IoT as a place to develop individual and collective thoughts and opinions. Further, as illustrated, if we combine these principles with the exposure of the child to the manipulation of information and fake news, state parties should identify proper actions in order not only to guarantee the right to freedom of expression in the information society services but to enhance it towards inclusiveness and pluralism as an opportunity for children to grow in a child-friendly and safe environment. In this regard, the role of the EU Regulation on DSA is particularly relevant as well, where it states that manipulative techniques for advertisements are forbidden. The recital 69 of DSA explains, indeed, that advertisements based on profiling activities, using special categories of personal data are prohibited because they may "*amplify societal harms, for example by contributing to disinformation campaigns or by discriminating against certain groups*".

II. Policies, guidelines, and standards

An equal access to a safe and fair digital environment and technologies application requires to address risks and detect mitigation measures. However, this is not sufficient, as institutions, public and private organisations, companies, and individuals shall responsibly contribute to grow up the next generation of adults as well.

According to article 19 CRC, for example, State Parties must adopt all legislative, administrative, social and educational measures to avoid any forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse. As we have seen, this principle is particularly sensitive in the digital age, considering the urgency to prevent the above illustrated phenomena like cyberbullying, grooming, sexting, primarily affecting child users. To introduce only control and monitoring systems cannot be the solution, since there is another general principle to be balanced: under Article 16 CRC, there is a prohibition on arbitrary or unlawful interference with children's privacy, family,

home or correspondence, which translates into a child-centred perspective the debate on privacy preserving and data protection in the digital age, also recalling the more recent formula included in Article 8 of the European Charter of Fundamental Rights.[34] Caregivers' and parental responsibilities become therefore the boundaries within which the child's autonomy may be framed in a sophisticated balance of rights and duties aimed at enhancing individual skills, while protecting them from risks and harms.[35]

The Council of Europe firstly adopted a Recommendation, namely the CM/Rec(2018)7 of the Committee of Ministers to Member States, providing guidelines to respect, protect and fulfil the rights of the child in the digital environment. This soft law mechanism aimed at driving the law and policy making processes in each State Party through the interpretation enshrined in human rights conventions as well as at including standards, emerging from relevant case law issued by the European Court of Human Rights.[36] Then, it launched a Strategy on the rights of Child 2022-2027, including safeguards addressed to the digitalisation and use of AI. The Guidelines appeared very useful to define the digital environment as the "*information and communication technologies (ICTs), including the internet, mobile and associated technologies and devices, as well as digital networks, databases, content and services*". This allowed to foster safeguards implementations by services providers, parents, and caregivers, and all relevant stakeholders, all responsible to guarantee a safe and resilient setting. Guidelines addressed also the opportunity to engage children more effectively in the decision-making process by highlighting educational paths, skills, and best practices to increase the value of child-friendly technologies. To achieve the first goal, State Parties must ensure high standards of online services and contents. The Guidelines identified also the so-called "*distinctive opportunities*" to enable online communication, gaming, networking and entertainment with children both in play and to peaceful assembly and association. The Strategy fosters six objectives, aligned with the above-mentioned risks, including

34 M. Ruiz-Casarez, T.M. Collins, E.K.M. Tisdall and S. Grover, *Children's rights to participation and protection in international development and humanitarian interventions: Nurturing a dialogue*, International Journal of Human Rights, 21, 2018 doi: <https://doi.org/10.1080/13642987.2016.1262520>.

35 B. Shmueli and A. Blecher-Prigat, *Privacy for children*, Columbia Human Rights Law Review, 42, 2011, 759 ff.

36 S. Livingstone, E. Lievens and J. Carr, *Handbook for Policy Makers on the Rights of the Child in the Digital Environment* (2020) COE <https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8>.

to keep children safe from violence, to guarantee equal opportunities in the current society, to support access to new technologies, to give them voice and participation, to support them in emergency situations and crisis, and develop a child-friendly justice. The main current challenge is to promote these objectives either in the physical dimension or in the digital one.

As far as child's best interests are concerned[37], the first condition for a child-friendly data-driven economy is to identify the proper methodological approaches to combine compliance *by design* and tailored decision-making in the given circumstances for each specific digital service/tool/activity/product. This approach should be adaptable according to a series of variables that may include, as seen, age and maturity of the user, digital skills both of the child and her parent/caregiver, exposure to each of the mentioned risks, level of awareness, etc. It should also include monitoring mechanisms to report gaps and detect best practices in order to achieve an everyday higher level of trustworthiness.[38] In fact, decision-making or data processing that could be acceptable for adults may not be so for children and, therefore, appropriate technical and organizational measures should be implemented to guarantee conformity with CRC principles in the digital dimension.

Current debates on AI, robotics, and digital services[39] regulations are not addressing specific technical and organizational measures for a child-friendly paradigm to comply with *by design* and *by default*. In particular, policy and law-making efforts are driven towards common requirements and standards for developers, intermediaries, service providers, etc. without highlighting the vulnerabilities emerging where children are the data subjects/end users. Thus, the role of parents, caregivers, educators, facilitators are the main driver to ensure case by case the pursuing of the best interests of the child in the use of AI-based technologies/digital services. As observed, this approach is not sufficient to empower children's rights if we consider the peculiarity of risks and opportunities that solutions from

37 E. Lamarque, *Il principio dei best interests of the child nella prospettiva costituzionale* (Franco Angeli 2016).

38 High-Level Expert Group on AI (2020) 'Ethics guidelines for trustworthy artificial intelligence', <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.

39 Proposal for a regulation on a European approach for artificial intelligence, in <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence>.

research and innovation development are bringing to children's everyday life.

In this regard, UNICEF proposed to fill such a gap, by drafting the Policy Guidance on AI for Children.[40] It identified nine requirements for child-centred AI, including recommendations on how AI techniques could be made suitable for children's well-being and safety, as well as to prepare them for future technological developments. These recommendations, however, require to be associated with technical requirements in order to find concrete applications in the services and products offered to children as users of the new technologies.

In this regard, standards developed by the Institute of Electrical and Electronics Engineers, namely the IEEE 2089-2021, are supporting the development of tailored procedures aiming to encompass the following key principles: the fact that the given system shall recognise if the user is a child; the fact that it is mandatory to distinguish children from young people as different categories of users; the fact that interfaces shall use of child-friendly language; the fact that within the balance between commercial interests and children's ones the latter shall prevail[41].

In this debate, the GDPR plays a pioneering role for two reasons. Firstly, it constitutes an example to protect personal data by including a risk-based data subjects-oriented approach aimed at continuously assessing the impact of each component of data processing (i.e. the means, purposes, nature of data, subjects, technology adopted). Secondly, Article 8 GDPR is dedicated to minors' consent for online data processing, opening new interpretations on the balance between the formal legal age and the actual maturity of young users. [42]

40 UNICEF, *Policy guidance on AI for children*, n. 27 above.

41 IEEE, *IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children*, 2021, <https://standards.ieee.org/ieee/2089/7633/>.

42 As mentioned, the framework becomes more complex as the same provision that states that a 16-year-old child can give valid consent for IoT data processing, it also leaves the opportunity for member states to decrease the age limit to 13 years. This last limit is the same as that introduced in the US Children Online Privacy Protection Act (COPPA), effective since 2000.L.A. Matecki, *Update: COPPA is ineffective legislation! Next steps for protecting youth privacy rights in the social networking era*, 2010, 5 Nw. J. L. & Soc. Pol'y. 369 http://scholarlycommons.law.northwestern.edu/njlsp/vol5/iss2/7, during the publication of this essay, new protections have been enacted for teens though the Kids Online Safety Council (KOSA) and the COPPA 2.0 bills, see S.1409 — 118th Congress (2023-2024), <https://www.congress.gov/bill/118th-congress/senate-bill/1409/text>.

In light of these remarks, a second challenge for child-friendly data economy consists of considering the digital dimension as a new scenario where children's rights must be protected, promoted, and enforced. Therefore, a multilevel paradigm towards parental responsibilities[43] must be adopted in order to include tailored actions and proactive approaches to child-friendly innovation and technologies.

In particular, proper roles and responsibilities have to be identified for parents/caregivers/facilitators in order to develop digital skills and competence and at the same time develop a privacy-preserving awareness to avoid digital-related risks.[44] An accountable approach would thus be adopted since the development of the given service/product addressed to children. It shall be indeed pursued by adults in a continuing balance of new knowledge and skills development functional to monitoring and detecting new harms and risks in order to prevent them[45].

More generally, parents and caregivers should thereby ensure education, care, and maintenance duties also in the digital environment, highlighting the different roles of each adult in a multilevel system of obligations and duties that might align with the concepts of responsibility, accountability, and liability in the digital dimension.

Finally, a child-friendly setting should be developed through proper actions and safeguards to address further vulnerabilities of children to concretely contribute to the purposes of inclusiveness and non-discrimination. For example, disabilities, socio-economic barriers, education gaps, digital divide issues are particularly sensitive ones for children as they may dramatically affect their growth and development in society. Specific attention shall therefore be addressed to vulnerabilities within the "children" as a category of users. For example, children with disabilities may constitute a specific category of vulnerable users. Risks and opportunities shall be addressed also in light of the specific principles stated for disabled persons, like for instance in the context of the Convention on the Rights of Persons

43 D. Amram, In familia respondēre. *La famiglia alla prova della solidarietà e del principio di responsabilizzazione. Contributo ad una ricostruzione sistematica* (Torino, 2020) 1–252.

44 J. Albo-Canals, D. Amram, K. Kaesling, J. Martinez Otero, R.G. Pensa et al., *Children's rights in online environments with social robots: The use case study of CORP: A collaborative online robotics platform*', ACM, 2021.

45 See also A. Pera – S. Rigazio, *Let the children play. Smart toys and child vulnerability*, Chapter 14.

with Disabilities.[46] Disabled children's quality of life, indeed, might be strongly improved by the digitalisation of services and products and the digital transition of healthcare, education, and more general of economy. Thus, the information society services could be considered as a bridge for inclusiveness in certain circumstances, but only when it is safe and reliable for multiple level of vulnerabilities of the users' categories.[47]

To better address vulnerabilities emerging from the compromission of the psycho-physical integrity, it is worth to explore how the digitalisation is impacting on the patient-clinician relationship.

C. Patients and clinicians

In this paragraph, we explore the effects of the digital transition of the healthcare services in order to address and mitigate the emerging vulnerabilities respect to the two main categories of stakeholders: the patients and the clinicians.

As known, the digitalization of healthcare services can encompass both diagnostic and treatment phases, activating patient participation in the process of personalized care. This is often referred to the so-called *P5 Medicine*, indicating technologies that promote i) predictive, ii) preventive, iii) personalized, iv) participatory, and v) psycho-cognitive medicine through the application of digital and AI-based technologies, arising ethical and legal issues to be addressed in order to mitigate new (and old) vulnerabilities for an effective improvement of the healthcare system.[48]

As a self-evident method to detect vulnerabilities we will address the concept of "sensitive" information represented by the notion of data belonging to specific categories under Article 4 GDPR[49]. Sensitive, as stated, is the

46 M. Alper and G. Gogging, 'Digital technology and rights in the lives of children with disabilities' (2017) New Media & Soc., 19(5): 726–40.

47 L. Lundy, B. Byrne, M. Templeton, and G. Lansdown, 'Report on children with disabilities in the digital environment' (2019) <https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f>.

48 See in D. Amram, A. Cignoni, T. Banfi, G. Ciuti, *From P4 medicine to P5 medicine: transitional times for a more human-centric approach to AI-based tools for hospitals of tomorrow*, Open Research Europe, 2022, 2:33 <https://doi.org/10.12688/openreseurope.14524.1>.

49 G. Comandé, G. Schneider, *Regulatory Challenges of Data Mining Practices: The Case of the Never-ending Lifecycles of 'Health Data'*, in European J. Health Law, 2018, 284 ff. <https://dx.doi.org/10.1163/15718093-12520368>. G. Bincoletto – P. Guarda,

information that can reveal certain characteristics of the data subjects and, for this reason, make them vulnerable in relation to their peer group. Information related to one's health status, for example, classifies the individual as a patient rather than a healthy person, profiling a potential vulnerability in their physical or mental sphere: therefore, health-related information produces a declarative effect of the vulnerability.

In this regard, the passage from the physical to the digital dimension, nothing changes for the identification of patients as a category of vulnerable persons.

The digitalization of the processing activities of health-related data, namely collection, use (and reuse), indeed, may have increased the risk of compromising the confidentiality of information included in data flows (through the increasement of occurrence that unauthorized access or unauthorised further processing might be performed, for example), but at the same time, it reduced the likelihood of information unavailability (primarily due to possible backup copies included in any data breach policy), contributing to a more effective management of the informative flow[50]. The same effect occurs with regard to the integrity of information: compared to paper-based support, the traceability of actions required to manage health-related data in the digital environment reduced the consequences of human errors, by allowing effective and faster countermeasures for content restoration/correction.[51]

An efficient data management may therefore facilitate the provision of healthcare services, but it may arise some issues within the clinician-patient relationship in terms of impact of the digitalisation on the asymmetry information between "professional" and "customer" roles. Therefore, it

A proactive GDPR-compliant solution for fostering medical scientific research as a secondary use of personal health data, Opinio Juris in Comparatione, 2021, 43 ff.

50 ENISA, *Data Pseudonymisation: Advanced Techniques and Use Cases*, 2021 <https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases>.

51 G. Wang, A. Badal, X. Jia et al., *Development of metaverse for intelligent healthcare*, in *Nat Mach Intell*, 2022, 4, 922 <https://doi.org/10.1038/s42256-022-00549-6>. Si veda G. Lofaro, *Dati sanitari e e-Health europea: tra trattamento dei dati personali e decisione amministrativa algoritmica*, in *MediaLaws*, 2022, 3, <https://www.medialaws.eu/rivista/dati-sanitari-e-e-health-europea-tra-trattamento-dei-dati-personali-e-decisione-amministrativa-algoritmica/>.

is extremely relevant to assess if and how the vulnerability may change through the digitalisation of the patient-clinician alliance.[52]

Firstly, the use of new technologies introduces an "intermediation" into the clinician-patient relationship, namely the human-machine interface that requires a tailored interaction, for instance, this is particularly evident in the case of robotic surgery, where healthcare services provision is mechanically supported by a tool solely driven by the surgeon. Secondly, while depersonalizing certain aspects of healthcare services, especially those related to data processing from analysis, technology enables greater personalization of other aspects of the same ones. By comparing a specific clinical framework with vast amounts of similar scenarios, there is an evident potential for improving the accuracy of the diagnosis and a simultaneous reduction in the overall state of vulnerability, meant as the compromission of psychophysical integrity of the patient. In this context, the clinician-patient relationship is supplemented by the human-machine component[53], which needs to be addressed both in terms of the relationship between the digital element and healthcare staff and with respect to the patients (and their vulnerabilities).

To investigate the impact on fundamental human rights and, consequently, assess the risks for their violation, it is observed that, in relation to healthcare staff, technological support must be accompanied by specific training aimed at developing skills for monitoring and intervening in the event of malfunction or inadequacy of the machine for the specific task. Additionally, healthcare professionals should acquire new interpretative methodologies for the results of automated processes to support decision-making operations in diagnosis or treatment.[54] From the patient's perspective, a series of issues arises regarding the need to ensure self-deter-

52 The Economist, *A digital revolution in health care is speeding up*, 04.03.2017; H.S. Sætra, E. Fosch-Villaronga, *Healthcare Digitalisation and the Changing Nature of Work and Society*. Healthcare (Basel). 2021 Aug 6;9(8):1007. doi: 10.3390/healthcare9081007.

53 D. Larrivee, *Values Evolution in Human Machine Relations: Grounding Computationalism and Neural Dynamics in a Physical a Priorism of Nature*, in *Front. Hum. Neurosci.*, 2021, 15:649544. doi: 10.3389/fnhum.2021.649544.

54 L. Lessard, W. Michalowski, M. Fung-Kee-Fung, L. Jones and A. Grudniewicz, *Architectural Frameworks: Defining the Structures for Implementing Learning Health Systems*, in *Implementation Science* 12(1) (2017) 78. DOI: 10.1186/s13012-017-0607-7.

mination[55] in healthcare choices in the digital dimension and beyond.[56] There are multiple ethical and legal aspects to addres[57]: from the conditions for achieving a satisfied level of trustworthiness in the performance of machines supporting clinical services, to mechanisms to share awareness on the consequences of data collection for potential reuse, to the need to train the system to improve the accuracy of services for altruistic purposes, including research, experimentation, statistical analysis for the overall advancement of diagnostic, treatment, and rehabilitation capabilities. Given that the result of the balance between the risks and opportunities of digitalization in the relevant sector should ideally yield a positive value, it is necessary to categorize vulnerabilities in a variety of scenarios in order to be able to shape a unified methodology to provide policy guidelines for a virtuous acceleration of the introduction and use of digital systems in healthcare facilities.[58]

Firstly, we may distinguish the state of emergency, from routine circumstances, like outpatient screening or surgical procedures, where standards and protocols are regularly applied with no exception like in the emergencies. Additionally, we need to address the increasingly common situation where patients actively participate in care and rehabilitation activities through monitoring devices and dedicated apps, where the active and informed role of the vulnerable subject is an essential part of the strategy effectiveness of the telemedicine services. [59]

I. Vulnerabilities in digitalised emergency, outpatient, and surgical services

Within the emergency scenario, for example, the digitalization of first aid operations represents a significant opportunity for operative coordination

55 G. Resta, *La regolazione digitale nell'Unione Europea. Pubblico, privato, collettivo nel sistema europeo del governo dei dati*, in *Riv. Trim. Dir. Pubb.,* 2022, 971 ff.

56 L. Palazzani, *Informed consent for clinical research in the context of the Covid-19 pandemic between bioethics and biolaw: a general overview*, *BioLaw J*. <https://doi.org/10.15168/2284-4503-843>.

57 M.H. Arnold, *Teasing out Artificial Intelligence in Medicine: An Ethical Critique of Artificial Intelligence and Machine Learning in Medicine*, in *Bioethical Inquiry* 18, 121–139 (2021) <https://doi.org/10.1007/s11673-020-10080-1>.

58 J. Pizoń, A. Gola, *Human–Machine Relationship—Perspective and Future Roadmap for Industry 5.0 Solutions*, in *Machines*, 2023, 11, 203 <https://doi.org/10.3390/machines11020203>.

59 See previous remarks in D. Amram, *La transizione digitale delle vulnerabilità e il sistema della responsabilità*, in *Riv. It. Med. Legale,* 2023, 1 ff.

through personal (and non-personal) data sharing. This approach requires the identification of a proper legal basis justifying such processing activities. In fact, the extraordinary and temporary situation in which natural or artificial events disrupt the normal sequence of actions and events as well as the direct or indirect involvement of persons in an emergency situation constitute *per se* a case of vulnerability. Indeed, physical and mental well-being - as well as the emotional, economic, social, or environmental conditions - can be differently affected by dealing with a specific emergency situation.

Data-driven technologies may process personal data under a series of conditions that may satisfy the lawfulness both under Article 9(2)(c), the vital interests of the data subject or third parties when "*the data subject is physically or legally incapable of giving consent*", and under Article 9(2)(i), public interest in the field of public health. In these cases, it is relevant to define where the data processing begins (through direct or indirect collection of information) and where it ends. In particular, to enable possible further processing (the so-called reuse of collected information), especially after the emergency situation, tailored technical and organizational measures must be implemented to the same data flow, also addressing different legal bases.[60] For example, measures such as the pseudonymization and encryption of data to remain within the bounds of lawfulness of processing might be required to switch from the emergency legal basis to the one enabling the reuse for statistics and research purposes, under for example Article 89 GDPR. These conditions are the same either in case of paper-based or digital informative flows. More complex is the question related to the governance of data flows if they are digitalised and if the converges in an everyday more frequent digital platform aiming to collect data, combining the different sources of triage services (from the ones collected *in situ* by first responders to those collected through geo-localisation systems, *eg* drones and other systems). It seems reasonable to consider that data collected to face emergencies could be processed by public organizations, as well as by private or public ones engaged in activities related to the

60 L. L. Skovgaard, S. Wadmann, K. Hoeyer, *A review of attitudes towards the reuse of health data among people in the European Union: The primacy of purpose and the common good*, Health Policy, Volume 123, Issue 6, 2019, 564 ff. <https://doi.org/10.1016/j.healthpol.2019.03.012>. See also the special issue G. Malgieri – P. De Hert, *Legal and Ethical Challenges of Data Processing in the research field*, in *Computer Law & Sec. Review*, 2020, 37 <https://www.sciencedirect.com/journal/computer-law-and-security-review/special-issue/10S60T5Q4Z8>.

described purposes. The development of technologies associated with systems aiming to develop unique triage sessions must take into account a series of regulatory aspects to prevent vulnerable individuals from being exposed to risks not mitigated by appropriate technical and organizational measures. In particular, the system must strive to comply with the principles of lawfulness, proportionality, minimization, and accountability, even in situations involving different jurisdictions. It should proactively identify which data shall be enabled or denied, for how long, and to which systems, both for incoming and outgoing data flows. It will also be necessary to identify countermeasures in the event of malfunctions to ensure the ability to restore the state of affairs in case of unauthorized loss, access, or modification as quickly as possible, so as not to compromise rescue operations. To this end, technical and procedural standards play an essential harmonising role at national, EU, and transnational level.[61]

Once the emergency management phase is completed, it is necessary to understand if (and how) the collected information can be reused for additional and different purposes. This perception may change from the physical to the digital collection of information. In fact, all possible players of first response activities might have interest to reuse the collected data for other purposes than the ones that enabled the original processing. For example, needs related to the evaluation and organization of first aid services may allow local (and non-local) oversight bodies to extract aggregated information to understand the scope of the intervention. However, it is necessary to define boundaries opening a generated database. From this perspective, anonymized data collected for public healthcare and similar purposes reasonably fall within the scope of the Open Data Directive and the Regulation on European data governance, also known as the Data Governance Act.[62] Unless there are reasons of public security, no limits appear to be set to making the collected data freely available in an intelligible format. Regarding personal data, especially health related ones, the natural

61 S. López Bernal, M. Quiles Pérez, E. T. Martínez Beltrán, M. Martín Curto, Y. Yanakiev, M. Gil Pérez, G. Martínez Pérez, *Opportunities for standardization in emergency scenarios in the European Union*, International Journal of Medical Informatics, Volume 179, 2023, <https://doi.org/10.1016/j.ijmedinf.2023.105232>.

62 See G. Carovano, M. Finck, *Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy*, Computer Law & Security Review, Volume 50, 2023, 105830 <https://doi.org/10.1016/j.clsr.2023.105830>; D. Amram, *Comparing EU Initiatives on Data: Addressing Risks and Enhancing Harmonisation Opportunities*, in *Opinio Juris in Comparatione*, 2023, 1 ff. <https://www.opiniojurisincomparatione.org/wp-content/uploads/2023/03/Amram_Online-First-1.pdf>.

subsequent destination after the initial first aid appears to be a medical record for the individual's healthcare purposes, thereby falling within the scope of Article 9(2)(h) of the GDPR.

In routine healthcare services, particularly in the outpatient scenarios, the primary use of patient data is governed by the healthcare purpose. However, it is important to note that the classification of information related to the individual's health status and its comparison with similar cases are part of the clinical method, even before the experimental one. The reconstruction of the clinical framework, especially in screening programs, results in data collection that needs to be classified and processed for decision-making purposes. The support of digital technologies in these activities is becoming increasingly common and incorporated into outpatient protocols and procedures. However, such technologies should be communicated to the patient to obtain informed consent, taking into account the implications for the established trust relationship with the clinician.[63]

The so-called social contact[64] that characterizes the relationship between the clinician and the patient undergoes adaptations in case of technological support that deserve to be analysed and interpreted in the context of the evolution of the information society. In particular, two scenarios are identified. The technological support for outpatient activities could still be in the study phase and patients are recruited based on a specific protocol approved by the relevant ethics committee. From the patient's perspective, they can choose whether to participate in the experiment or not, and the decision not to use technological support for healthcare provision shall not affect the clinician-patient relationship. Consequently, the patient can choose whether or not to provide consent to the use and reuse of data collected for experimental purposes. In this case, the patient's vulnerability is determined not only by their health conditions, but also by the informative

63 M. Jungkunz, A. Köngeter, K. Mehlis, E.C. Winkler and C. Schickhardt, *Secondary Use of Clinical Data in Data-Gathering, Non-Interventional Research or Learning Activities: Definition, Types, and a Framework for Risk Assessment*, in *Journal of Medical Internet Research* 23(6) (2021) e26631, doi: 10.2196/26631.

64 F. Giardina, *Responsabilità contrattuale ed extracontrattuale: significato attuale di una distinzione tradizionale*, Milano, 1993, F.D. Busnelli, *Verso un possibile riavvicinamento tra responsabilità contrattuale ed extracontrattuale*, in *Resp. civ. prev.*, 1977, 784, Id., *Itinerari europei nella «terra di nessuno tra contratto e fatto illecito»: la responsabilità da informazioni inesatte*, in *Contr. e impr.*, 1991, 539 ff., R. Pardolesi - R. Simone, *Nuova responsabilità medica: il dito e la luna (contro i guasti da contatto sociale?)*, in *Foro it.*, V, 2017, 4, 167.

asymmetry related to the development of the given experimental protocol, which must include specific risks mitigation measures for the system used in the particular outpatient setting. Additionally, ethical and legal assessments are made regarding the reliability of the algorithmic system used to make automated decisions for diagnostic and treatment purposes as a part of the ethical protocol.[65] The second case concerns the technological support for outpatient activities that is already integrated into the regular protocol of the service. The information system is an essential part of the equipment necessary for service delivery, and the patient, adequately informed, may not find alternatives to the use of the given technology for the provision of the healthcare services in that facility. The refusal of consent would thus result the inability to provide the service. However, also in this case patients shall maintain the control upon their information, and they can always prevent the reuse of their data by denying the consent to that specific data processing.

When the two described scenarios are each other consecutive, it seems reasonable to consider opening a phase of organizational and professional adaptation for the healthcare personnel affected by the introduction of technological innovation into the system. In fact, in the event that the experimentation is successful, and the new device is authorized by the competent ministry to be marketed or introduced into the corresponding department, it is necessary to put oneself in the position of the clinician and delve into the critical issues that may arise regarding the provision of the service in the daily context. In other words, in order to reshape the standards of diligence in light of the innovative element, it will be necessary to undertake a series of initiatives aimed at mitigating the vulnerabilities arising from the human-machine relationship [66] and identifying possible additional issues that may arise in that specific environment.

65 N. Naik, B.M.Z. Hameed, D.K. Shetty, D. Swain, M. Shah, R. Paul, K. Aggarwal, S. Ibrahim, V. Patil, K. Smriti, S. Shetty, B.P. Rai, P. Chlosta and B.K. Somani, *Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?*, in *Front. Surg.*, 2022, 9:862322. doi: 10.3389/fsurg.2022.862322.

66 See the High-Level Group on Trustworthy AI, https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment, see K. Hawley, *How to Be Trustworthy*, Oxford Un. Preff., 2019. M. Agbese et al., *Governance in Ethical and Trustworthy AI Systems: Extension of the ECCOLA Method for AI Ethics Governance Using GARP*, 2023, E-informatica: Software Engineering Journal 17.1 e R.V. Zicari et al., *On Assessing Trustworthy AI in Healthcare: Machine Learning as a Supportive Tool to Recognize Cardiac Arrest in Emergency Calls*, in *Frontiers in Human Dynamics*, 2021, 3.

From this perspective, a new category of vulnerable persons emerges: the one of the healthcare staff that needs to develop specific professional skills and competence to deal with the new technology. In particular, it is essential that the training will be aimed to avoid possible distortions caused by excessive reliance on technological support[67], or conversely, reluctance driven by the fear of a machine's substitutive effect or the individual clinician's cultural and educational context. New roles might emerge in the organisation. In fact, specialized skills aimed at preventing malfunctions or safely activating functionality restoration plans in case of defaults should be associated with the development of intervention capabilities in a domain that is different from the healthcare one. The composition of the staff - and thus the work shifts - should also take into account, the greater or lesser predisposition to use the new tool to avoid negatively impacting the quality of delivered services.[68]

In addition to outpatient activities, new technologies are increasingly finding their place in surgery rooms. In fact, advances in the field of surgical robotics guarantee the execution of specific tasks with high standards of precision and accuracy through the supervision of the healthcare professional guiding the device. Thus, representations of virtual environments allow for the planning of increasingly complex procedures and anticipate, through simulation, the possible consequences of certain actions and choices in the virtual twin scenario, thereby increasing the level of accuracy of the procedure and significantly reducing the chances of error and, consequently, of harms for patients.

From the patient's perspective, in order to create the digital twin of the operating room setting, at least the recording and reproduction of vital conditions and parameters shall be expected as the data processing activity necessary to perform the surgery. Therefore, information systems must guarantee the availability, integrity, and confidentiality of data flows to prevent, for example, patient-related values from short-circuiting or being replicated on machines associated with other subjects, or to ensure interoperability of communications when the assembly with other tools is neces-

67 Committee on Social Affairs, Health and Sustainable Development, *Artificial intelligence in health care: medical, legal and ethical challenges ahead*, 2020 <http://www.assembly.coe.int/LifeRay/SOC/Pdf/TextesProvisoires/2020/20200922-HealthCareAI-EN.pdf>.

68 European Parliamentary Research Service, *Artificial intelligence in healthcare*, 2022 <https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729512/EPRS_STU(2022)729512_EN.pdf>.

sary. The risks related to privacy protection must, therefore, be assessed, mitigated, and monitored not only at the time of the introduction of the digital twin system in the operating room, but also during individual procedures[69]. It is necessary, in fact, for a series of parameters to be continuously monitored to ensure the functionality of the system, so that reality becomes computable, communications more flexible, and processes optimized. In particular, the management of the virtual space must be robust and reliable, providing high standards of security in the authorization architecture for performing individual operations, as well as contractual clauses capable of allocating roles and responsibilities, while maintaining an appropriate level of confidentiality for the nature of the data being processed.[70]

Among the advantages of using such technologies, considering the position of the surgeon and their respective staff, ergonomic comfort during the operation stands out. This leads to better precision of movements, reducing the likelihood of tremors, and also facilitates access to anatomically challenging areas, thanks to the possibility of having a three-dimensional or augmented representation of the surgical site. However, a new digital vulnerability to be addressed concerns the gap between perception and reality in the virtual or augmented environment, which may be experienced differently by the operator depending on their physical and/or emotional conditions. Studies in this field emphasize the need to assess the reliability and validity of the system through tests that highlight the behaviours of the operators when interacting with virtual reality.[71] This helps identifying the suitability requirements for operators to safely use digital twin technology.

The benefits for the patient, indeed, are related to the accuracy and precision of the machine: generally, minimal incisions limit post-operative effects (such as pain, infections, etc.) and reduce recovery times, including

69 V. Damjanovic-Behrendt, *A Digital Twin-based Privacy Enhancement Mechanism for the Automotive Industry*, *in International Conference on Intelligent Systems (IS)*, Funchal, Portugal, 2018, 272-279, doi: 10.1109/IS.2018.8710526, Z. Chen, J. Wu, W. Gan and Z. Qi, *Metaverse Security and Privacy: An Overview*, *in IEEE International Conference on Big Data (Big Data)*, Osaka, Japan, 2022, 2950-2959, doi: 10.1109/BigData55660.2022.10021112.

70 C. Alcaraz - J. Lopez, *Digital Twin: A Comprehensive Survey of Security Threats*, in *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, 1475-1503, third quarter, 2022, doi: 10.1109/COMST.2022.3171465.

71 D. R. Sanchez, E. Weiner, A. Van Zelderlend, *Virtual reality assessments (VRAs): Exploring the reliability and validity of evaluations in VR*, https://doi.org/10.1111/ijsa.12369; E. Weiner - D. R. Sanchez, *Cognitive ability in virtual reality: Validity evidence for VR game-based assessments* <https://doi.org/10.1111/ijsa.12295>.

hospitalization. Again, the role of technical standards is paramount to develop procedure able to fulfil ethical and legal requirements for a trustworthy use of digitalised healthcare services.[72] All of these remarks are true in an ideal scenario where the healthcare professional-machine relationship is well-established and accepted.

Another critical aspect that arises in the digitalisation of healthcare services is related to the reuse of collected information for screening purposes. As mentioned for the emergencies, also in these cases, it is necessary to identify the legal basis that can justify the reuse of data collected for healthcare purposes and design an effective governance for information access and sharing. These activities usually require the development of digital platforms and infrastructures capable to securely managing incoming and outgoing flows, identifying roles and responsibilities to comply with regulatory obligations, including the need for pseudonymization, allocation of access and sharing privileges, or performing activities.[73]

In this regard, the proposed regulation for a European Common Space for Health Data states that there must be a separation between those ones who generate the data, those who manage them, and those who request access for reuse. This is to ensure the anonymity of patients (data subjects) whose pseudonymized data, through subsequent processing, could potentially enable re-identification.

The mediation of the clinician-patient alliance through human-machine interfaces is particularly evident within telemedicine scenarios, where it is applied through remote communication for the collection of those parameters, which, if connected to mobile phone applications and/or wearable devices, may gather information, process it, and allow - with the clinician's validation - to provide prescriptions, dosages, instructions for the continuation of treatment or rehabilitation pathways, etc., in other words, to remotely deliver supporting healthcare services.[74] Boundaries on the nature

72 Wen Sun et al., An Introduction to Digital Twin Standards, GetMobile: Mobile Computing and Communications, Volume 26, Issue 3, September 2022,16–22 <https://doi.org/10.1145/3568113.3568119>.

73 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, 144.

74 See the EU Commission Communication COM(2008)689; Italian Ministry of Health, *Telemedicina. Linee di indirizzo nazionale* <https://www.salute.gov.it/imgs/C_17_pubblicazioni_2129_allegato.pdf>; Istituto Superiore Sanità instructions, *Indicazioni ad interim per servizi assistenziali di telemedicina durante l'emergenza*

of the healthcare services, for example, have been included in tailored guidelines[75], like the Italian ones identifying technical and organisational safeguards to frame telemedicine: from the assessment on possible cultural, digital, environmental barriers for the patient by the clinician, to the certifications required to the adopted software.[76] In fact, access to a stable internet connection, proven interoperability of the healthcare software with the operating system installed on the patient's devices, the presence of system recovery mechanisms in case of power outages, confirmed presence of antivirus software to prevent unauthorized access, are just some of the elements to be considered for the activation of such telemedicine services. Furthermore, the effectiveness of technological innovation will be as efficient as the patient (or the caregiver) is able to correctly perform the procedures. Therefore, if the patient demonstrates the ability to wear the device properly, set up the collection and transmission of information following the provided instructions, and, last but not least, manage and understand digital communication to continue treatment.[77] The digital divide shall be considered as *a priori* obstacle to the prescription of telemedicine support, considering the appropriateness standards of care[78]. Within this framework, the role of the vulnerable subjects, namely the patients, can be enriched with new aspects that make them more involved, aware, and an active leading actors in their own care journey.

sanitaria COVID-19, 12/2020 <https://www.iff.it/documents/20126/0/Rapporto+ISS+COVID-19+n.+12_2020+telemedicina.pdf/387420ca-0b5d-ab65-b60d-9fa426d2b2c7?t=1587114370414>.

75 Italian Ministry Decree, 21.09.2022 recante *Approvazione delle linee guida per i servizi di telemedicina - Requisiti funzionali e livelli di servizio.*

76 A. Sorrentino; L. Fiorini; G. Mancioppi; F. Cavallo; A. Umbrico; A. Cesta; A. Orlandini, *Personalizing Care Through Robotic Assistance and Clinical Supervision*, in *Frontiers in Robotics and AI*, 2022 <https://www.frontiersin.org/articles/10.3389/frobt.2022.883814/full>.

77 From this concept we may shape the content of the principle of appropriateness in healthcare, see AA.VV., M. Sesta (ed.), *L'erogazione della prestazione medica tra diritto alla salute, principio di autodeterminazione e gestione ottimale delle risorse sanitarie*, Maggioli, 2014.

78 See G. Finocchiaro, *Intelligenza artificiale e responsabilità*, in *Contr. impr.*, 2020, 724; U. Salanitro, *Intelligenza artificiale e responsabilità: la strategia della commissione europea*, in *Riv. dir. civile*, 2020, 1246 f.; A. Fusaro, *Quale modello di responsabilità per la robotica avanzata? Riflessioni a margine del percorso europeo*, in *Nuova Giur. Civ. Comm.*, 2020, I, 1344 ff.

D. The interplay of technical and organisational standards to protect users

In the previous paragraphs, we have outlined some critical issues that can arise in a variety of scenarios where the provision of digital services and products are addressed to vulnerable users, like children, and patients. We identified risks to be mitigated in relation to data flows capable of exposing persons to new vulnerabilities and assessed the critical issues for those individuals who are not normally considered as vulnerable – such as adults, parents, caregivers, and clinicians – when they become so in relation to technological innovation, for example, due to a lack of knowledge or awareness of specific risks related to the digital dimension of their activities or of the ones performed by vulnerable persons they are taking care of. We also analysed how the exposure to the risk of compromising fundamental rights increases for individuals who are already vulnerable – such as patients – for various reasons, such as the potential loss of control over the information concerning them that are more easily exploitable in the digital environment than in the physical one.[79]

Furthermore, we deepened the fact that despite the risks associated with the digitalization and innovation of services and products, the scope of opportunities is disruptive not only in the clinical and scientific fields – where advances in time and quality of diagnosis, treatment, and care are already proven – but also in terms of access to culture, inclusion and education as a societal revolution, looking especially at children, as the citizens of tomorrow. This result is confirmed where multiple vulnerabilities shall be overcome in the same context, like in case of disabled children care and education sector: the data-driven society may strongly improve their quality of life, making the difference in terms of personalised services and inclusion strategies.[80]

In the data economy, as illustrated, the reuse of information serves as an asset to boost innovation in every sector. The impact of the digital transition on services and products deals with a series of aspects, touching both digital vulnerabilities and the vulnerabilities in the digital environment. To this end, the development of technical standards may improve not only the performance – and therefore the quality- of services and products, but it may also increase the trustworthiness in terms of ethical and legal

79 J. Van De Hoven et al., *Towards a Digital Ecosystem of Trust: Ethical, Legal and Societal Implications*, in *Opinio Juris in Comparatione*, 2021, 131 ff.

80 UNICEF, *Global report on assistive technologies*, 2015 <https://www.unicef-irc.org/children-with-disabilities>.

compliance with the key values and principles that may find in specific procedures and workflows a new methodological approach to assess the impact of a given solution and application on users' fundamental rights.

In research, development, and innovation, the methodology consists of the identification of technical specifications, solution development, and assessment in terms of acceptability and usability among users, the same workflow could be validated by associating to each step an impact assessment in order to define legal requirements, to identify (and maintain coherent) roles and responsibilities within the organizations involved in each step of the development, to design training requirements for users considering their grounds of vulnerability, and share awareness pursuing pre-determined goals for the other relevant stakeholders in order to better harmonise the introduction of the digitalization in the given supply chain.

The iteration of a similar life-cycle describes a new standard of professional diligence that might be considered as a general obligation to addressing vulnerabilities in the given scenario beyond the existence of specific enforceable regulatory tools, setting legal obligations to comply with. In fact, like the technical standards, also the ethical and legal ones might just be globally absorbed in the development cycle and market placement as a pre-requirement to pursuing shared values and needs with the objective to achieve a more inclusive and non-discriminatory society to boost the data economy.