LA REVUE DES JURISTES DE SCIENCES PO

Direction scientifique :
Beatriz BOTERO ARCILA et Lucas COSTA DOS ANJOS
Rédacteurs en chef :
Octavie JACQUET et Giorgio GUGLIOTTA

FÉVRIER 2024 - **N°25**
15e ANNÉE - ISSN 2111-4293

▶ Dossier thématique

Law and Technology : Towards a New Digital Rule of Law

LexisNexis

SciencesPo
ÉCOLE DE DROIT

Sommaire

1 Édito

Octavie Jacquet,
Rédactrice en chef,
Étudiante au sein de l'École de droit

Giorgio Gugliotta,
Rédacteur en chef,
Étudiant au sein de l'École de droit

Chères lectrices, Chers lecteurs,
Nous sommes très heureux de vous présenter ce nouveau numéro de la *Revue des Juristes de Sciences Po* consacré au thème des interactions entre nouvelles technologies et droit, avec pour Directeurs scientifiques les Professeurs Botero Arcila et Costa dos Anjos.
En 1997, Richard Susskind soulignait déjà la nature révolutionnaire des défis posés par l'innovation technologique dans son ouvrage *The Future of Law : Facing the Challenges of Information Technology*. Plus de vingt ans plus tard, ce numéro de la Revue tente de donner un tour d'horizon de l'architecture réglementaire actuelle, développée autour de nouvelles technologies numériques en constante évolution, ainsi qu'à mettre en lumière certains défis majeurs que les derniers développements ont entraînés. De manière plus significative, ce numéro tente de démontrer que les interactions entre droit et technologie peuvent certes aboutir, pour reprendre les mots de Lawrence Lessig, à *« une sorte de réglementation de la créativité que nous n'avons pas vue auparavant »* ; mais que, d'autre part, elles engendrent par ailleurs une créativité unique en matière de réglementation et d'encadrement de ces technologies. Le numéro actuel suit ainsi la ligne directrice tracée par le troisième numéro de la Revue de Janvier 2011. Celui-ci, consacré au sujet du droit et de l'innovation, s'interrogeait sur *« le début de la fin »* anticipé par Susskind dans l'ouvrage *The End of Lawyers*. En outre, il appelait à une mise à jour essentielle plus de dix ans après. Bien qu'il ne prétende pas être exhaustif, objectif sisyphéen en matière de nouvelles technologies, ce dernier numéro se concentre plutôt sur des problématiques spécifiques, telles que les accords de libre échange, la propriété intellectuelle, ou encore la réglementation de l'Intelligence Artificielle. Il cherche enfin à susciter une réflexion critique au sujet des nouveaux défis que ces nouvelles technologies ne cessent de soulever.
Les articles proposés ont été rédigés par un groupe de contributeurs d'une grande diversité, aussi bien en ce qui concerne leur nationalité que leur parcours académique et professionnel. Cette diversité sans précédent trouve son expression plus immédiate dans la nature profondément bilingue de ce numéro, qui propose exceptionnellement plus de contributions en anglais qu'en français. Elle est d'ailleurs le reflet direct de nos différents parcours et nationalités en tant que Rédacteurs en Chef de cette édition. Pour cette raison, nous nous sentons cette fois obligés de nous adresser à nos lecteurs et contributeurs dans les deux langues. C'est ainsi que nous souhaitons vivement remercier les contributeurs qui ont participé à la rédaction du présent numéro, tout particulièrement pour l'excellence de leurs contributions et l'éclairage qu'ils apportent à un thème d'une actualité perpétuellement renouvelée et métamorphosée. Nous remercions aussi nos Directeurs scientifiques pour leur soutien et leurs précieux conseils dans l'élaboration de ce numéro. Enfin, nous remercions chaleureusement les membres du Comité de rédaction pour leur travail tout au long de la réalisation de la 25e édition de la *Revue des Juristes de Sciences Po*.
En vous souhaitant une excellente lecture !■ → Suite page 2

Revue des Juristes de Sciences Po
REVUE SEMESTRIELLE

Photo de couverture :
© Marta Nascimento / Sciences Po

Origine du papier : Allemagne
Taux de fibres recyclées : 6 %
Certification : 100 %
Impact sur l'eau : P_{TOT} = 0,01 kg / tonne

Imprimerie :
Evoluprint - Groupe Sprint
Parc Industriel Euronord
10 rue du Parc - 31150 Bruguières

Dear readers,

We are extremely happy to present this new issue of the *SciencesPo Law Review*, devoted to the subject of the interaction between law and technology, and featuring Professors Botero Arcila and Costa dos Anjos as Scientific Directors.

As early as 1997, Richard Susskind was underlining the revolutionary nature of the challenges posed by technological innovation in a book called " *The Future of Law : Facing the Challenges of Information Technology* ". More than twenty years later, this issue seeks to offer a snapshot of the current regulatory paradigm around ever-changing new digital technologies, as well as bring to light some major - or sometimes less thought-about - challenges that the latest developments have entailed. Significantly, it tries to demonstrate that law and technology together might indeed result in " *a kind of regulation of creativity we've not seen before* ", in Lawrence Lessig's words, but it most importantly produces a unique creativity of regulation. This issue also positions itself in the legacy of a previous issue of the Review (n° 3 of January 2011), dedicated to law and innovation, that questioned the " *beginning of the end* " anticipated by Susskind in the *The End of Lawyers*, and that called for a much-needed update after ten years. Far from having the pretension of being exhaustive, this issue focuses on specific topics such as trade agreements, intellectual property or Artificial Intelligence regulations, and seeks to trigger some critical thinking about the new challenges these technologies keep on raising.

Rarely, in the history of our Law Review, the articles proposed have been authored by a pool of contributors so diverse, both in terms of academic, professional, and national backgrounds. This unique diversity of inputs finds its first and most immediate expression in the markedly bilingual nature of the present issue, exceptionally featuring more contributions in English than in French. Such diversity is perhaps more directly embodied by our different personal and academic backgrounds as Co-Editors in Chief of this issue.

For this reason, we felt bound to address our readership, on this specific occasion, in both languages. Thus, we wish to express our gratitude to all the contributors who have taken part in the preparation of this present issue. We would like to thank them particularly for the excellence of their contributions, as well as for the insight that they have provided into a subject whose enduring relevance is persistently marked by novelty and change. We thank our Scientific Directors for their support and precious advice during the development of this issue. We would finally like to thank the members of our Editorial Board for their patient participation in the development of this 25th issue of the *SciencesPo Law Review*.

En vous souhaitant une excellente lecture !■

LES AUTEURS

Frédérique Berrod : est professeure de droit de l'Union européenne à Science Po Strasbourg depuis septembre 2008. Elle est titulaire d'une chaire Jean Monnet depuis décembre 2021, consacrée aux « Narratifs européens de la Frontière » (NEFLAW). Elle est spécialisée dans l'enseignement du droit de l'Union européenne (droit institutionnel de l'UE, droit du marché intérieur, droit de la concurrence, droit des frontières, droit de l'énergie, droit des produits de santé, droit du marché intérieur numérique, droit des données en Europe) et responsable du Master 2 « Droit des produits de santé en Europe » à la Faculté de droit de Strasbourg.
Elle est membre du Centre des études Internationales et européennes (EA 7307) et du centre d'excellence franco-allemand Jean Monnet et du réseau international d'excellence Jean Monnet FRONTEM. Ses champs de recherche s'étendent de l'espace européen de l'énergie, à l'Europe des produits de santé et au marché intérieur numérique et aux frontières en Europe. Elle développe des recherches sur les articulations normatives entre les conventions du Conseil de l'Europe et le droit de l'Union européenne.

Beatriz Botero Arcila : is Assistant Professor of Law at Sciences Po Law School in law and technology and a Faculty Associate at the Berkman Klein Center for Internet and Society at Harvard University. She holds a doctorate from Harvard Law School where she defended a dissertation on the governance of smart cities and urban platforms and the data they collect. Her research and work focus on the governance of data and artificial intelligence. Recent work has focused on the governance of public data, data sharing agreements, AI liability and generative AI.

Mirra Burri : is Professor of International Economic and Internet Law at the Faculty of Law of the University of Lucerne, Switzerland. She teaches international intellectual property, media, internet and trade law. Mira's current research interests are in the areas of digital trade, culture, copyright, data protection and data governance. Mira is the principal investigator of the project 'Trade Law 4.0' (ERC Consolidator Grant 2021–2026). She consults the European Parliament, UNESCO, ASEAN, the WEF and others on issues of digital innovation. Mira is also a member of the Research Council of the Swiss National Science Foundation.

Julien Cabay : is Professor at Université Libre de Bruxelles (ULB) where he holds the Chair in Intellectual Creation and Innovation Law and is Director of JurisLab, a research unit of the Center for private law located in the FabLab ULB. He is also Associate Professor at Université de Liège (ULiège), where he teaches in the LL.M. in IP & Competition Law organized by the EU Legal Studies Institute. Next to his main affiliations, he is Invited Professor (Gastdocent) at KULeuven (Master of IP; ICT Law), Invited Professor at Centre d'études internationales de la propriété intellectuelle (CEIPI) of University of Strasbourg (University Diploma in AI & IP), Lecturer at Brussels School of Artificial Intelligence (Executive Master in Law & AI), Affiliated Researcher at Digital Law Center (DLC) of University of Geneva and member of the Belgian Council for Intellectual Property. In the past, he has been Research Fellow (2010-2014) and PostDoc Researcher at National Fund for Scientific Research (2016-2020), Visiting Research Fellow at Columbia University in the City of New York (2012-2013) and Global Policy Fellow at Instituto de Tecnologia e Sociedade do Rio de Janeiro (2018). His main fields of expertise are Copyright Law; AI & IP; Fundamental Rights & IP; IP & Open Science.

Lucas Costa dos Anjos : is a postdoctoral research fellow in the New Digital Rule of Law project, and Coordinator of the Digilaw Clinic, at Sciences Po Paris École de Droit, with a focus on algorithmic transparency and AI regulation, specially from a Global South perspective. He is a data protection specialist at the Brazilian Data Protection Authority - ANPD, an affiliated researcher at JurisLab, at Université libre de Bruxelles and an Associate Professor in the Law Department of Universidade Federal de Juiz de Fora, in Brazil. He holds a PhD in Law from Université libre de Bruxelles and Universidade Federal de Minas Gerais, under joint supervision. He is also the founder and was a scientific advisor of the Institute for Research on Internet and Society - IRIS, an internet governance non-governmental organization.

Rangita de Silva de Alwis : is a Professor and an expert on the treaty body to the UN Convention on the Elimination of All Discrimination Against Women (CEDAW) and the Women, Peace and Security Focal Point. At the University of Pennsylvania Law School, where she is faculty, she teaches International Women's Rights; Women, Law, and Leadership; and the Policy Lab, including the Policy Lab on AI and Bias, and directs the Global Institute for Human Rights. She also teaches Globalization and Human Rights at the Wharton School of Business and Women, Peace and security at the Harvard Kennedy School of Government. She will be a Visiting Fellow at the Oxford University Bonovero Institute on Human Rights in 2024.
In recognition of Rangita's global work in advancing women's rights, she was named the Hillary Rodham Clinton Distinguished Fellow on Gender Equity, Georgetown Institute for Women, Peace and Security. She is also a Senior Fellow at the Harvard Law School Centre for Legal Profession.

Séverine Dusollier : is Professor of Intellectual Property in the Law School of Sciences Po Paris and holds a Senior Chair at the Institut Universitaire de France. She is the director of the law school research centre, member of its doctoral committee and the Head of the Master in Innovation Law. Recognised as an international expert in copyright, she is a Qualified Member of the CSPLA (French Copyright Council) and a founding member of the European Copyright Society. From 2014-2019, she was the holder of an ERC (European Research Council) research grant on commons and inclusivity in property. Her current research interests are digital issues of copyright, the concept of authorship, contractual protection of authors and performers, exceptions and limitations, commons and property, public domain.

Giorgio Gugliotta : Rédacteur en chef, étudiant à l'Ecole de droit

Octavie Jacquet : Rédacteur en chef, étudiante à l'Ecole de droit

Emma James : is currently a Masters Student at Sciences Po Paris School of International Affairs, where she is majoring in International Governance and Diplomacy.

Gregory Lewkowicz : is a professor at the Université libre de Bruxells, director of the Smart Law Hub ans member of the Perelman Centre. He is a principal investigator at the AI for the Common Good Institute (FARI) in Brussels. His research focus on the interactions between law & digital technology and the emergence of SMART (Scientific, Mathematical, Algorithmic, Risk and Technology-driven) Law.

Federica Paolucci : is Ph.D. Candidate at Bocconi University.

Oreste Pollicino : is a Professor of Constitutional Law and Media Law at Bocconi University. He is a Senior Emile Noele Global Fellow at the New York University.

Sarah Roman-Jakob : is a legal professional with a Juris Doctor from Northwestern Pritzker School of Law and a Master's in Economic Law from Sciences Po Law School, with a keen interest law and technology. As part of the inaugural year of Sciences Po's Digilaw Clinic, Sarah actively engaged in research projects addressing the complexities of AI and digital identity. Sarah is now a practicing lawyer in New York.

Ritha Sarf : is a graduate of Sciences Po Law School with an undergraduate degree in Finance and Business Analytics from McGill University. With a multidisciplinary background, she is interested in bridging the gap between law and technology as the latter grows to affect all fields. She strives to meaningfully analyze the complexities at play in order to inform socially robust tech policy and guide companies in fostering mindful innovation with a lense calibrated toward fairness and justice.

Bernard Stirn : entré au Conseil d'État en 1976, Bernard Stirn y a présidé la section du contentieux de 2006 à 2018. Enseignant à Sciences Po de 1976 à 2023, il est l'auteur de nombreux ouvrages, notamment les Libertés en questions (13 ème édition en 2023). Il a également présidé le conseil d'administration de l'Opéra national de Paris de 2001 à 2018. Élu en 2019 à l'Académie des sciences morales et politiques, il en est le secrétaire perpétuel depuis 2023.

LES AUTEURS

Oliver Sylvain : is a Professor of Law at Fordham University and a Senior Policy Research Fellow at Columbia University's Knight First Amendment Institute. His research is in information and communications law and policy. His most recent writing, scholarship, and public speaking engagements are on online intermediary liability, commercial surveillance, artificial intelligence, and community-owned networked computing. The National Science Foundation and the John S. and James L. Knight Foundation have awarded him grants to support this work. He was a Senior Advisor to the Chair of the Federal Trade Commission from 2021 to 2023.
Olivier teaches Legislation and Regulation, Administrative Law, Information Law, U.S. Data Protection Law and Privacy, and information law related courses. At Fordham, he has been the Director of the McGannon Center for Communications Research, the Academic Director of the Center for Law and Information Policy, and a research affiliate at the Center on Race, Law, and Justice. Before entering academia, Olivier was a Karpatkin Fellow in the National Legal Office of the American Civil Liberties Union in New York City and a litigation associate at Jenner & Block, LLC, in Washington, D.C. Until September 2021, he was the Board President of the ACLU's New York affiliate and sat on the Academic Advisory Board for the Open Markets Institute and the Advisory Committee for the Cyber Civil Rights Initiative.

Julia Vieira : a Brazilian lawyer and Sciences Po Law School alumna, has a Master's in Economic Law with a focus on Global Governance Studies. She was part of the first cohort at the Digilaw Legal Clinic at Sciences Po, where her interest lies at the intersection of law, technology, and society. Julia's diverse interests in cinema, soccer, and politics enhance her perspective on societal issues in her legal career.

Perspectives

2 Bytes & Pieces : Reflections on Digital Identity

Sarah ROMAN-JAKOB

Julia VIEIRA

Emma JAMES,
DIGILAW Clinic, SciencesPo Law School

XXX
900109
90100009
900010019
90100009
9 001 9
0
0010001000000100001
0100 1100100000000 0010
0001 0000100010 1000
000 001000001 001
010 10010001 000
01 0101010 01
0 011100 0
001000010
100000100100
000100110001000
00101100000100000
001011000001000011 00
000011000111001000000 00
0010001001010100100000000
0101000010101010000000000

1 - " Bytes and Pieces " admits an image of something unconstructed and not fully known. From fragmentary form, one may be able to construct the whole, yielding their own power to bring the pieces together. The same notion applies to construction in a digital world but building with bytes instead of physical bits.

Constructing and deconstructing collective and individual identities is part of the human experience. This booklet will invite the reader to reflect, learn, and question the use of their digital identity, beginning as virtual bytes that reverberate into physical realities. While identity is layered and malleable, for the purposes of this project, the term " digital identity ", as defined by the authors, refers to digital information and data that can be used to identify natural or legal persons online including identity attributes like personal information, behavior, and digital footprints.

The first article will argue the existence of power imbalances within public-private entity relationships when applied to the individual identity construction context. The second article will explore data exploitation mechanisms that weaken individual autonomy through examining online dating services. The third article interrogates digital identity use and data privacy of " i-voting " (internet voting) in Estonia. The articles will address risks such as the use of digital identity to allow or obstruct access to state resources, invasion of privacy, exploitation of data, or risks to democratic participation. The public (e-Estonia), private (dating apps), and public-private (government-corporate partners) sectors, build power through digital identity construction and management in multitudinous ways. The goal is not to find an all-encompassing solution to these issues facing digital identity, but to provoke intro and extrospection as each of us are confronted with a rapidly changing world.

These reflections in bytes and pieces were brought together by three students at the Paris Institute of Political Studies, Sciences Po. They were built throughout the academic year in meetings, classrooms, and virtual rooms with the hope of learning what digital identity means not only within an academic context but also with regards to our own digital existence. Fruitful discussions between different nationalities and experiences converged into the pieces you will engage with below. We hope the reader will hear the echoes of both the optimism and apprehension that we faced regarding digital identity both in writing and looking into our own futures.

Finally, we are immensely grateful to our faculty and mentors at Sciences Po and The Institute for Technology in the Public Interest (TITiPI) for all the guidance and encouragement they provided throughout this process.

3 Constructing Digital Identities : Examining the Public and Private Role in Digital Identity Construction

Sarah ROMAN-JAKOB,
DIGILAW Clinic, SciencesPo Law School

1 - " I think, therefore I am " [1]. A Cartesian quote floating under the bolded letters of a name constructed specifically for an individual's social media profile, seeming at once enlightened and pedantic. Descartes' famous concept of consciousness, later bled into concepts like philosopher Derek Parfit's psychological continuity [2]. Psychological continuity is the idea that while our own identity appears singular to ourselves, identity exists in the realms of an individual's personality, amassed experience, memories, psychological states, and therefore is not a singular unified self, but an amalgamation of these and other factors meeting at a variety of crossroads throughout one's life [3]. Individuals are not an unchanging Cartesian soul, but an accumulation of our experiences that gives us the impression of psychological continuity ; that we exist as one being in the world [4]. Psychological continuity is one way to understand the self and how we construct our identity in our own mind, how one differentiates the self from the other. This article argues that the ability of individuals to exercise their power to construct or manage their own identity based on their own self-perception or psychological continuity is an inherent power. Likewise, when others, such as a government or a private actor, construct or manipulate individuals identities, this is similarly an exercise of power.

While psychological continuity creates the impression of a singularly defined self, our identity is in fact malleable and illusive. That malleability translates online through different avenues between a mixture of identity attributes. Identity attributes might be a name, email, race, religion, driver's license number, employment, or even personality traits. The lines between online personae, behavioral information, and identity as perceived by distinct others like community, corporations, or governments, often intermix with one another, only adding to the complexity. Though, the ability to exercise control over any identity or personal attributes, controlling who can access the identity information, which attributes are disclosed, and what the attributes mean to different actors, is power. Those that can leverage their positive identity attributes to their benefit online have a better chance of accessing public resources, creating wealth, and obtaining a dignified standard of living. An exercise of the power of identity management might mean the ability to identify as a sex worker in one space and not in another, or a dual citizen who can identify as an EU or non-EU citizen.

To further illustrate, consider artist JLo who starred in the movie Hustlers where she portrayed Ramona, a pole dancer from the Bronx [5]. She further posted a nude photo on Instagram and articles responded with titles such as, " Jennifer Lopez Drops a Cute Nude Photo on Instagram for Her 53rd Birthday " [6]. At the same time, pole dance creators struggled to identify themselves and share their content online, with little to no news reporting on the topic. Instagram blocked videos or images which included a pole, regardless of how the content creators were dressed.

While technology has allowed some to benefit from their ability to maintain and control their digital identity, for others it has created obstructions to financial resources or stigma.

Individuals and communities further share identity construction and management with both public and private actors. This matters because identity decisions can have severe implications for an individual's quality of life. Modern state organization compels public actors to set out certain attributes associated with identity and use them in a uniform way to identify citizens. The state wants to make the individual uniquely identifiable by constructing attributes and attaching them to individuals or communities. This may include attributes like ethnicity, a social benefits number, or a credit score. The state uses this individual or collective identity data to determine access to the state's resources or territory ; whether that be medical coverage, education, or the ability to reside within the state's borders. There are benefits and risks to this system. An individual may want to be identifiable to the state for available state resources. Another individual who engages in undocumented migrant work might want to remain unidentifiable to the state. Giving up the power to privately determine which identity attributes are public, and who can use them under which circumstances, can mean access or obstruction to resources. For an EU resident it may mean resource access ; for a Syrian refugee it may mean resource obstruction.

Just like public actors, private actors also construct individuals identities for their own purposes. Private actors use similar identity attributes, building on many categories already constructed by the state or individual. For example, within the financial services sector, private and public actors often interact in the management

1. Vijay Shankar Balakrishnan, " The Birth of Consciousness : I think, therefore I am ? ", *The Lancet Neurology*, Vol. 17, no. 5, 402 (2018).
2. Nora Schreier et al., " The Digital Avatar on a Blockchain : E-Identity, Anonymity and Human Dignity ", *ALJ Austrian Law Journal*, Volume 8, 203-204 (2021).
3. Derek Parfit, " Personal Identity ", *The Philosophical Review*, Vol. 80, no. 3, 3 (1971).
4. *Id.*
5. Julie Miller, " I Wasn't That Impressed : Hustlers' Real-Life Ramona Reviews the Film ", *Vanity Fair* (Sept. 16, 2019), https://www.vanityfair.com/hollywood/2019/09/hustlers-the-movie-jennifer-lopez-real-life.
6. Alyssa Bailey, " Jennifer Lopez Drops Cute Nude Photos from Her 'Marry Me' Music Video Shoot "*Cosmopolitan*, *Yahoo Life*, (Feb. 11, 2022), https://www.yahoo.com/lifestyle/jennifer-lopez-drops-cute-nude-154300597.html.

of an individual's identity. The public sector relies heavily on banks in the private sector to support individuals access to personal and mortgage lending, tax refunds, and general money and wealth management. Of course, private actors fulfill these roles for the benefit of the customers gained and profits made through government contracts. The following section will analyze one specific private entity, LoanLink24 online mortgage services, to better understand the ways in which private actors work as agents of the public sector in constructing the digital identity of their customers. It will also demonstrate that private use of digital identity, even when private actors are acting as agents of the public, can create obstruction to resources like government-supported access to housing. Finally, the article will conclude by arguing there will be an expansion of this public-private relationship under the new EU Regulation on Digital Identity.

This article argues that constructing identity, either by oneself or by the other, is a power. New relationships between the public and private sector threaten to create unique challenges to an individual's power to construct and manage their own identity, particularly their digital identity. The power imbalances stemming from public-private joint action in identity construction increase individual's risk of digital identity misuse and mismanagement. The public and private sectors' joint usurpation of identity construction creates barriers to that individual's power to meet their own needs and achieve a standard of living that promotes the dignity of the individual and increases reliance on both public and private actors.

1. Examining the Public-Private Connection in Digital Identity Construction

2 - Mortgage brokers serve as one of the state's agents in distributing public resources to individuals through private means and play an important role as gatekeepers of housing and general socio-economic mobility. As Article 25 of the Universal Declaration of Human Rights states : " Everyone has the right to a standard of living adequate for (...) housing and medical care and necessary social services " [7]. While the public sector may be responsible for ensuring minimum standards against homelessness and general access to housing, quality of life often lies outside of meeting minimum standards. Just beyond survival housing, private actors come in and fill the large gap of financing needs public actors do not provide. While housing is generally considered a fundamental right, a private actor's decisions can widely impact what quality of home an individual can access based on their identity and personal attributes. One of those private actors is LoanLink24. LoanLink24 is a German online-only mortgage brokerage founded in 2017 which claims to leverage " advanced algorithms to compare and track mortgage products from over 400 lenders ", enabling clients to make informed and unbiased financial decisions [8].

Loanlink24 is one of the mortgage brokers responsible for creating access to public resources, such as German KfW loans (*Kreditanstalt für Wiederaufbau*). KfW Development Bank is a German state-owned development bank which offers a range of loans for initiatives in Germany, including home mortgages [9]. A KfW loan comes at a lower-than-market interest rate for those who want to purchase or build a home [10]. This example is important as banking and financial services increasingly move online [11]. LoanLink24 gages an individual's general mortgage suitability by using an online mortgage quiz [12]. The quiz presents a variety of identity questions submitted digitally. In *Table 1*, fictional borrowers were created and given the same identity attributes with the exception of residency. Person 1 was made a non-EU resident and Person 2 was made an EU resident.

	Live-in Owner/ Lessor	Residency	Value of Property	Minimum Down Payment Required by LoanLink	Living Status	Employment	Minimum Monthly Income Required by LoanLink
Person 1	Live-in Owner	Non-EU Resident	300.000 €	117.210 €	Living Alone	Employed	3.750 €
Person 2	Live-in Owner	EU Resident	300.000 €	30.210 €	Living Alone	Employed	2.778 €

Mortgage Table 1

LoanLink24 helps establish which identity attributes, like credit score or residence, create a " good " KfW loan candidate. It is important to reflect here and recognize the extent to which an individual's online digital identity can impact the quality of their life and socio-economic mobility.

Consider findings from this OECD research report [13] :

- " Low homeownership countries exhibit high wealth inequality, even when income inequality is low "
- Beyond economic considerations, the report also found " access to mortgage markets allows credit constrained households a better chance of owning their own home "
- Public policy tends to favor homeowners to renters, and politically, the median voter in many countries is a homeowner

Therefore, creating barriers to mortgages can directly affect wealth accumulation, political and civic participation, and general life quality.

As a private actor, LoanLink24's action to raise barriers of access for non-EU residents may harm individual goals of home ownership. One can clearly see that changing a single identity factor, EU resident or non-resident, drastically changes an individual's ability to afford their own home via LoanLink24 mortgage. The results of the quiz show that a non-EU resident needs to have €87.000 additional cash or savings immediately available for

7. United Nations, *Universal Declaration of Human Rights*, Article 25 (1948), https://www.un.org/en/about-us/universal-declaration-of-human-rights.
8. As of publishing, the company LoanLink24 has since been acquired for an undisclosed amount by Baufi24. See *LoanLink24*, https://www.loanlink24.com/about-us/.
9. KfW Entwicklungsbank, https://www.kfw-entwicklungsbank.de/International-financing/KfW-Entwicklungsbank/.
10. LoanLink24, " Mortgage Calculator ", https://www.loanlink24.com/mortgage-calculator/repayment-calculator.
11. *"There has been a significant increase in the use of mobile phones and the internet to conduct financial transactions. Between 2014 and 2017, this has contributed to a rise in the share of account owners sending or receiving payments digitally from 67 percent to 76 percent globally, and in the developing world from 57 percent to 70 percent. "* The World Bank, press release, " Financial Inclusion on the Rise, But Gaps Remain, Global Findex Database Shows " (Apr. 19, 2018), https://www.worldbank.org/en/news/press-release/2018/04/19/financial-inclusion-on-the-rise-but-gaps-remain-global-findex-database-shows.
12. LoanLink24, " Financing Options Quiz, ", https://loanlink.finlink.de/start/finance_type ?primaryColor=92B726&sourceCalculatorUrl=https :%2F%2Fwidgets.finlink.de%2Fde%2Fbaufinanzierung-rechner%2Fbudgetrechner%3FprimaryColor%3D92B726&organization=loanlink&language=en&lang=en.
13. Orsetta Causa et al., " Housing, Wealth Accumulation and Wealth Distribution : Evidence and Stylized Facts ", *OECD Economics Department Working Papers*, no. 58, 9 (2019).

a down payment, without any explanation within the interface of the quiz as to how this decision is made.

Preferential treatment for EU residents has been cited for a variety of reasons. The Mortgage Credit Directive requires banks to take on heightened risks of exchange rate fluctuations [14], or banks cite the difficulty in accessing secured assets located in a different country [15]. Although, questions remain. How can the monetary difference in risk be as great as €87.000 ? The Directive does not require a 40% mandatory down payment, so how have private or semi-private institutions like the KfW Development Bank, and Loanlink24 as its agent, allowed this practice to flourish ? How can a government, implementing a mortgage program to assist in housing individuals pursuant to their fundamental rights, allow private banks and implementing mortgage brokers to take this much power in identifying who is worthy to receive a mortgage and under what conditions ?

For non-EU residents wanting to utilize LoanLink24 services and relinquish their digital identity information to apply for loans from over 400 German financial institutions listed on their website, the non-resident might be effectively barred from homeownership after a quiz which took little over 5 minutes to complete. When individuals have the power to construct or deconstruct their own identity attributes depending on the circumstances, this has a direct impact on their quality of life. Imagine fictional Person 3 is a French and UK citizen. They may have the right to utilize their identity attributes and act as a French citizen when purchasing a property through LoanLink24 in Germany. Then when that identity no longer suits them, they might leave the property, return to England, and become a lessor to a renter who cannot afford home ownership.

As a mortgage broker, LoanLink24 is monitoring and implementing the ideal identity of a mortgage candidate by choosing specific identity attributes and monitoring individual's responses. Additionally, it is important to recognize that this entire online process completely excludes individuals with no digital identity. Without an online presence and the power to offer one's identity online, an individual cannot access these online-only services. The ability to compare offers quickly and efficiently from so many German financial institutions all in one place increases an individual's chances of finding the best-priced mortgage. As a result, it increases their chances of homeownership. Consider populations like the elderly who don't have the skills or tools to access online identity, or other non-EU residents like migrant workers from outside of the EU : where does this growing online-only financial system leave them ?

Here, an individual's ability to control their identity, to offer it digitally, or to change it, is a power. Germany has a beneficial resource it needs to share with individuals seeking home ownership, aiming to house populations within Germany. Germany therefore has some power over the distribution of this resource and power to decide which identities benefit from it. This power has been further passed to LoanLink24, a new gatekeeper of this benefit. LoanLink24's decisions on what identity attributes create a low or high-risk borrower create barriers to individual power to access housing. Unlike walking into a bank, comparing loans and options from over 400 institutions through LoanLink24 creates better access to home ownership and socio-economic mobility. The fact that it is entirely digitized requires an individual to create and share their digital identity to access this service.

The following section will take this understanding and further examine the public-private relationship in the context of the proposed EU Regulation on Digital Identity. It will argue that the new regulation will take the existing public-private connection and expand and strengthen it through the creation of a new digital identity wallet for all EU citizens. Mandatory private participation in the EU digital identity wallet and engagement of additional private actors as agents of public actors will lead to the increased risk of obstruction to public resources, similar to risks seen with mortgages and access to housing.

2. Expanding the Public-Private Relationship through EU Digital Identity Regulation

3 - The public sector clearly relies on the private sector to distribute resources, and to identify individuals it deems to be suitable receivers of resources. With this existing relationship in mind, one might want to take a closer look at the upcoming developments in EU digital identity, particularly the EU Commission's proposal to amend Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market and establish a framework for a European Digital Identity (eIDAS). In 2021, the EU set out a vision for digital transformation of the Union by establishing " Europe's Digital Decade " [16]. The Digital Decade includes eIDAS, which aims to create an EU digital identity wallet for all members of the EU [17]. In the field of identity construction, a public actor in addition to a Member State, the EU, is also exerting its influence to promote this new concept of an EU-wide digital identity wallet. The wallet will include digitized versions of Member State distributed identities, such as passports, driver's licenses, or educational diplomas [18]. Additionally, the wallet is modeled after other private wallets, like the Apple Wallet, and has the technological capacity to contain credentials from the private sector such as prescriptions, banking cards, airplane tickets, or gym memberships [19].

These developments are important because they form new relationships between the public and private sectors that impact individual identity construction. Historically, individual Member States were responsible for creating and distributing identity attributes such as passport numbers or driver's licenses [20]. One pertinent and interesting debate in the eIDAS proposal was whether to establish an EU-wide identity number to all citizens of the EU [21]. The original proposal of eIDAS included this new identity number. However, Parliament, representing Member States, pushed back against this new assertion of power over identity construction [22]. In January 2023, the Commission released the " Toolbox for the Technological Blueprint of the EU Digital Walle " which dropped the EU identity number [23]. Instead, the Commission settled for digital forms of IDs established and managed by Member States to be placed in the

14. Directive 2014/17/EU on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/ ?uri=CELEX :32014L0017&rid=6.
15. Marcel Fafchamps, " Credit Constraints, Collateral and Lending to the Poor ", *Revue d'économie du développement*, Vol. 22, no. HS01, 72 (2014).
16. European Commission, " Europe's Digital Decade : digital targets for 2030 ", https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en#digital-rights-and-principles.
17. European Commission, " European Digital Identity ", https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en.
18. European Commission, " Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity ", 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/ ?uri=CELEX%3A52021PC0281.
19. Avast, " eIDAS 2.0 : Latest News & Progress, " *YouTube video*, 15 :34 (July 2022), https://www.youtube.com/watch ?v=NjmY5yiNu9k&t=934s.
20. European Commission, " Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity ", *op. cit*.
21. *Id.*
22. This issue was discussed by Cristian Terhes, a Romanian politician currently serving as a Member of the European Parliament for the Christian Democratic National Peasants' Party (PN?-CD) and serves as Parliament Committee Chair for the Committee on Civil Liberties, Justice and Home Affairs, *id*.
23. *Id.*

wallet [24]. Parliament fought back against the proposed EU ID number, ensuring it was not instated as part of the final regulation [25]. Giving such an express power of digital identity construction and management to the EU Commission could create future risk to citizens and weaken Member State sovereignty. While there is no EU-wide ID number, by establishing an EU digital wallet, the EU Commission is still exercising its power in stating which Member State identities will qualify for the EU digital wallet [26]. The Commission will mandate which identifying attributes must be included in an ID, Member State IDs' technological standards, mandated digital availability, and assurance levels [27]. This raises concern as it is difficult to believe all Member States will be equally impacted by the EU Commission's technological standards for digitally mandated Member State identifications. Technological infrastructure as mandated by the EU could create higher or lower burdens for various Member States, and by proxy, create burdens on their citizens.

The proposal not only openly creates new relationships constructing digital identity between the EU and Member States, but also with private actors. For example, Article 28 states, " [w]ide availability and usability of the European Digital Identity Wallets require their acceptance by private service providers, " meaning all variety of private actors including transport, banking and financial services, or health, will be required to accept the identity wallets [28]. Under eIDAS, while some entities like those listed above will be required to accept the wallet [29], others like private gyms will have the option of utilizing it [30]. Any private actor accepting the wallet must also report their use to the EU [31]. This new relationship requires private actors to report to the EU Commission when they accept the EU digital wallets. This means the EU will know which private actors are using the digital wallets and information on how EU citizens are interacting with private companies. This further usurps identity management power from individuals, who could be listed as a consumer at a private company reporting its identity collection to the Commission. Being unable to control the line of access between the private actor and the EU Commission could create serious risks to identity privacy. This new reporting requirement can reach from passport services, or services where individuals might anticipate EU Commission identity access, to hotels or gyms, where EU reporting is not typically expected.

It is further interesting to consider who will be running the technological infrastructure of the digital identity wallet. An eIDAS proposal recital states, " conformity of European Digital Identity Wallets with [eIDAS] requirements should be certified by accredited public or private sector bodies designated by Member States " [32]. Therefore, private sector identity and trust services could step into the role of providing technological infrastructure for digital wallets. While the text states " public or private ", some Member States will not be able to maintain the infrastructure themselves and will pass this identity construction and verification to private actors. For example, Romania and Bulgaria are working with private actors who recently received funding or approvals to digitize identity verification procedures, noting that these private actor services are eIDAS-compliant [33]. Like LoanLink24, the private actor becomes a gatekeeper in the management and implementation of a public resource, like digital identity. In this instance, the private actors will be working with the EU Commission and Member States to provide a public resource.

This new digital identity gives both private and public actors the power to say what identity attributes make an individual identifiable on an EU level. Mandatorily included attributes will be name, date of birth, and unique identifier, like a national ID, whereas listed optional attributes include address, gender, or national tax ID [34]. While the EU and Member States can say what attributes are required for digital identity, private actors may serve as gatekeepers of access and maintenance of the system. The new relationship between these three actors could create new barriers to individual identity management. The private actors who would be responsible for digital identity infrastructure and verification while acting as an agent for the public, may also be impacted by their own networks of influence in the private sector. For instance, the private Linux Foundation announced in February 2023 they will launch OpenWallet Foundation intended to " power interoperable digital wallets " with constructing eIDAS infrastructure in mind [35]. The foundation's voting members include private actors in the digital identity space such as Visa, Accenture, Avast, or Huawei [36]. Who will assess the impact of private actors influence on one another as they serve in these identity construction and management roles ?

In addition, the private actors will also be influencing individuals' access and use of their digital identity. The wallet will also run on a mobile phone, presumably a smartphone [37]. This decision made by public actors and carried out by public or private actors will specifically disadvantage non-smartphone users in the EU. According to the EU, 5% of EU citizens have never owned a mobile phone [38]. While this number seems small, it also excludes people who might not want to transfer all their personal identity information into digital form. These barriers to digital identity may only grow in the future. Since the goal of the EU is to ensure wide adoption, the increase of digital identity use might slowly make physical identification difficult or unwanted [39]. One study found a 31% increase in Apple Pay transactions only between 2020 and 2021 [40]. As digital apps and mobile phones become increasingly adopted,

24. European Commission, " Commission recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework ", 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/ ?uri=CELEX%3A32021H0946.
25. This issue was discussed by Cristian Terhes in " eIDAS 2.0 : Latest News & Progress ", *op. cit.*
26. European Commission, " Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity ", *op. cit.*
27. *Id.*
28. *Id.*
29. *Id.*
30. This issue was discussed by Vedran Lalic, the Head of the Office for MEP Romana Jerkovic (Group of the Progressive Alliance of Socialists and Democrats in the European Parliament) and Rapporteur for eIDAS file, in " eIDAS 2.0 : Latest News & Progress ", *op. cit.*
31. European Commission, " Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity ", *op. cit.*
32. *Id.*
33. Constantin Macri, " Romanian startup Qoobiss has received ADR approval for its eKYC solution ensuring remote user identity verification ", *Business Review* (Feb. 7, 2023), https://business-review.eu/tech/romanian-startup-qoobiss-has-received-adr-approval-for-its-ekyc-solution-ensuring-remote-user-identity-verification-241266. *See also :* " Bulgarian Development Bank provides €2.5 million of funding to Evrotrust ", Evrotrust (Feb. 10, 2023), https://evrotrust.com/blog/bulgarian-development-bank-provides-2-5-million-of-funding-to-evrotrust.
34. European Commission, " Commission recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework ", *op. cit.*
35. Paul Sawers, " Linux Foundation Europe Launches the OpenWallet Foundation to Power Interoperable Digital Wallets ", *TechCrunch*, (Feb. 23, 2023), https://techcrunch.com/2023/02/23/linux-foundation-europe-launches-the-openwallet-foundation-to-power-interoperable-digital-wallets.
36. *Id.*
37. European Commission, " Commission recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework ", *op. cit.*
38. Eurostat, " Digital economy and society statistics – households and individuals " (Dec. 2022), https://ec.europa.eu/eurostat/statistics-explained/index.php ?title=Digital_economy_and_society_statistics_-_households_and_individuals.
39. European Commission, " Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity ", *op. cit.*
40. Arnav Gupta, " The Economics of Apple Pay ", *Michigan Journal of Economics* (Nov. 15, 2022), https://sites.lsa.umich.edu/mje/2022/11/15/the-economics-of-apple-pay/.

this could construct higher barriers to those without phones, or who don't wish to adopt the wallet, and overall, an individual's ability to construct and control their identity.

One last consideration, what are the risks of these new relationships ? While the relationship between public and private actors existed long before digitization, one interesting aspect is, as the technological infrastructure of the wallets is built, private actors have a widened impact on the actual use and access to digital identities that is not thoroughly explained. Will eIDAS give private actors unprecedented influence in the identity construction of EU citizens ?

In the same token, if these private actors are responsible for maintaining the technological infrastructure, the EU may be similarly responsible for keeping the private actors accountable and functioning. Private actors need to be compliant with data security, privacy, cybersecurity, and free and accessible use. The eIDAS provides for accountability measures on these counts [41], but in this two-way relationship, who is keeping the public actors, the EU or the Member States, accountable ? The General Data Protection Regulation (GDPR) already carves out exemption from the desired practices surrounding data protection for purposes of national security, defense, or public interest [42]. Could there be a scenario where weighing the proportionality of the public interests and fundamental rights of privacy allows the EU to access identity data from all EU citizens ? Looking back to data challenges during the Covid 19 pandemic, this scenario is not difficult to imagine.

41. European Commission, " Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity ", *op. cit.*
42. European Commission, " Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the 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) ", https://eur-lex.europa.eu/eli/reg/2016/679/oj.

Conclusion

4 - While some of this intellectual posturing may never come to fruition, this article should exemplify the importance of monitoring and questioning the power relationships that exist between private and public actors. The public actor's power to construct an individual's identity for the organized state also prompts the relationship between the public and the private actor to which they delegate power to carry out their responsibilities of state management and resource distribution. Private use of digital identity and the creation of eIDAS seems to evolve this public-private relationship in a new way. The power imbalances stemming from public-private joint action in identity construction increases the risk of misuse and mismanagement of the digital identity of individuals. Concerns regarding the growing closeness of the relationship could create issues for the public sector who will be increasingly liable for the private sector and has more unchecked power due to exceptions for public interest and action. Because we know there is a risk to fundamental rights and human dignity via private actors enforcing digital identity in serving their role as agents of the state, eIDAS shows the potential risk when expanding that framework to new identity spaces. This evolving relationship could mean expanded challenges to that access by both public actors and private agents of the public.■

4 Virtual Love, Real Consequences : How Dating Apps Are Exploiting Your Digital Identity

Julia VIEIRA,
DIGILAW Clinic, SciencesPo Law School

1. Dating Apps Background

1 - In a world where philosopher Zygmunt Bauman's coined concept of " liquid love " [1] predominates, superficiality is treated as a key characteristic of consumer society, which further extrapolates to relationships. According to Bauman, the great attraction of the Internet is not the ease of connecting and making friends, but the ease of disconnecting. And in this virtual world, we have the option to swipe right, left, and when things don't go as expected, at least for one of the parties, there is no conversation, no signal, it simply ends in " ghosting. "

Disposable or not, liquid or not, dating apps are part of modern reality, and according to a collective study, 323 million people use dating apps worldwide [2]. Tinder was the most downloaded app in 2021, followed by Bumble, but Badoo remains the most popular in Europe. In the same year, the dating app market profits amounted to $5.61 billion. According to apptweak research, the conglomerate Match Group that owns Tinder, Hinge, Plenty of Fish, OKCupid, Meetic, Match.com, dominates the dating space [3]. Match Group accounts for more than 56% of total downloads, taking the majority of the pie [4]. Magic Labs, which owns Bumble and Badoo, accounts for 33% of total downloads.

Here, the goal is to bring information about the part of reality that is not as explicit as some of the photos that are exchanged on these dating apps but which have a great impact on the lives of individuals and also on society as a whole. For this, I will " spill the tea " and describe the ways users are susceptible to the misuse and mismanagement of their digital identity, how their data is exploited by Big Tech companies in order to profit from it, and how this data exploitation can undermine democracy and personal autonomy.

Yes, this is a lot of information, but hopefully, after this article, you will be more aware of how this power imbalance works, how to protect yourself, if at all possible, and the regulatory measures that the European Union has taken to limit the power of the big tech companies and protect citizens.

What is digital identity ?

Digital identity can be understood as information and data used to identify individuals or entities, such as personal information, behavior, and digital footprints. Digital identity can also be intentional or unintentional, the former being what you share online and the latter being the data collected by websites and applications, for instance. As a result, digital identity is not static, but constantly evolving as you interact online, especially if you are a user of at least one of the " BIG FIVE " [5] many platforms and services.

2. Online Dating Scandals

2 - Digital identity breaches on dating apps can occur in a number of ways. Some of the most common include :

- *Data leakage :* when the personal information of users such as name, email address, credit card information, and other sensitive information is stolen or exposed by hackers or other malicious entities ;
- *Improper information sharing :* when dating apps share users' personal information with third parties without users' consent or a clear privacy policy ;
- *Information misuse :* when dating apps use users' personal information for purposes other than those for which users have given consent ;

Such digital identity breaches can have serious consequences for users, including identity theft, cyberstalking, financial fraud, and other types of cybercrime.

In recent years, there have been a number of scandals [6] involving dating apps that have exposed sensitive user data including location, messaging, banking data, and health conditions of users :

- *Tinder data breach :* in 2016, a vulnerability in the Tinder app allowed hackers to access users' sensitive data, including their location data and messages ;
- *Grindr data breach :* in 2018, it was revealed that the popular gay dating app Grindr was sharing users' sensitive personal information, including HIV status, with third-party companies ;
- *Ashley Madison data breach :* in 2015, the dating website Ashley Madison, which specialized in facilitating extramarital affairs, suffered a massive data breach that exposed the personal information of millions of users, including names, addresses, and credit card information ;
- *OKCupid data experiment* : in 2014, it was reported that the dating app OKCupid was conducting psychological experiments

1. Zygmunt Bauman, " Liquid Love : On the Frailty of Human Bones ", Polity (2003).
2. David Curry, " Dating App Revenue and Usage Statistics (2023) ", *Business of Apps* (May 2, 2023), https ://www.businessofapps.com/data/dating-app-market/.
3. Lea Marrazzo, " Most Popular Dating Apps per Country ", *apptweak*, (Feb. 14, 2022), https ://www.apptweak.com/en/mobile-app-news/check-out-the-most-popular-dating-apps-by-country.
4. Source : apptweak, https ://www.apptweak.com/en. Download estimates for the top 10 most popular dating apps in the United States, United Kingdom, France, Germany, Italy, and Spain between Aug. 8, 2021 and Feb. 8, 2022.
5. The so-called " BIG FIVE " or " GAFAM " are the Big Tech companies who dominate the information technology industry. Google,Amazon,Facebook, Apple and Microsoft are the companies which give rise to the acronym.
6. Judith Duportail, " I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets ", *The Guardian* (Sept. 26, 2017), https ://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold.

on users, including manipulating their newsfeeds to see how they responded.

A. - Ashley Madison Scandal[7]

3 - In 2015, the dating website Ashley Madison, which specialized in facilitating extramarital affairs, suffered a massive data breach that exposed the personal information of millions of users, including names, addresses, and credit card information. The repercussions of this scandal included :

- The company faced several legal actions following the data breach. One of them was a class-action lawsuit settled for $11.2 million in 2017 [8], which was brought on behalf of users whose personal information was exposed in the breach ;
- The data breach had a significant impact on Ashley Madison's reputation, with criticism arising for not protecting the users' privacy and also for promoting infidelity. The company's CEO at the time resigned shortly after the data breach was made public ;
- The data breach had personal consequences for many users, some of them reported receiving blackmail threats or being publicly shamed as a result of their personal information being exposed publicly ;
- The Ashley Madison data breach scandal resulted in increasing scrutiny of security practices by online companies and a push for better data protection measures and transparency around data collection.

B. - OkCupid Scandal[9]

4 - Christian Rudder, OkCupid's co-founder and data scientist, at the time, wrote an article entitled " We Experiment On Human Beings ! " [10] where he gives three examples of experiments the firm had performed with users in order to improve their algorithm. Not only that but he also made a strong statement when it comes to tech companies treating humans as lab rats : " if you use the internet, you're the subject of hundreds of experiments at any given time, on every site. That's how websites work ".

In order to prove the algorithm's accuracy when it comes to its " matching " rating, OkCupid *" lied to a portion of users about how strongly they matched with other users, and observed how many single messages led to a full conversation. Sure enough, they found that two users who actually had a 90% match but were told that they had a 30% match were less likely to carry on talking than two users who actually had a 30% match but were told they had a 90% match. In other words, Rudder says, 'if you have to choose only one or the other, the mere myth of compatibility works just as well as the truth' "*. [11]

The OkCupid experiment proved that, according to users, personality and looks were equivalent.

However, we all know this is not true and considering the sexist pictures used by the app to prove its point in the abovementioned experiment.

C. - Discrimination in Online Dating

5 - Several studies have proved that we are far away from an inclusive and non-discriminatory environment on dating apps. One of the reasons for that is the lack of diversity and awareness in tech companies, dominated by white males, that results in discriminatory practices.

Here are some examples of digital identity issues (that pretty much reflect the offline dating circumstances. Even though online dating created new problems, such as ghosting and catfishing, for instance, other aspects are just reinforced) when it comes to dating :

- *Race :* a study published in the Journal of Sex Research [12] found that racial minorities, particularly Black and Asian individuals, were less likely to receive matches or messages on dating apps compared to White individuals. It was also found that people of color face both explicit and implicit forms of racism on dating apps ;
- *Body shape :* people who are overweight or obese are less likely to receive matches and messages on dating apps compared to those who are thinner. Also, people who include their body type in their dating app profiles are more likely to receive messages from people who prefer that specific body type ;
- *Gender :* a study conducted by Pew Research Center [13] found that women are more likely to experience gender-based harassment and unwanted sexual advances on dating apps compared to men. Women receive more messages overall on dating apps, but men are more likely to initiate messages and initiate contact with more desirable partners. The research [14] concluded that 53% of women agree that online dating is more dangerous than other ways of meeting people ;
- *Sexual orientation :* a study published in the journal of Sex Research [15] found that LGBTQ+ individuals are more likely to face discrimination and harassment on dating apps compared to heterosexual individuals. Another study published by Essy Knopf's [16] website found that gay men face pressure to conform to certain standards of masculinity on dating apps, which can lead to feelings of rejection and low self-esteem.

3. European Legal Frameworks Regarding Privacy

6 - At this point, you have already understood that dating apps share a massive amount of user's personal data to third-party companies, most of them specialized in online advertisement. Then, these companies are able to make conclusions about individuals and segments of consumers in order to target them with personalized ads. Not only are you receiving the advertising as a dating app user, but you are receiving them when you are more susceptible. Hence, the purpose of the adtech companies [17] is not limited to advertising but also to control your behavior and profit from it.

The oversharing and overcollection of personal data leave consumers with little control over their data and little knowledge on how their data is being collected and used. The current system shows an abusive and unequal relationship between users and tech

7. Kim Zetter, " Hackers Finally Post Stolen Ashley Madison Data ", *Wired*, (Aug. 18, 2015), https ://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/.
8. Jonathan Stempel, " Ashley Madison parent in $11.2 million settlement over data breach ", *Reuters* (July 15, 2017), https ://www.reuters.com/article/us-ashleymadison-settlement-idUSKBN19Z2F0.
9. Alex Hern, " OKCupid : We experiment on users. Everyone does ", *The Guardian* (July 29, 2014), https ://www.theguardian.com/technology/2014/jul/29/okcupid-experiment-human-beings-dating.
10. Christian Rudder, " We Experiment On Human Beings ! ", *OkTrends* (blog), (July 28, 2014), https ://web.archive.org/web/20140728200455/http://blog.okcupid.com/index.php/we-experiment-on-human-beings/.
11. *Id.*
12. Patrick A. Wilson et al., " Race-Based Sexual Stereotyping and Sexual Partnering Among Men Who Use the Internet to Identify Other Men for Bareback Sex ", *The Journal of Sex Research*, Vol. 46, no. 5, 399-413 (2009).
13. Aaron Smith, " 15% of American Adults Have Used Online Dating Sites or Mobile Dating Apps ", *Pew Research Center : Internet, Science & Tech* (blog) (Feb. 11, 2016), https ://www.pewresearch.org/internet/2016/02/11/15-percent-of-american-adults-have-used-online-dating-sites-or-mobile-dating-apps/.
14. *Id.*
15. Patrick A. Wilson et al., *op. cit.*
16. Essy Knopf, " Dating Apps are surveillance capitalism at its most cynical ", *Essy Knopf* (Feb. 9, 2021), https ://essyknopf.com/dating-apps-and-surveillance-capitalism/.
17. Oracle, " What is adtech ? ", *Oracle India*, https ://www.oracle.com/in/cx/advertising/adtech/#types. According to Oracle, adtech is *" a broad term that categorizes the software and tools that agencies, brands, publishers, and platforms use to target, deliver, and measure their digital advertising efforts. Adtech software platforms help brands and agencies purchase advertising space. They also help publishers price and sell their ad space "*.

companies, which leads to a huge impact to citizens' personal autonomies and to our democracies too.

From a legal standpoint, can these processing operations be justified ?

Article 12 of the United Nations' Declaration of Human Rights [18] establishes that : " no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation ". Hence, the right to privacy is a human right that should be guaranteed as a way to protect one's dignity, personal identity, and autonomy. Additionally, the International Covenant on Civil and Political Rights [19] and the Convention on the Rights of the Child [20] also recognize privacy and data protection as human rights to be safeguarded. In Europe, the right to privacy and data protection are fundamental rights embodied in the EU Treaties and in the Charter of Fundamental Rights [21].

The legal framework in Europe when it comes to privacy is primarily governed by the General Data Protection Regulation (GDPR) [22], which came into effect in May 2018. The GDPR is a comprehensive privacy law that applies to all businesses operating within the European Union (EU), as well as businesses outside the EU that process the personal data of EU citizens.

The GDPR provides individuals with a number of rights with respect to their personal data, including the right to access, rectify, and erase their data, as well as the right to object to the processing of their data. The GDPR also requires businesses to obtain explicit consent from individuals before collecting, processing, or sharing their personal data, and to implement appropriate technical and organizational measures to ensure the security and protection of that data.

The above-mentioned regulation also requires businesses to implement appropriate technical and organizational measures to ensure the security and protection of personal data that is shared with third parties. This includes entering into data processing agreements with third-party service providers that specify the responsibilities of each party with respect to data protection.

Overall, the legal privacy framework in Europe is designed to provide individuals with greater control over their personal data and to ensure that businesses handle that data in a transparent and responsible manner. Even though the GDPR is considered as a landmark piece of legislation towards a better protection of personal data, the Regulation has its limitations. The scope is limited to the EU territory ; companies found a way to circumvent the transparency requirements ; enforcement already proved to be challenging and ends up leaving the data of innumerable individuals vulnerable as we could see with the data breaches previously presented.

After analyzing the terms and conditions of some of the most popular dating apps in the world, it was observed that most of the companies do the basics to comply with the GDPR and have very generic and similar rules, such as obtaining the explicit consent of users before sharing their personal data and allowing them to share users' data with third parties :

- *For legal reasons :* the company may share user data with third parties if it is required to do so by law or in response to a valid legal request ;
- *To provide services :* the company may share user data with third-party service providers that help the company to provide its services, such as cloud storage providers or customer support providers ;
- *To prevent fraud or safety issues :* the company may share user data with third parties if it believes in good faith that such sharing is necessary to prevent fraud, protect the safety of users or others, or enforce its terms and conditions.

Additionally, the companies make sure to state that measures to ensure that the third parties with whom they share the data have proper security measures to guarantee the protection of the referred data. Even though it is beautiful in theory, just like a catfish, the reality is not the same.

The report " *Out of Control : How Consumers are Exploited by the Online Advertising Industry* " [23] published by the Norwegian Consumer Council in 2020, raises concerns about the lack of transparency and user control over their personal data in ten mobile apps, including dating apps, as well as the potential for discrimination and abuse based on the data sharing practices of these apps. It was found that sensitive personal information from users is collected, including their exact location, sexual orientation, religious and political beliefs, drug use, among other information, and this data is transmitted to multiple third-party companies.

After comparing the privacy policies of 5 dating apps, the only one that specifies some of the third parties to whom personal data from users are shared is Grindr :

> For the avoidance of doubt, Grindr only shares HIV status, Last Tested Date, and vaccination status with necessary Service Providers such as companies that host data on our behalf (i.e., Amazon Web Services) or help in processing data access requests you initiate (i.e., PartnerHero) – we do not share this information with any advertising companies [24].

Maybe it has something to do with the $11.7 million fine the Norwegian Data Protection Authority imposed on Grindr for illegally sharing details about users' sexual orientation and location with several advertising companies [25] :

Why are we so vulnerable as users ?

4. Surveillance Capitalism

7 - " Surveillance capitalism " is a term coined by Shoshana Zuboff, a professor at Harvard University, in her book *The Age of Surveillance Capitalism* [26], where she describes the business practices of the Big Tech companies that rely on the collection and analysis of vast amounts of user data in order to generate profits. According to Zuboff, these companies are engaged in a new form of capitalism that involves the commodification of personal data, and the creation of new forms of power and control over individuals and society as a whole.

Zuboff argues that the rise of surveillance capitalism is rooted in the convergence of several factors, including the proliferation of digital technologies that make it possible to collect and analyze vast amounts of data in real-time, the decline of traditional forms of advertising and the search for new sources of revenue, and the emergence of a new business model based on the monetization of user data.

18. United Nations, *Universal Declaration of Human Rights*, (1948), https ://www.un.org/en/about-us/universal-declaration-of-human-rights.
19. Office of the United Nations High Commissioner for Human Rights, *International Covenant on Civil and Political Rights* (adopted Dec. 16, 1966), https ://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.
20. United Nations Convention to Combat Desertification, " The Official documents of the United Nations (UN ODS) ", https ://www.unccd.int/resources/knowledge-sharing-system/official-documents-united-nations-un-ods.
21. See, for example, Art. 7 and 8 of the Charter of Fundamental Rights of the European Union ; Art. 16(1) of the Treaty on the Functioning of the European Union (TFEU) ; Art. 1(2) and Recital 1 GDPR.
22. Intersoft Consulting, " General Data Protection Regulation (GDPR) ", (2018), https ://gdpr-info.eu/.
23. Forbrukerrådet, report " Out of Control – How consumers are exploited by the online advertising industry ", *ConPolicy*, (Jan. 24, 2020), https ://www.conpolicy.de/en/news-detail/out-of-control-how-consumers-are-exploited-by-the-online-advertising-industry.
24. Grindr, " New Privacy and Cookie Policy " (June 2022), https ://www.grindr.com/privacy-policy/how-we-may-share/.
25. Natasha Singer and Aaron Krolik, " Grindr is fined $11.7 million under European privacy law ", *The New York Times* (Jan. 25, 2021), https ://www.nytimes.com/2021/01/25/business/grindr-gdpr-privacy-fine.html.
26. Shoshana Zuboff, *The Age of Surveillance Capitalism : The Fight for a Human Future at the New Frontier of Power*, New York (N.Y.) : Public Affairs, 2019., n.d.

Under this new model, companies like Google and Facebook track and analyze user behavior across multiple platforms and devices, using this data to build detailed profiles of individuals and groups, and to target them with personalized advertising and other forms of content. These companies also use their data-driven insights to influence and shape user behavior, through techniques like " persuasive design " and " dark patterns " that exploit cognitive biases and manipulate user choices.

Zuboff argues that the rise of surveillance capitalism raises profound questions about privacy, autonomy, and the nature of democracy itself, and that it requires a new framework for understanding and regulating the power dynamics of the digital economy. She has called for a " digital declaration of rights " that would enshrine the principles of individual autonomy, privacy, and democratic governance in the design and regulation of digital technologies.

Amy Kapczynski, a professor at Yale Law School, criticizes some aspects of Zuboff's analysis in the article " The Law of Informational Capitalism [27]. While Kapczynski praises Zuboff's book for its comprehensive analysis of the ways in which digital technologies have transformed capitalism and society, she also raises some critiques.

One of Kapczynski's main critiques of Zuboff's analysis is that it places too much emphasis on individual agency and consumer choice, while neglecting the role of structural power imbalances and the need for collective action to counter the harms of surveillance capitalism. Kapczynski argues that a more robust critique of surveillance capitalism must consider the broader social and economic forces that enable and perpetuate it as well as the political and legal implications of surveillance capitalism. She notes that Zuboff tends to focus on the harms of surveillance capitalism at the level of individual privacy and autonomy but does not engage as deeply with the implications of these harms for democratic governance and the public sphere. She suggests that Zuboff's book offers a valuable framework for thinking about the challenges and opportunities of the digital age and underscores the need for new legal and political strategies to address the harms of surveillance capitalism from the vantage point of larger systematic change.

Even though there are some differences among the ideas of the two scholars, it is unquestionable that our data is being sold and is sustaining a profitable industry. According to Worldwide Digital Ad Spending 2021 [28], $646 billion will be spent on digital ads worldwide by 2024.

There is no better way to understand the importance of adtech from a business point of view than from one of the industry players. Here is why the advertise-based industry on dating apps is so important, according to Oracle Advertising [29] :

> Because of the large amounts of money that is spent on digital advertising. With that amount of volume, adtech helps buyers optimize their budgets and sellers maximize their revenue stream. The goal is to get better ad placements, deliver the right content to the right person, and reduce the amount of wasteful spending. Ad tech also provides comprehensive behavioral data that can be used to target potential audiences better and measure campaign success. Thanks to data-driven insights from billions of consumers' device interactions, it's become more popular as companies discover how cost-effective these solutions are.

Based on what was presented so far, we can infer that, at the moment, the economic interest of companies has had a greater weight than the fundamental rights and freedoms of users. The " Out of Control : How Consumers are Exploited by the Online Advertising Industry " report explains it perfectly :

> In addition to undermining the right to privacy, the comprehensive surveillance many of these companies engage in poses a systemic threat to fundamental rights such as the freedom of opinion and expression, freedom of thought, and the right to equality and non-discrimination. Meanwhile, the system is so complex that consumers cannot have any reasonable expectation of this happening. It can be assumed that such a threat may significantly outweigh any perceived legitimate interest that data brokers and other adtech actors have in monetizing this data [30].

5. What has been done so far + What else can be done ?

8 - Shoshana Zuboff referred to the Digital Services Act (DSA) as " the first comprehensive declaration of a digital future founded on the legitimate authority of democratic rights and the rule of law, and a signal that the principles of a self-governing demos might survive the digital century " [31], but she also mentions that " a great deal of work remains to be done. Much of what occurs in our information spaces today is profoundly illegitimate, but because it is unprecedented it is not yet illegal " [32].

The Digital Services Act [33] is a Regulation proposed by the European Commission to update the Electronic Commerce Directive 2000 regarding illegal content, transparent advertising, and disinformation, and modernize the legal framework for digital services. It aims to create a safer digital space in which the fundamental rights of all users of digital services are protected, promote a more transparent framework for online platforms while at the same time innovation, growth and competitiveness is preserved. Here are some of the provisions when it comes to the fundamental rights of users :

- *Freedom of expression :* the DSA requires digital service providers to respect the freedom of expression of their users, subject to certain limitations such as hate speech, incitement to violence, and the spread of disinformation ;
- *Right to information :* the DSA requires digital service providers to provide users with clear and transparent information about their policies and practices, including with respect to content moderation and data protection ;
- *Right to redress :* the DSA requires digital service providers to establish effective and accessible mechanisms for users to lodge complaints and seek redress for violations of their rights ;
- *Non-discrimination :* the DSA prohibits digital service providers from discriminating against users on the basis of their nationality, place of residence, or any other ground ;
- *Protection of minors :* the DSA requires digital service providers to take measures to protect minors from harmful content and behavior, and to obtain parental consent for the processing of personal data of minors.

If it is going to be effective, only time can tell. In the meantime, now that you are aware of the panorama, do not hesitate to observe how the scenario evolves and maybe you will feel propelled to engage in the discussion and participate in the transformation of this unequal dynamic.■

27. Amy Kapczynski, " The Law of Informational Capitalism ", *The Yale Law Journal*, Vol. 129, no. 5, 1460-1515 (2020).
28. Ethan Cramer-Flood, " Worldwide Digital Ad Spending 2021 ", *Insider Intelligence* (Apr. 29, 2021), https ://www.insiderintelligence.com/content/worldwide-digital-ad-spending-2021.
29. Oracle, " What is adtech ", *Oracle* India, https ://www.oracle.com/in/cx/advertising/adtech/.
30. Forbrukerrådet, *op. cit.*, p. 177.
31. Vincent F. Hendricks, " BigTech Business Model, Big Deal, Big Trouble ", *The OECD Forum Network* (May 4, 2022), https ://www.oecd-forum.org/posts/big-tech-business-model-big-deal-big-trouble.
32. *Id.*
33. European Commission, " The Digital Services Act : Ensuring a safe and accountable online environment ", https ://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en.

5 The Benefits and Risks of i-Voting with Digital Identity

Emma JAMES,
DIGILAW Clinic, SciencesPo Law School

1 - For many countries around the world, voting is an essential part of their democracy, allowing them to have a say in governance. Voting has taken on various forms and enfranchised different groups of people over time. While voting in Ancient Greece was only open to unenslaved men who voted by a public show of hands [1], modern day voting has evolved quite a bit. Nowadays, the voting process in countries worldwide often looks quite similar, with most having the same few basic steps :

1. Presenting oneself to a polling station ;
2. Providing an identity document for identity verification ;
3. Heading to a private polling booth where one's ballot is filled ;
4. Submitting the ballot to be counted.

It is possible to have deep and engaging discussions about all parts of the voting process, but step two is particularly fascinating, as it concerns the nebulous concept of *identity*. Having already looked at constructions of digital identity in the private and public-private sectors, let us now turn to the public sector.

In the public sector, governments began collecting data via censuses to gain an accurate picture of their population, in an effort to better tax their citizens. Thus began the construction of legal identities. In the past few centuries, data collection has increased as governments look to improve the allocation of public services and resources to their citizens. For instance, driver's licenses often require one's height, weight, and hair color, as well as a personal identifying number, to ensure car insurance is provided for the correct person (and their car) and that the insurer deals with the correct parties.

Until relatively recently, such data was collected and stored using written documents. However, with the coming of the fourth industrial revolution and the widespread use of computers, the world has begun its evolution into a paper-online hybrid model. As technology progresses, the online approach has seemed to become increasingly central to both data collection and the uses of data (such as public service provisioning).

Estonia is a prime example of this wave of the digitalization of public services, to the point where the country has also become known by the name *e-Estonia*, a nickname adopted by the country that refers to Estonia's 'digital society' [2]. Specifically, this so-called 'digital society' helps to enable digital interactions between the state and its citizens. Through Estonia's online services, citizens are able to submit tax returns, conduct banking transactions, vote, and register new businesses. The country even offers " e-Residency ", for those living outside the country to access its digital services.

One of the pillars of e-Estonia, enabling citizens to access these 'e-services', has been the mandatory electronic identification document (e-ID). First implemented in 2002, it is a 'normal' identification card that can also be used online. The e-ID has a chip containing a " personal data file ", along with an authentication key to access online services and a digital signature key to provide legally-binding signatures.

Significantly, this identity card is used for i-voting (voting via the internet). Estonia first implemented online voting in 2005, allowing people throughout – and outside of – the country to vote in elections from the convenience of their homes, or anywhere else with a computer and an internet connection. Currently, the country has conducted 11 elections (national, local and European Parliament elections) using i-voting, and the method has gained popularity, with over 40% of voters listing it as their preferred voting method [3]. Estonia has been enthusiastic about sharing its experiences with i-voting, allowing many nations to observe elections [4]. And as it can be seen through the map by the International Institute for Democracy and Electoral Assistance (IDEA), enthusiasm for i-voting has spread, with 13 other countries joining in and implementing this new form of voting in some capacity [5].

While i-voting was a groundbreaking achievement in the e-delivery of public services and is achieving growing popularity, its implementation raises some important questions. What does it mean for a country which has " largely [shooed] away concerns about data privacy " to foster a culture of normalizing privacy collection and maintenance of a significant amount of citizen data ? [6] How might this affect civic participation or fundamental rights to privacy ? Other concerns include issues around the authenticity of votes that are not monitored by an electoral governing body while they are cast, an issue which is rendered further complex when considering marginalized populations.

This article will dive into i-voting in Estonia : looking at how it functions, the history behind its development and implementation, and its legal basis. Then, we will take a more critical look at how digital identity is interwoven in the i-voting system and the power dynamics between citizens and the state.

1. How does i-voting work, exactly ?

2 - As previously described, i-voting is the process by which one votes in elections online. In the Estonian case, it requires a computer, a stable internet connection, a secure government website, a

1. Dave Roos, " How People Voted in Ancient Elections ", *HISTORY*, (Nov. 4, 2022), https ://www.history.com/news/ancient-elections-voting.
2. E-Estonia, https ://e-estonia.com/.
3. E-Estonia, " Factsheet : I-Voting " (Mar. 2020), https ://e-estonia.com/wp-content/uploads/2020mar-facts-a4-v02-i-voting.pdf.
4. Tarvi Martens, " Electronic voting : What Europe can learn from Estonia ", *Microsoft Corporate Blogs* (interview) (May 10, 2019), https ://blogs.microsoft-.com/eupolicy/2019/05/10/electronic-voting-estonia/.
5. International IDEA, " Use of E-Voting Around the World " (Oct. 17, 2015), https ://www.idea.int/news-media/media/use-e-voting-around-world.
6. Mark Scott, " Estonians Embrace Life in a Digital World ", *The New York Times* (Oct. 8, 2014), https ://www.nytimes.com/2014/10/09/business/international/estonians-embrace-life-in-a-digital-world.html.

central server, a secure fashion of digitally authenticating someone, and their digital signature. I-voting does not require being in any specific location (other than being in proximity to an internet connection), so users are able to vote from anywhere in the world rather than just designated polling stations. Citizens are able to i-vote anytime within the designated period for early voting, typically ten to four days before the day of the election [7]. These i-votes can be changed and resubmitted as many times as the voter would like. As of 2021, if a voter changes their mind between the early voting period and election day, they are able to replace their i-vote by voting in-person on election day [8].

To understand how i-voting appears in the eyes of a voter, Erika Piirmets describes her voting process [9] :

1. She first connects to the internet and downloads the Estonian voting application from a website ;

2. She then inserts her e-ID card into the smart card reader (or mobile phone) to verify her voting and district eligibility ;

3. Erica sees the list of candidates and selects the one she wants to vote for. The candidate's name is then displayed on the computer screen ;

4. Then, she clicks the " vote " button, which requires her to enter her personal pin code. Entering this code provides her digital signature to the vote ;

5. Erica is now finished voting !

6. In the system, the vote is encrypted once the digital signature is added and it is anonymized, then sent to the central server. After election day, the vote is de-encrypted to ascertain who the vote was for.

2. How did i-voting come to be implemented in Estonia ?

3 - In order to understand how Estonia came to embrace i-voting, it is necessary to understand how Estonia became e-Estonia. After the fall of the Soviet Union, Estonia regained independence in 1991. The small country, only recently separated from the USSR, had little by way of financial resources, had few options to kick-start its economy as it was without a large landmass or population [10]. It was also around this time that a wave of computerization first swept North America and Europe, and the internet was beginning to become more readily available to the general public. These two major elements led to the Estonian government recognizing that the use of the internet and other digital technologies would allow the country to provide public services, but at a lower cost.

During the 1990s, Estonia made two decisions that paved the way for the creation of e-Estonia [11] :

- The decision to create the X-Road data exchange middleware ;
- The creation of the e-ID and associated digital infrastructure to contain users' authentication tokens and data.

The X-Road middleware allowed for the information systems of public and private actors to exchange data, while the new e-ID cards combined citizens' physical and digital public identities and allowed them to access public services and resources, such as using their e-IDs to access their banking accounts (from privately-owned banks). The all-encompassing nature of the e-services provided in Estonia has led to their wide adoption by the Estonian public, who trust the e-services greatly. According to Raag, who surveyed Estonians in 2020, around 82% of the sampled population felt that their government's e-services were trustworthy [12].

The idea of i-voting itself was first brought forth by the Estonian government in 2001, as a way to boost voter turnout rates, particularly for the youth, and to enable voting to be a more convenient process for citizens [13]. Legislation was quickly adopted in 2002, setting out the conditions to enable i-voting. The first year i-voting was implemented was in 2005, where 1.95% of voters in the local elections of that year tried out the service. Since 2005, i-voting has become more and more commonplace, with 43.8% of participating voters using i-voting to cast their ballots in the 2019 national elections [14].

3. What is the legal framework behind i-voting ?

4 - The legal and regulatory framework is a complex tapestry of national legislation. The following pieces of legislation are significant to i-voting :

The Identity Documents Act [15] (1999) : this act established the requirement for Estonian citizens and residents to have an identity card and regulates the issuance of such a document. Since the adoption of e-IDs, the act has been updated to include provisions for digital identity documents and digital identification [16]. E-IDs are necessary to access i-voting.

The Digital Signatures Act [17] (2000) : this act outlines the necessary conditions for the usage of legally-binding digital signatures, a requirement to authenticate one's vote.

Population Register Act [18] (2019) and *Personal Data Protection Act (2008) [19] :* these two acts define the conditions and reasons for which personal data from the Population Register may be used, and what data is included in the Population Register.

While these four acts create the basis upon which data and identity is used in i-voting, the *Riigikogu Election Act, Local Government Council Election Act* and the *Referendum Act (2002)* were adopted shortly before the first i-vote, creating an early-voting period in which i-votes could be cast, and carving out how e-IDs would be used in the processes and the ability to change one's i-vote, among other provisions.

Importantly, the Estonian government has always maintained an openness to feedback about how their i-voting system can be improved, both by making the majority of the source code of voting applications open source [20], and allowing monitoring from international organizations. They have received recommendations from the Office for Democratic Institutions and Human Rights of the Organization for Security and Cooperation in Europe (ODIHR/OSCE), an intergovernmental organization who has been monitoring and providing reports on Estonian national elections since the implementation of i-voting. The most significant feedback includes [21] :

- The 2011 report suggested that i-voting's legal framework needed updating. In response, the government amended its legis-

7. Piret Ehin et al., " Internet voting in Estonia 2005-2019 : Evidence from eleven elections ", *Government Information Quarterly*, Vol. 39, no. 4 (Oct. 2022).
8. *Id.*
9. Erika Piiermets, " How did Estonia carry out the world's first mostly online national elections ", *e-Estonia* (Mar. 7, 2023), https ://e-estonia.com/how-did-estonia-carry-out-the-worlds-first-mostly-online-national-elections/.
10. Mark Scott, *op. cit.*
11. Piret Ehin et al., *op. cit.*
12. Toomas Raag, " Eesti digiriik naudib nii kohalike elanike kui e-residentide toetust ", *Pealinn* (June 4, 2020), https ://pealinn.ee/2020/06/04/eesti-digiriik-naudib-nii-kohalike-elanike-kui-e-residentide-toetust/.
13. Office for Democratic Institutions and Human Rights, " Republic of Estonia Parliamentary Elections, 4 March 2007 – OSCE/ODIHR Election Assessment Mission Report " (Jun. 28, 2007), https ://www.osce.org/files/f/documents/1/1/25925.pdf.
14. Piret Ehin et al., *op. cit.*
15. Estonian Parliament, *Identity Documents Act* (adopted Feb. 15, 1999), https ://www.riigiteataja.ee/en/eli/504022020003/consolide.
16. Piret Ehin et al., *op. cit.*
17. Estonian Parliament, *Digital Signatures Act* (adopted Mar. 8, 2000), https ://www.riigiteataja.ee/en/eli/530102013080/consolide.
18. Estonian Parliament, *Population Register Act* (adopted Oct. 25, 2017), https ://www.riigiteataja.ee/en/eli/522032019005/consolide.
19. Estonian Parliament, *Personal Data Protection Act* (adopted Feb. 15, 2007), https ://www.riigiteataja.ee/en/eli/507032016001/consolide.
20. See https ://github.com/vvk-ehk/ivxv.
21. Piret Ehin et al., *op. cit.*

lation to introduce an Electronic Voting Committee to oversee i-voting and conduct post-election audits of the system.

- Reports in 2011 and 2015 advised improving the accountability of the i-voting system. To that effect, " vote verification with a second device [...] was introduced ahead of the 2015 [national] elections, " and the ability to verify one's vote has reached the central server of the i-voting election system.
- The 2019 report states that significant improvements have been made to the system, but continues to recommend that procedures are put in place to reduce the risk of disinformation campaigns and internal attacks to the i-voting system.

4. Why do we care (or not) about i-voting ? (alternatively, a critical examination of i-voting and Estonia's privacy culture)

A. - Cultures of Privacy

5 - According to Siim Tuisk, a politician for the Estonian Social Democratic Party, " I would say that we [Estonians] definitely have less emphasis on privacy, less emphasis on fighting against the government " [22]. Telling, he reveals " [Estonians] didn't really care about privacy, " when the e-ID system was first put in place [23]. When combined with a government who has largely brushed aside concerns regarding data privacy, it seems as though Estonia has fostered a very relaxed culture surrounding the issue. And for better or for worse, the country's citizens seem to trust their government and feel confident about how their data is being used in the public sphere, with an aforementioned 82% trusting Estonian e-services [24].

The situation begs the question, what does it mean for a state to foster a culture in which people are not overly concerned about their privacy ? Citizens of democratic countries with strong social protection systems and low amounts of corruption – like Estonians – may not have a deep sense of cynicism or inherent mistrust of their government. Thus, they may not have a strong inclination against providing the government their personal information and data if it allows them to access convenient services like i-voting. For instance, i-voting requires providing a digital signature, which is associated, via the e-ID, to identity attributes such as their home address, name, medical records and tax files.

While Estonia does have legislation regulating digital identity, via the *Identity Documents Act* and the *Personal Information Protection Act*, it is always necessary to remain critical and vigilant to ensure that such laws are properly followed. When citizens begin to accept intrusions on their privacy without critical thought towards the implications, it is a slippery slope and can enable conditions allowing for the government to act more invasively with data and face less pushback. This is not to say that Estonia is on the pathway to authoritarianism or improper use of data – it in fact attempts to be transparent in how data is used and processed. Estonia's election system is open source, so anyone is able to examine the code behind the structure, and the Data Protection Inspectorate is required to publish an annual report regarding the government's compliance with the *Personal Information Protection Act*. However, transparency is only useful in the public sphere when citizens take advantage of this transparency to ensure that the government is using data responsibly and not overstepping its grounds. Without citizen oversight, it is meaningless.

This lack of concern regarding one's privacy has implications for i-voting. If citizens have a laissez-faire attitude towards how i-voting actually works and how their votes and the data attached to them are being encrypted, how can they ensure that their governments are held accountable to the standards of a free and fair election ? While elections in Estonia have been observed by the Office for Democratic Institutions and Human Rights (ODIHR), this is at the request of the Estonian government rather than a sort of ground-up initiative from the Estonian people. States can legislate for transparency, however, they are unable to create legislation that prompts citizens to take a meaningful look at the privacy of their data, especially when this data is rendered potentially vulnerable through important systems like the i-voting system. Instead, scrutiny must come from the bottom-up, through citizen-led initiatives that encourage the population at large to take a critical look at data privacy.

B. - Risk to Voters

6 - Though the i-voting system seems to succeed in protecting votes in the i-voting system via encryption and anonymization [25], there are still ways in which one's digital identity may be compromised. E-IDs, through which public service access is mediated, are a mandatory form of identity document. [26] Therefore, every voter has access to the capability to vote on the internet whether they choose to take advantage of the possibility or not. Seeing as one's i-vote can be changed as often as possible until the day of the election, it is important to question the authenticity and privacy of internet voting.

This is particularly important for vulnerable groups. For instance, those in assisted living or elderly care homes may provide their ID cards and PIN numbers to staff to help them vote, or perhaps a grandchild helps their grandparent vote online. The person physically doing the voting could vote for who they want, rather than who the ID card holder would like. Because one's physical presence is not required at a polling station, it is impossible to be 100% certain there is no interference when voting. While this is also an issue while using mail-in voting, i-voting is becoming a norm within Estonia, while mail-in voting was traditionally considered an alternative to in-person voting. Thus, this risk to voters may be becoming more prevalent with the increased usage of i-voting.

Furthermore, is the e-ID and PIN combination strong enough proof of identity to be used for an action as significant as voting ? There will always be the possibility of identity theft/fraud in any situation, whether online or in-person, but it seems as though there is much more of an opportunity to use someone's identity improperly when there is no one physically monitoring you.

The lack of physical monitoring during voting also brings up the issue of undue influence/coercion. It is not necessarily possible for the Estonian election authority to tell when there has been undue influence when i-voting – especially when your vote can be recast as many times as desired. While recasting of i-votes can arguably help to deter the effects of coercion – i.e., if someone comes into your house and forces you to vote a certain way, you can change your vote after they have left – there is the more insidious and probable situation of coercion via misinformation campaigns and the like. For instance, malware could also be installed which simply changes one's vote at the time of submission. Alternatively, malware on a computer could record your first i-vote and then target you with misinformation in order to convince you to switch your vote. The Estonian election authority, and more broadly the Estonian government, are unable to ensure that voter's computers

22. Leonie Cater, " What Estonia's digital ID scheme can teach Europe ", *POLITICO*, (Mar. 12, 2021), https ://www.politico.eu/article/estonia-digital-id-scheme-europe/.
23. *Id.*
24. Toomas Raag, *op. cit.*
25. Valimised, " Questions about the reliability of i-voting ", https ://www.valimised.ee/en/internet-voting/frequently-asked-questions/questions-about-reliability-i-voting.
26. E-Estonia, " ID-Card ", https ://e-estonia.com/solutions/e-identity/id-card/.

are virus-free, and not all citizens have the digital literacy to know about and protect their computers from viruses.

There are misinformation campaigns regardless of whether i-voting is used, however, it would be difficult to imagine the aforementioned situations taking place after a person has voted in a polling station. This is because it is not possible to change your vote after voting in-person, and because it is extremely difficult for third-party actors to associate anything (be it an IP or physical address, name, etc.) to a voter when they vote in-person.

This brings us to the next question...

C. - Is i-voting really necessary ?

7 - One of the reasons i-voting was instituted in Estonia was in part to " boost youth voter turnout " [27].

Despite youth being generally internet savvy and spending a lot of time online, voter turnout in the 18-25 age group had decreased, according to Mihkel Solvak, an associate professor of tech research [28]. Voting online comes with risks to the election system, and to voter privacy. I-voting has not actually increased overall voter turnout [29], and more importantly, has had no significant effect on youth voter turnout (one of the main aims), which leads one to question the point of implementing i-voting.

There is an argument, especially in light of the pandemic, that i-voting can provide a safer alternative when it is dangerous to be around other people and that it can make voting more accessible to groups who may have difficulty getting to voting stations (i.e., those with physical disabilities or who live far away from voting stations). However, i-voting may also represent a case of " function creep, " or the expansion of a technology's use beyond its originally intended purpose [30]. While internet voting may be convenient for many Estonians, this convenience does not appear to be fulfilling its intended purpose of encouraging civic participation. Therefore, when mail-in ballots were previously already available in Estonia, it is important to question whether i-voting actually provides a significant enough benefit to outweigh the potential costs to election integrity and individuals' privacy.

Conclusion

8 - The intersection between government, digital identity and how it is used in essential democratic functions like voting is very complex. There are benefits to technologies like i-voting – it can make voting more accessible and, in general, can be more convenient than heading to a voting station. However, i-voting also has the risk of creating issues for security or fundamental rights like privacy.

While one may argue that i-voting has fared well in Estonia, it is a wealthy country with a high development index and level of trust in its government, and a close-knit, cohesive society with a population smaller than many of the world's major cities. Furthermore, it has been a leader in the digital transformation of public services since it gained independence from the Soviet Union in the early nineties and has been an early adopter of services like e-IDs and i-voting. This early adoption has led to a feeling of ease and familiarity among Estonians in using such technologies to access important benefits and rights through the state.

Given the unique set of factors that have made it possible for the country to digitize their public services and voting " en masse " in a relatively secure fashion that is largely accepted by its people, is it possible to digitalize voting and other public services in countries that are much larger and more diverse ? Perhaps there will be far more opportunities for the digital identities, especially of marginalized/vulnerable groups, to be compromised. Alternatively, perhaps countries who are more cynical towards their governments and value privacy more will find innovative ways to improve the framework for i-voting Estonia has established.

Parting Thoughts

As you can hopefully see, digital identity is a complex subject that interacts with the law in many different realms of life – be it the public sphere, the private sphere or somewhere in between. An individual's identity is an important construction that is key to one's sense of self, and these online identities, are not solely built by the individual, but rather by a combination of different actors. While we are not able to provide any definitive answers for the road ahead, or what *should* be done to protect or contest our nebulous of online identities, we do hope that we have encouraged and prompted the reader to take an inquisitive look at digital identity systems involved in our everyday lives. By providing background on how actors use digital identity within their constructed system, we invite the reader to question : what might people gain or lose as a result of this use ? By continuing to be critical of digital identity construction and the ways in which digital identity is used, we can help to ensure those wielding power in the digital identity space remain accountable to both individuals and collective communities.■

27. Waqas Chugtai, " Online voting is more available than ever. So what effect does it have on voter turnout ? ", *CBC News*, (Nov. 3, 2022), https ://www.cbc.ca/news/canada/toronto/online-voting-turnout-effect-1.6637975.
28. *Id.*
29. *Id.*
30. Collins English Dictionary, " Definition of 'function creep' ", https ://www.collinsdictionary.com/dictionary/english/function-creep.

Dossier Thématique

6

Law and Technology : Towards a New Digital Rule of Law

Beatriz Botero Arcila,

Assistant Professor of Law at Sciences Po Law School

Lucas Costa dos Anjos,

Postdoctoral research fellow in the New Digital Rule of Law project, and Coordinator of the Digilaw Clinic, at Sciences Po Paris École de Droit

As Scientific Directors of this issue of *La Revue des Juristes de Sciences Po*, we are proud to present a compilation that is both timely and essential : *Law and Technology : " Towards a New Digital Rule of Law "*. The title reflects the ongoing work at the heart of the SciencesPo Law School, and we hope they will elucidate the rationale behind this curated selection of articles, each contributing to our understanding of the relationship between law and the rapidly evolving digital and technological landscapes.

The disruptive nature of digital technologies in trade and market regulation stands out as a significant theme in this issue. Some of the articles in this issue, like those by Professor Burri traces the crucial transition from the early days of digital trade, characterized by non-binding agreements, to the current landscape where such agreements are increasingly binding and enforceable within international trade law. This evolution reflects the broader trends in internet governance and highlights the urgent need for adaptable legal responses to emerging digital paradigms. M^{me} Berrod's piece brings us to the present, while discussing the European effort to regulate artificial intelligence. Professor Dusollier and Professor Sylvain explore the role and power of new digital service providers. Professor Dusollier does it in the context of fair remuneration to authors and performers in music streaming. Professor Sylvain alludes to the need to think about our socio-legal and technical structures beyond the rights-framework in the data protection context.

Simultaneously, the issue delves into the profound impact of technology on the digital rule of law, with a special focus on AI governance and the concept of digital identities. The pieces by Professor Lewkowicz & Ms Sarf and Professor Cabay explore the intersection of fundamental rights with technical standardization, challenging traditional legal concepts in the digital age. These articles offer valuable insights into the necessity of integrating fundamental rights into evolving legal structures, especially as we confront the legal ramifications of artificial intelligence and its applications. Professor de Silva de Alwis' piece on *digitized* gender violence raises attention on some of the contemporary and more urgent forms of challenges and risks to fundamental rights generated by technologies, that ultimately might erode the democratic space.

An integral part of this issue is the *" Bytes and Pieces "* booklet, crafted by the students of the DIGILAW Clinic at SciencesPo Law School, that sheds a complementary perspective on the interactions between law and technology. Their reflections on digital identity explore the nuanced dynamics of power in public-private relationships and the ethical and legal implications of digital identity management. They analyse topics related to the exploitation of personal data in online dating apps, and the risks of internet voting systems, as seen through Estonia's *i-voting* initiative. These discussions are crucial to understanding how digital identities are constructed, managed, and how they can be misused or manipulated, posing significant risks to individual autonomy and democratic participation.

This compilation of articles not only aligns with but is also profoundly informed by the overarching project of the Sciences Po Law School : *Towards a New Digital Rule of Law*. This initiative seeks to address the unique challenges that the internet poses to democratic values and the rule of law. The diverse selection of articles in this issue, from discussions on digital trade to AI governance and the multifaceted nature of digital identity, collectively contribute to a broader understanding of these challenges.

They invite readers to engage critically with the dynamic and challenging intersection of law and technology. Our aim is not to present definitive solutions but to spark intellectual curiosity and critical thinking. Each article, in its way, reflects the complexity and the importance of adapting legal systems to the digital age, highlighting the importance of evolving legal thought to address the intricate hurdles and opportunities presented by digital transformations.

For us, it becomes clear that the law cannot remain static in the face of technological advancement. Instead, it must evolve, incorporating new approaches and rationales to ensure that it remains relevant and effective in safeguarding rights, upholding democratic values, and promoting

the common good in our digital era. This issue of *La Revue des Juristes de Sciences Po* represents a step towards understanding and shaping a new digital rule of law, one that is responsive to the needs and challenges of our time. Thus, this issue serves as a reminder of our commitment to fostering a nuanced dialogue on the intersection of law and technology. We hope that it will inspire our readers to reflect on the role of law in our digital society and contribute to the ongoing discourse on how we can collectively shape a just, equitable, and democratic digital future.■

Introduction

7 Conférence inaugurale du diplôme universitaire « Droit et technologies du numérique » de Paris II (jeudi 14 septembre 2023)

Le droit et le numérique

Bernard STIRN,

Président de section honoraire au Conseil d'État,
secrétaire perpétuel de l'Académie des sciences morales et politiques

1 - Sans être d'aucune façon un spécialiste des questions numériques, qui me restent au contraire à bien des égards mystérieuses, et alors que j'ai souvent le sentiment de me trouver du mauvais côté de la « fracture numérique », j'ai volontiers accepté l'honneur que vous me faites ce soir en me conviant à prononcer la conférence inaugurale de votre diplôme universitaire. Si je n'ai pas hésité à répondre positivement, et peut-être imprudemment, à cette invitation, c'est d'abord parce qu'elle venait du professeur Simon Porcher, qui me rappelait qu'il avait naguère suivi mes cours à Sciences Po. C'est aussi parce que j'ai pu mesurer au cours d'une carrière professionnelle commencée au Conseil d'État à une époque où les seuls outils étaient le stylo, la gomme et la colle, combien le numérique avait modifié les méthodes et les conditions de travail des juridictions. C'est enfin parce que nombre de grands débats d'aujourd'hui sur les libertés concernent la régulation juridique de l'internet, des réseaux sociaux, des géants du numérique.

À défaut de vous apporter la compétence d'un expert, je vais donc essayer de vous délivrer un témoignage et de m'interroger avec vous sur des questions qui demeurent largement ouvertes et évolutives. Le temps d'échange qui suivra mon propos nous permettra d'éclairer ensemble un peu davantage ces vastes sujets.

Comme les autres domaines, le droit et le travail des juridictions ont connu de véritables transformations sous l'effet de la révolution numérique. En retour le droit et les juges se trouvent confrontés à des questions inédites qui les conduisent à essayer de donner à l'univers du numérique un cadre juridique approprié et garant des droits fondamentaux. Aussi pouvons-nous constater un mouvement réciproque : le numérique influe sur le droit et sur les juges, le droit et les juges influent sur le numérique.

1. Le numérique influe sur le droit et sur les juges

2 - Au cours du dernier demi-siècle, les effets du numérique ont conduit à la fois à la naissance d'une nouvelle branche du droit et à de profondes évolutions dans le travail des juges.

A. - Le droit du numérique, une nouvelle branche du droit

3 - Le droit du numérique se construit au travers d'une dialectique efficace entre droit national et droit européen.

Un rôle pionnier a été joué par la France dans ce processus. La loi du 6 janvier 1978 relative aux fichiers, à l'informatique et aux libertés est en effet le premier grand texte qui se saisit des questions alors toutes nouvelles posées par l'apparition et par les premiers développements de l'informatique. [1] Elle pose des principes fondateurs, en matière de droit d'accès et de rectification, de protection des données sensibles, d'interdiction de faire apparaître les origines raciales, les opinons politiques, philosophiques ou religieuses, les appartenances syndicales. [2] Selon une formule à l'époque novatrice et appelée à un grand avenir, elle confie à une autorité administrative indépendante, la Commission nationale de l'informatique et des libertés (CNIL), la mission de veiller au respect des prescriptions qu'elle édicte et, le cas échéant, d'infliger des sanctions. [3] On connaît le succès de l'institution, qui déploie une intense activité et s'est forgée une autorité incontestée. En 2022, la CNIL a examiné plus de 13 000 plaintes, adressé 147 mises en demeure, infligé 21 sanctions pour un montant total supérieur à 100 millions d'euros. [4]

La loi du 7 octobre 2016 pour une République numérique a prolongé le mouvement en ouvrant la voie vers l'*open data*, qui assure un libre accès à l'ensemble des données publiques. [5]

Le droit national s'inscrit dans l'espace européen. En particulier, l'article 8 de la Charte des droits fondamentaux de l'Union européenne protège très fortement les données personnelles. [6] Sur son fondement ont été adoptés le Règlement général pour la protection des données personnelles (RGPD) du 27 avril 2016, [7] et la directive du même jour qui concerne les traitements relatifs à la préven-

1. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
2. *Ibid*.
3. *Ibid*.
4. CNIL, « *Le rapport annuel 2022 de la CNIL* », [https ://www.cnil.fr/fr/le-rapport-annuel-2022-de-la-cnil].
5. Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.
6. Charte des droits fondamentaux de l'Union européenne, art. 8.
7. Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

tion et à la répression des infractions. [8] En octobre 2022 sont publiés deux règlements, le *Digital Services Act* (DSA) et le *Digital Markets Act* (DMA), qui imposent aux opérateurs des obligations renforcées en matière de lutte contre les contenus illégaux, d'appels à la haine ou à la discrimination, d'atteintes aux processus électoraux. [9] D'une grande qualité, ces instruments de droit dérivé ont une portée qui dépasse les frontières de l'Union pour s'imposer à tous les géants de l'internet. Ils démontrent la capacité de l'Union à peser sur les débats mondiaux et à conférer à son droit, lorsqu'il est bien conçu, une portée extraterritoriale.

Le droit national est modifié en retour de manière à être en pleine conformité avec le droit de l'Union. Après le RGPD a ainsi été votée la loi du 20 juin 2018 relative à la protection des données, [10] puis l'ordonnance du 12 décembre 2018 a opéré une refonte de la loi du 6 janvier 1978. [11] Un code du numérique, qui pourrait aussi couvrir la communication audiovisuelle, reste sans doute à bâtir pour mieux ordonner notre droit interne. Mais nul doute que le droit du numérique est pleinement devenu une branche du droit. Le numérique a en même temps transformé le travail des juges.

B. - La révolution numérique, une transformation de l'activité des juridictions

4 - La révolution numérique a porté sur tous les aspects de la vie des juridictions. Le travail quotidien des magistrats, les relations avec les parties, l'accès aux décisions de justice ont été profondément modifiés. Les défis de l'intelligence artificielle soulèvent pour l'avenir de nouvelles questions.

Le travail des juges est longtemps demeuré solitaire et artisanal. Chacun effectuait des recherches dans les ouvrages et les recueils, photocopiait les documents principaux, rédigeait à la main rapports et projets de décision. Ces souvenirs, qui sont ceux de mes premiers pas au Conseil d'État en 1976, témoignent d'une époque qui paraît lointaine tant les évolutions commencées dans la seconde moitié des années 1980 ont été rapides et considérables. Elles ont été d'autant plus facilement accueillies qu'elles rapprochaient le travail juridictionnel des autres activités et qu'elles répondaient fort bien à ses besoins. Pour rechercher les textes et les précédents, le numérique permet d'aller plus vite et avec davantage de sûreté. Les modifications des projets de décision au fur et à mesure des délibérations successives sont apportées plus facilement et plus clairement sur un document d'ordinateur que sur un papier maintes fois corrigé et raturé. Les courriers électroniques facilitent les échanges avec les collègues. En deux décennies environ, tous les magistrats ont abandonné le stylo pour la souris, sont devenus familiers des banques de données, qu'elles soient celles des éditeurs juridiques ou celles constituées par les juridictions elles-mêmes pour leur travail interne, ont engagé avec leurs collègues des processus de travail dits « collaboratifs » au travers de documents joint à des mails. La crise de la covid-19 a ouvert d'autres pistes encore, en particulier de séances par voie de téléconférence. Le Conseil constitutionnel, le Conseil d'État et la Cour de cassation ont cependant rappelé, par des décisions convergentes, que, même en période d'état d'urgence sanitaire, la prolongation des gardes à vue ne pouvait être automatique [12] et que la personne poursuivie devait pouvoir comparaître physiquement devant les juridictions répressives [13].

Les changements n'ont pas été moindres dans les relations avec les justiciables. A l'époque des courriers recommandés, des copies de mémoires, des volumineux dossiers a succédé le temps de la téléprocédure. Un portail du justiciable s'est ouvert devant les juridictions civiles. Devant le juge administratif, les applications « Télérecours » et « Télérecours citoyens » permettent d'assurer toutes les étapes de la procédure par voie électronique, dépôt des requêtes, échanges de mémoires, notification des décisions. Le mode numérique est même obligatoire pour les collectivités publiques, à l'exception des communes de moins de 3500 habitants, et pour les avocats. Tous se sont habitués à ces évolutions, qui sont source d'économies et facilitent le travail quotidien.

Toutes les décisions juridictionnelles sont enfin gratuitement accessibles en ligne. [14] Cela impose au préalable l'anonymisation du nom des parties et parfois, en cas de danger pour la sécurité ou la vie privée des intéressés, une anonymisation complémentaire pour les magistrats, les agents de greffe ou certains tiers. Le Conseil d'État et la Cour de cassation ont la responsabilité de la diffusion en ligne des décisions des juridictions de leur ordre. Depuis 2021, les décisions du Conseil d'État et les arrêts de la Cour de cassation sont tous accessibles en ligne. Pour les jugements des autres juridictions, le calendrier est échelonné jusqu'à 2025 [15]. On peut certes parfois regretter qu'un numéro remplace le nom du requérant, teinté de davantage d'humanité et plus facile à mémoriser. On peut davantage encore s'inquiéter d'une masse de décisions accessibles sans classement ni hiérarchie. Des travaux sont en tout cas à mener pour mieux organiser, présenter, analyser un volume considérable de décisions qu'une simple accumulation rendrait vite écrasant sans être véritablement éclairant. Une telle mise en ordre s'impose en particulier dans la perspective, parfois inquiétante, de l'utilisation par la justice de l'intelligence artificielle.

Des apports incontestablement positifs découlent certes de l'intelligence artificielle. Elle procure, en particulier, des informations qui permettent d'éviter les procès inutiles, de disposer de barèmes, de faciliter les actions collectives et les actions de groupe, de recentrer le juge sur les questions délicates. Mais l'intelligence artificielle présente aussi de réels dangers, en termes de profilage des juridictions voire des juges, de fixité et d'automaticité de la jurisprudence, de biais dans la construction des algorithmes. Lors d'un colloque organisé sur le sujet en février 2018, Jean-Marc Sauvé, alors vice-président du Conseil d'État, déclarait : « Le risque des logiciels prédictifs est que le juge, sous l'effet de la surveillance résultant d'un traitement massif de décisions de justice, perde sa liberté d'appréciation et son indépendance et préfère se ranger, par « sécurité », à l'opinion dominante ou majoritaire de ses pairs. Or le propre de la justice est que chaque affaire soit examinée pour ce qu'elle est, avec sa part d'originalité et d'irréductible complexité qui ne saurait être systématisée par un logiciel, aussi puissant soit-il ». [16]

Avec les développements de « Chat GPT », on pourrait imaginer des jugements entièrement rédigés par l'intelligence artificielle. Nul

8. Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.
9. Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) (Texte présentant de l'intérêt pour l'EEE) ; Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques).
10. Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.
11. Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel.
12. Cass., crim., 26 mai 2020,n° 20-81.971 ; CC, décision n° 2020-878/879 QPC du 29 janv. 2021.
13. CC, décision n° 2020-872 QPC du 15 janv. 2021 ;CE, réf., 27 nov. 2020, n° 446712 : Lebon (*Association des avocats pénalistes*) ; CE, 5e et 6e Ch. réun. 5 mars 2021, n° 440037 (*Ordre des avocats au Conseil d'État et à la Cour de cassation et autres*).
14. Légifrance, « Légifrance », [https ://www.legifrance.gouv.fr/].
15. Arrêté du 28 avril 2021 pris en application de l'article 9 du décret n° 2020-797 du 29 juin 2020 relatif à la mise à disposition du public des décisions des juridictions judiciaires et administratives.
16. Conseil d'État, « La justice prédictive », 12 févr. 2018 [https://www.conseil-etat.fr/publications-colloques/discours-et-interventions/la-justice-predictive].

doute que des précautions sont à prendre pour assurer la capacité créatrice de la jurisprudence, préserver la liberté d'appréciation du juge, garantir la neutralité et la transparence des algorithmes. Prenons garde que l'intelligence artificielle ne vienne multiplier le nombre de ceux qui déclareraient, comme Alceste dans le Misanthrope de Molière : « J'ai pour moi la justice et je perds mon procès ». [17] Il importe en tout cas que demeure vraie la phrase du bâtonnier Jacques Charpentier, dans ses Remarques sur la parole, publiées en 1961 et rééditées en 2018 par le professeur Bruno Dondero et par Bertrand Périer, avocat au Conseil d'État et à la Cour de cassation : « Nul prophète ne saurait prévoir quelles seront, tel jour, à telle heure, les réactions de trois juges, en présence de telle affaire, exposée par tel avocat ». [18]

Si le numérique influe sur le droit et les juges, la réciproque est également vraie.

2. Le droit et les juges influent sur le numérique

5 - Nul ne peut songer à arrêter les progrès du numérique. Mais l'utilisation incontrôlée des instruments qui en découlent ne serait pas sans danger pour le débat public et pour les libertés de chacun. De nouveaux défis sont en conséquence à relever, qui appellent un encadrement par le droit et demandent l'attention et la créativité des juges.

A. - Le nécessaire encadrement du numérique par le droit

6 - Des enjeux difficiles sont à relever pour que le développement du numérique, au travers, en particulier, des réseaux sociaux, se fasse dans un cadre respectueux de la liberté individuelle, de la vie privée, de la cohésion de la société, des exigences de la sécurité collective. Il s'agit de concilier la liberté d'expression et la protection des personnes, d'éviter la diffusion des propos haineux, des discours discriminatoires, des appels à la violence, de conférer les moyens nécessaires aux autorités chargées d'assurer le maintien de l'ordre public et de poursuivre les auteurs d'infractions pénales.

La démocratie elle-même se trouve en question. « La liberté de parler s'est perdue dans la viralité » nous dit Monique Canto-Sperber. [19] Et mon confrère Daniel Andler écrit dans son ouvrage Intelligence artificielle, intelligence humaine, La double énigme : « Les libertés démocratiques sont mises en danger par les systèmes de surveillance fondés sur l'intelligence artificielle ». [20] Nul doute qu'au regard de la puissance des géants de l'internet, du champ mondial de leur domaine d'action, des défis immenses se posent, en termes de liberté, de souveraineté, d'effectivité.

Une certaine autorégulation est certes assurée par les grands opérateurs eux-mêmes. Facebook s'est doté en 2018 d'un « conseil de surveillance », qui se prononce sur les litiges relatifs au contenu des messages circulant sur le réseau. [21] Après l'assaut contre le Capitole, Twitter a fermé en janvier 2021 le compte de Donald Trump, qu'Elon Musk a rouvert en novembre 2022. [22]

Mais ces procédures internes, qui n'offrent ni transparence ni garanties d'impartialité, ne sauraient en aucun cas suffire. Il revient aux autorités publiques d'affirmer des principes de loyauté de la collecte, de proportionnalité du traitement aux buts recherchés, d'exactitude des données, de droit à la rectification et à l'effacement. Des procédures sont à définir pour affirmer la responsabilité des auteurs de traitement et des gestionnaires de réseau, organiser les voies de recours, ouvrir aux autorités policières et judicaires les voies et moyens d'exercer leur mission.

Ces préoccupations sont ressenties dans l'ensemble des pays. Elles se sont traduites par des textes dans les droits nationaux comme dans le droit européen.

L'équilibre est parfois délicat à trouver. Ainsi le Conseil constitutionnel a censuré la proposition de loi Avia, qui reposait pourtant sur de bonnes intentions. Tout en rappelant que l'appel à la haine sur internet constitue un abus de la liberté d'expression et de communication qui porte gravement atteinte à l'ordre public et aux droits des tiers, il a jugé que le dispositif retenu par le législateur, avec notamment la création d'un délit de refus de retrait dans les vingt-quatre heures de contenus manifestement illicites au regard de leur caractère haineux, n'était pas assorti de garanties suffisantes et faisait peser sur les opérateurs des contraintes excessives [23]. En revanche, il a estimé conformes à la Constitution des mesures mieux définies, adoptées pour transposer la directive européenne relative à la diffusion en ligne de contenus à caractère terroriste [24].

Les mêmes difficultés de juste équilibre se retrouvent au regard des impératifs de sécurité. Restrictive dans l'appréciation de ces impératifs, la Cour de justice de l'Union européenne n'admet pas que les États membres imposent aux fournisseurs de services de communication électronique une obligation générale et indifférenciée de conservation des données [25]. Devant les réactions de plusieurs cours nationales, soucieuses de préserver les moyens d'action de la police et des autorités judicaires, elle n'a apporté une atténuation à cette jurisprudence qu'en cas de « menace grave pour la sécurité nationale » [26]. Et il a fallu au Conseil d'État une forte logique conciliatrice pour juger que le droit de l'Union, tel qu'interprété par la Cour de justice, ne compromet cependant pas les exigences constitutionnelles que sont la sauvegarde des intérêts fondamentaux de la Nation, la prévention des atteintes à l'ordre public, la lutte contre le terrorisme et la recherche des auteurs d'infractions pénales. Le Conseil d'État a, en effet, estimé que la conservation des données de connexion imposée aux opérateurs par le droit français était pour l'essentiel justifiée, conformément aux principes posés par la Cour de justice, par les exigences de la sécurité nationale. Il a seulement rappelé que les besoins et les menaces devaient faire l'objet d'un réexamen périodique [27]. Ces jurisprudences croisées du juge européen et des juges nationaux font déjà ressortir combien le numérique fait appel à l'attention et à la créativité des juridictions.

B. - L'attention et la créativité des juges devant le numérique

7 - Une jurisprudence à la fois attentive et créative des différentes juridictions nationales et européennes consacre le numérique comme une source de droits fondamentaux tout en veillant à entourer son utilisation de précautions nécessaires à la garantie des libertés.

Particulièrement significative de l'affirmation des droits fondamentaux issus du numérique est la décision par laquelle le Conseil constitutionnel a jugé que la liberté de communication, proclamée par la Déclaration des droits de l'homme, comporte aujourd'hui celle « d'accéder aux services de communication au public en

17. Molière, *Le Misanthrope* : Hachette, 2013, V, 1, v. 1492-1498.
18. B. DONDERO et B. PERIER, « Préface », in J. CHARPENTIER, *Remarques sur la Parole*, LGDJ, Coll. Anthologie du Droit, 2e éd., 2018, p. 5.
19. C. Legros, La liberté d'expression à l'heure du numérique ou la difficile quête de l'équilibre sur les réseaux sociaux, Le Monde, 2 avril 2021 [https ://www.lemonde.fr/idees/article/2021/04/02/reseaux-sociaux-et-liberte-d-expression-inventer-des-dispositifs-pour-proteger-nos-democraties_6075320_3232.html].
20. D. Andler, Intelligence artificielle, intelligence humaine : la double énigme : Gallimard, 2023.
21. Meta, « *Lancement du Conseil de surveillance* », 6 mai 2020 [https://about.fb.com/fr/news/2020/05/lancement-du-conseil-de-surveillance/].
22. Le Monde avec AFP, « Le compte Twitter de Donald Trump rétabli par Elon Musk », 20 novembre 2022 [https://www.lemonde.fr/pixels/article/2022/11/20/le-compte-twitter-de-donald-trump-retabli-par-elon-musk_6150712_4408996.html].
23. CC, décision n° 2020-801 DC du 18 juin 2020.
24. CC, décision n° 2022-841 QPC du 13 août 2022.
25. CJUE 21 déc. 2016, C-203/15 et C-698/15, *Tele2 Sverige*.
26. CJUE 6 oct. 2020, C-623/17, C-511/18, C-512/18, C-520/18.
27. CE, 21 avril 2021, n° 393099 : Lebon (*société French Data Network*).

ligne, eu égard au développement généralisé d'internet et à son importance pour la participation à la vie démocratique et à l'expression des idées et des opinions ». Le juge constitutionnel en déduit que des restrictions d'accès au réseau ne peuvent résulter que d'une décision de l'autorité judiciaire et ne sauraient être décidées par une autorité administrative de régulation [28].

Des précautions s'imposent néanmoins, en particulier pour le recueil des données sensibles, la protection des données personnelles, la garantie d'un droit à l'oubli numérique. Sur ces trois points, quelques décisions à la fois emblématiques et concordantes méritent d'être rappelées.

Le Conseil d'État a précisé qu'un fichier relatif aux aides accordées aux rapatriés d'Afrique du Nord ne peut faire apparaître, même indirectement, leur appartenance religieuse [29]. Il a rappelé que le juge doit pouvoir vérifier la pertinence des informations contenues dans un fichier, même s'il s'agit d'un traitement non publié pour des motifs de sécurité publique, comme le fichier CRISTINA que tenait la direction centrale du renseignement intérieur [30]. Il contrôle la nature des informations recueillies et la durée de leur conservation au regard de la finalité du traitement, qu'il s'agisse du fichier ELOI relatif à l'éloignement des étrangers [31] ou de la « base-élèves » des services de l'Education nationale [32]. Une même attention aux données sensibles est portée par le Conseil constitutionnel lorsqu'il censure la loi qui crée, sans l'encadrer suffisamment, un fichier d'identité comprenant des données biométriques [33] ou un registre national des crédits aux particuliers destiné à recenser l'ensemble des incidents de paiement liés à ces crédits [34].

La Cour de justice de l'Union européenne témoigne d'une grande attention à la protection des données personnelles. Elle a, pour la première fois, censuré une directive au regard de la Charte des droits fondamentaux en jugeant que la directive du 15 mars 2006 sur la conservation des données à caractère personnel ne comportait pas les garanties impliquées par la Charte [35]. Elle fait preuve de la même rigueur au regard des accord internationaux conclus par l'Union. Elle a ainsi invalidé l'accord entre l'Union européenne et le Canada sur le transfert des données des dossiers passagers (PNR) [36] et censuré à deux reprises, sur la saisine d'un entreprenant étudiant en droit autrichien, Maximilian Schrems, un accord avec les États-Unis sur le transfert de données personnelles [37]. Une même vigilance inspire la Cour européenne des droits de l'homme. Elle précise ainsi que les systèmes de surveillance de masse des données informatiques doivent être suffisamment encadrés par la loi et elle observe à cet égard des insuffisances au Royaume-Uni et en Suède [38].

La Cour de justice a aussi proclamé le droit à l'oubli numérique [39]. Elle a indiqué qu'il revient aux juridictions nationales d'assurer l'équilibre entre le droit à l'information et celui de ne pas voir indéfiniment associé à son nom, sur internet, des données, même exactes, relatives à des antécédents judiciaires ou à la vie personnelle. Sa décision ajoute qu'un déréférencement exigé par le droit de l'Union s'applique sur le territoire de l'Union et que si le droit de l'Union n'impose pas un déréférencement mondial, il n'interdit pas non plus de l'exiger lorsque les caractéristiques d'une affaire le justifient [40]. Dans le cadre ainsi tracé, le Conseil d'État a tranché différents cas d'espèce, en précisant que l'arbitrage entre le droit au déréférencement et le droit à l'oubli dépend de la nature des données en cause, de leur contenu, des conditions et de la date de la mise en ligne ainsi que de la notoriété de la personne concernée, de son rôle dans la vie publique et de sa fonction dans la société [41]. La Cour de Karlsruhe juge dans le même sens qu'une personne condamnée pour meurtre en 1982 peut exiger que son nom ne soit plus associé à cette condamnation « tant d'années après les faits » [42]. Une inspiration analogue se retrouve sur l'autre rive de l'Atlantique lorsque la Cour suprême du Canada enjoint à Google de procéder à un déréférencement à l'échelle mondiale, en indiquant qu'« Internet n'a pas de frontière – son habitat naturel est mondial » [43]. De son côté, la Cour européenne des droits de l'homme juge que l'obligation de déréférencement s'impose non seulement aux moteurs de recherche mais aussi aux responsables de journaux en ligne, sans qu'il en résulte une atteinte excessive à la liberté de la presse [44], au respect de laquelle on sait qu'elle est très attentive.

Un vaste mouvement d'interférences réciproques est ainsi engagé entre le droit et le numérique. Votre diplôme universitaire vous permettra d'en appréhender les différents éléments, dont j'ai seulement essayé de retracer les grandes lignes, d'en approfondir l'analyse, d'en suivre l'évolution puisqu'il s'agit d'une matière encore récente et qui connaît sans cesse de nouveaux développements techniques et juridiques. La régulation des géants du numérique, l'utilisation maîtrisée de l'intelligence artificielle, en particulier, sont de vastes chantiers qui ont pour enjeu la démocratie. Dans son livre, *Les ingénieurs du chaos*, Giuliano da Empoli montre combien les manipulations des réseaux numériques sont susceptibles d'empoisonner la vie publique. Il écrit que « pour les ingénieurs du chaos le populisme naît de l'union de la colère avec les algorithmes ». [45] Votre diplôme universitaire sur le droit et le numérique est le meilleur antidote à ces périls. Nul doute qu'avec lui, vous empruntez, sous la conduite du professeur Simon Porcher et de Gabriel Sebban, maître de conférences, une voie passionnante, pleine de progrès, riche de promesses intellectuelles et professionnelles. Tous mes vœux cordiaux et confiants vous accompagnent sur ce chemin.■

28. CC, décision n° 2009-580 DC du 10 juin 2009.
29. CE, Sect., 5 juin 1987, n° 59674 (*Kaberseli*).
30. CE, 31 juil. 2009, n° 320196 : Lebon (*association AIDES*).
31. CE, 30 déc. 2009, n° 312051 : Lebon (*association SOS-Racisme*).
32. CE, 19 juil. 2010, n° 334014 (*M. Fristot et M^me^ Charpy)*.
33. CC, décision n° 2012-652 DC du 22 mars 2012.
34. CC, décision n° 2014-690 DC du 13 mars 2014.
35. CJUE 8 avril 2014, C-293/12 et C-594/12, *Digital Rights Ireland et Seitlinger* e.a..
36. CJUE 26 juil. 2017, 1/15 AVIS.
37. CJUE 6 oct. 2015, C-362/14, *Maximilian Schrems* et 16 juil. 2020, C-311/18, *Facebook Ireland et Schrems*.
38. CEDH 25 mai 2021, n° 58170/13, 62322/14 et 24960/15 *Big Brother Watch c/ Royaume-Uni* et 25 mai 2021, n° 35252/08, *Centrum för Rättvisa c/ Suède*.
39. CJUE 13 mai 2014, C-131/12, *Google Spain et Google*.
40. CJUE 24 sept. 2019, C-507/17, *Google*.
41. CE, 6 déc. 2019, n° 391000, 393769, 395335, 397755, 399999, 401258, 403868, 405464, 405910, 407776, 409212, 423326 et 429154.
42. Bundesverfassungsgericht, 27 nov. 2019, 1 BvR 16/13.
Berlin (AFP), La justice allemande renforce le droit à l'oubli sur internet, France 24, 27 novembre 2019,
[https://www.france24.com/fr/20191127-la-justice-allemande-renforce-le-droit-%C3%A0-l-oubli-sur-internet].
43. Google Inc. c. Equustek Solutions Inc., [2017] 1 R.C.S. 824
44. CEDH 25 nov. 2021, n° 77419/16, *Biancardi c/ Italie*.
45. G. da Empoli, *Les ingénieurs du chaos* : Folio, 2019.

The disruptive nature of tech in the field of trade and market regulation

8 The Digital Transformation of Trade Law

Mira BURRI,

Professor of International Economic and Internet Law
at the Faculty of Law of the University of Lucerne, Switzerland

The article explores the transformations triggered by digitalization in the domain of global trade law and evaluates the nature and the effects of the unfolding legal adaptation in this field of international law. After a brief introduction into the sweeping effects of digitalization on trade, the article discusses the deliberate regulatory responses to the challenge of digitalization formulated in free trade agreements (FTAs), with a particular focus on the most advanced models of digital trade regulation, including the newer generation of Digital Economy Agreements (DEAs). The article seeks to contextualize and assess the impact of the existing and evolving legal framework and its adequacy for the contemporary data-driven economy. It also points at some deficiencies in the ongoing transformation of digital trade law and potential setbacks going forward.

Introduction

1 - " Electronic commerce " [1] or " digital trade ", [2] as it is now more frequently referred to, has been one of the very few areas of international economic law where one can observe patterns of regulatory cooperation and new rulemaking across different venues. It could be argued that electronic commerce is an old trade negotiation topic, and it is only natural that now, over two decades after the adoption of the 1998 Work Programme on Electronic Commerce by the members of the World Trade Organization (WTO), [3] there is some actual progress. Such an assumption of linear development would however be flawed. Not only have the scope and the contents of the negotiation topic of e-commerce profoundly changed, but also how governments now approach the digital economy as a set of regulatory questions that go beyond the mere liberalization of pertinent services sectors and the reduction of tariff and non-tariff barriers to trade. [4]

The article delves into this new complexity and seeks to show the transformation of the regulatory topic from trade law 2.0 (as the mere trade in goods and services online) towards trade law 4.0 (as the regulation of the data-driven economy). [5] It further explores the dynamics of digital trade regulation in the past decade in a complex geopolitical setting by looking at some broader trends, as well as at distinct regulatory models endorsed by free trade agreements (FTAs) and the new templates of the Digital Economy Agreements (DEAs) that also signal room for innovation in trade law. The article goes then back to the multilateral forum of the WTO and reveals how FTAs have worked as regulatory laboratories and asks whether their results can be translated to the WTO. The article concludes with some thoughts on how the topic of digital trade, as linked to the underlying digitalization processes, is transforming global trade law – with both strands of legal innovation and certain setbacks that are linked to geopolitical differences on the one hand and on the other hand, to the difficulties of interfacing domestic governance regimes with commitments in the domain of digital trade law, as countries have their own sensibilities and public policy objectives.

1. From Trade 2.0 to Trade 4.0

2 - The process of adapting trade law to digitalization started early on, as the WTO members launched in 1998 a Work Programme on Electronic Commerce that sought to explore (albeit without a negotiating mandate) the implications of the Internet for trade in goods, trade in services and the protection of intellectual property (IP) rights. In the two decades since the WTO initiative, much has changed, however. Policymakers now increasingly focus on a new set of issues – in particular around the data-driven economy. [6] There are good reasons for this shift : first, it can well be justified by the advanced digitalization and specifically, the critical importance of data to societies. In the context of trade policies, this has translated to ensuring data flows across borders, as data is embedded in a growing number of services and goods and there is critical interdependence between cross-border data flows and digital growth and innovation – in existing sectors but also in emerging domains, such as artificial intelligence (AI) or the Internet of Things (IoT). [7] The second reason can be linked to a new set of regulatory questions that the use of data and its borderless nature have opened – in particular those around data sovereignty and the protection of privacy, national security and other domestic values and interests. [8] What is apparent in this context, as the article discusses below, is that the emerging digital trade law seeks to

1. The WTO Work Programme on Electronic Commerce defined " electronic commerce " as " the production, distribution, marketing, sale or delivery of goods and services by electronic means ". See WTO, Work Programme on Electronic Commerce, WT/L/274, at para. 1.3 (30 September 1998). The WTO continues to use " e-commerce " under the Joint Initiative (see WTO, Joint Statement Initiative on Electronic Commerce, WT/L/1056, 25 January 2019) but in recent texts uses " digital trade " as alternative language.
2. While there is no single definition, a joint effort by the IMF, OECD, UN, and WTO defines " digital trade " as " all international trade that is digitally ordered and/or digitally delivered ". See IMF, OECD, UN and WTO, *Handbook on Measuring Digital Trade*, 2nd ed. (2023) ; also M. Burri & A. Chander, " What Are Digital Trade and Digital Trade Law ? ", *AJIL Unbound* 117 (2023), 99-103.
3. WTO (1998), supra note 1.
4. See e.g., S.J. Evenett & J. Fritz, *Emergent Digital Fragmentation : The Perils of Unilateralism* (CEPR Press, 2022).
5. Trade law 1.0 can be defined as analogue trade, while trade law 3.0 would correspond to the state of digital trade that already includes global value chains and advanced services trade but does not yet account for the importance of data flows.
6. See e.g., M. Burri (ed), *Big Data and Global Trade Law* (Cambridge University Press, 2021) ; S. Peng, C. Lin & T. Streinz (eds), *Artificial Intelligence and International Economic Law* (Cambridge University Press, 2021).
7. See e.g., A. Chander, " AI and Trade ", in M. Burri (ed), *Big Data and Global Trade Law* (Cambridge University Press, 2021), 115-127.
8. See e.g., M. Burri, " Interfacing Privacy and Trade ", *Case Western Journal of International Law* 53 (2021), 35-88 ; A. Chander & P.M. Schwartz, " Privacy and/or Trade ", *University of Chicago Law Review* 90 (2023), 49-135.

address these new regulatory issues that go beyond classic WTO topics – such as reduction of tariffs or services liberalization, and targets domestic regimes.

2. Digital Trade Rulemaking in Free Trade Agreements

A. - Overview

3 - The regulatory environment for digital trade has been shaped by FTAs. Of the 433 PTAs signed between January 2000 and November 2023, 214 contain provisions relevant for e-commerce/digital trade, and 122 have dedicated e-commerce/digital trade chapters, [9] with the significant jump in these commitments occurring in the past few years. Although the pertinent rules are still heterogeneous and differ as to issues covered, the level of commitments and their binding nature, it is overall evident that the trend towards more and more detailed provisions on digital trade has intensified significantly over the years. The relevant aspects of digital trade governance are spread across the treaties and can be found in : (1) the specifically dedicated electronic commerce chapters ; (2) the chapters on cross-border supply of services (with particular relevance of the telecommunications, computer and related, audiovisual and financial services sectors) ; as well as in (3) the IP chapters. [10] This article's single focus is on the electronic commerce/digital trade chapters and the DEAs, which have become the source of expansive rulemaking and illustrate well the importance of the new data economy issues.

One can group the digital trade chapter rules into two loose categories : (1) rules that seek to facilitate digital trade and (2) rules that deal with data governance issues, including the key topic of data flows. While in the first cluster of issues the number of FTAs that contain such rules is substantial, there is a greater variety in the second cluster with fewer agreements with rules on data, as well as various conditionalities attached to them.

B. - Trends and Models in Digital Trade Rulemaking

4 - There are different ways of mapping the landscape of digital trade rulemaking. Most of the existing enquiries follow a country-based approach and sketch the emergent models of the main stakeholders – the United States (US), the European Union (EU) and China. [11] This article adopts a slightly different method and starting with one basic model – that of the 2018 Comprehensive and Progressive Agreement for Transpacific Partnership (CPTPP) – traces the rule-frameworks, especially the most recent treaties that are representative of the current actors " positioning, that go beyond it (" CPTPP-plus ") or diverge from it (" CPTPP-minus "). The CPTPP is a suitable starting point, as it is the first FTA with a sophisticated electronic commerce chapter [12] ; it is a mega-regional treaty with multiple signatories, [13] whose impact has been augmented with the accession of the United Kingdom (UK) and pending applications by a number of countries, such as China, Taiwan, Ecuador and Costa Rica ; the final reason stems from the fact that the CPTPP digital trade model has diffused in a substantial number of subsequent agreements. [14]

The CPTPP contains important provisions that seek, on the one hand, to facilitate digital trade by providing a level of interoperability between domestic regulatory regimes and on the other, to curb data protectionism. Illustrative of the first category are the rules on the domestic electronic transactions framework with binding obligations for the parties to follow the principles of the UNCITRAL Model Law on Electronic Commerce 1996 or the UN Convention on the Use of Electronic Communications in International Contracts. [15] The provisions on paperless trading and on electronic authentication and electronic signatures complement this by securing equivalence of electronic and physical forms. [16] Furthermore, in terms of conditioning the domestic regulatory environment, the CPTTP e-commerce chapter includes provisions, albeit in a soft law form, on consumer protection, [17] spam control, [18] net neutrality, [19] as well as on cybersecurity. [20] The CPTPP also addresses the new importance attached to data protection – yet, there seems to be a prioritization of trade over privacy rights, as there is no reference to benchmarks and weaker protection schemes at home would suffice. [21] This reflects the US stance, as the US has (at least thus far) a fragmented privacy protection regime with relatively low standards, which has also been problematic in securing transatlantic data flows. [22]

In the second category of data-relevant rules, the CPTPP includes a clear ban on localization measures, [23] a ban on forced technology transfer of source code, [24] as well as a hard rule on free data flows, explicitly including personal information. [25] While certain restrictions are permitted if they do not amount to " arbitrary or unjustifiable discrimination or a disguised restriction on trade " and " impose restrictions on transfers of information greater than are required to achieve the objective ", [26] the scope of the exception is unclear. [27] This can be linked to legal uncertainty, as well as unworkable safeguards for domestic constituencies, as pointed out by New Zealand's Waitangi Tribunal with regard to the rights of the Maori. [28]

The CPTPP model has been replicated and expanded by subsequent US agreements, which also confirmed the liberal US approach to digital trade, as initiated by its 2001 " Digital Agenda ". The renegotiated NAFTA, which is now referred to as the " United States-Mexico-Canada Agreement " (USMCA) follows all critical lines of the CPTPP with regard to both the facilitation of digi-

9. This analysis is based on a dataset of all data-relevant norms in trade agreements (TAPED) administered by the University of Lucerne. For all data, see https ://unilu.ch/taped.
10. For analysis of all relevant chapters, see M. Burri, " The Regulation of Data Flows in Trade Agreements ", *Georgetown Journal of International Law* 48 (2017), 408-448.
11. See e.g., H. Gao, " Digital or Trade ? The Contrasting Approaches of China and US to Digital Trade ", *Journal of International Economic Law* 21 (2018), 297-321 ; M. Burri, " Data Flows and Global Trade Law ", in M. Burri (ed), *Big Data and Global Trade Law* (Cambridge University Press, 2021), 11-41 ; M. Burri, " The Impact of Digitalization on Global Trade Law ", *German Law Journal* 24 (2023), 551-573.
12. The chapter is identical with the negotiated electronic commerce provisions under the Transpacific Partnership Agreement (TPP), so the influence of the US position on digital trade is discernible.
13. CPTPP parties are Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Vietnam. The US withdrew from the preceding TPP negotiations with the start of the Trump administration.
14. See e.g., the 2016 Chile-Uruguay FTA, the 2016 updated Singapore-Australia FTA (SAFTA), the 2017 Argentina-Chile FTA, the 2018 Singapore-Sri Lanka FTA, the 2018 Australia-Peru FTA, the 2019 Brazil-Chile FTA, the 2019 Australia-Indonesia FTA, the 2018 USMCA, 2019 Japan-US DTA, and the 2020 DEPA between Chile, New Zealand and Singapore.
15. Article 14.5 CPTPP.
16. Articles 14.9 and 14.6 CPTPP.
17. Article 14.17 CPTPP.
18. Article 14.14 CPTPP.
19. Article 14.10 CPTPP.
20. Article 14.16 CPTPP.
21. Article 14.8 CPTPP.
22. See Burri, as well as Chander & Schwartz, both supra note 8.
23. Article 14.13(2) prohibits the parties from requiring a " covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory ".
24. Article 14.17 CPTPP.
25. Article 14.11(2) CPTPP.
26. Article 14.11(3) CPTPP.
27. While this language appears familiar to trade lawyers in reference to the general exception clauses of Article XIV GATS and Article XX GATT 1994, the CPTPP does not, in contrast to the WTO provisions, provide an exhaustive list of public policy objectives and simply speaks of a " legitimate public policy objective ". In addition, there is no GATT or GATS-like qualification of " between countries where like conditions prevail ".
28. New Zealand's Waitangi Tribunal, Report on the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (2021), in particular at 132-142.

tal trade, [29] as well as with respect to ensuring unhindered data flows. [30] Beyond these similarities, the USMCA goes " CPTPP-plus " in some respects : first, by including " algorithms " in the ban on requirements for the transfer or access to source code ; [31] second, by limiting the liability of " interactive computer services " providers for third party content, [32] which secures the application of Section 230 of the US Communications Decency Act – a safe harbour that endorses the First Amendment for platforms but has been in recent times under attack in the face of fake news and other negative developments related to platforms " power. [33] The third and rather liberal commitment of the USMCA parties is with regard to open government data [34] and seeks to facilitate public access to and use of government information provided " in a machine-readable and open format and can be searched, retrieved, used, reused, and redistributed ". [35]

The US approach towards digital trade issues has been confirmed also by the 2019 US-Japan Digital Trade Agreement (DTA), signed alongside the US-Japan Trade Agreement. The treaty replicates almost all provisions of the USMCA and the CPTPP, [36] including the new USMCA rules on open government data, [37] source code [38] and interactive computer services [39] but notably covering also financial and insurance services as part of its scope. It also adds a new provision regarding information and communications technology (ICT) goods that use cryptography, again in an effort to curb forced technology transfer. [40]

Truly innovative in the landscape of digital trade rulemaking and going substantially " CPTPP-plus " has been the new generation of DEAs. So far five such agreements have been agreed upon : the aforementioned 2019 Japan-US DTA ; the 2020 Singapore-Australia DEA ; the 2020 Digital Economy Partnership Agreement (DEPA) between Chile, New Zealand and Singapore ; [41] the 2021 Korea-Singapore DEA and the 2022 UK-Singapore DEA. [42] Despite some variations, the DEAs can be said to share a common template. On the one hand and taking here the example of the DEPA, the DEAs tend to include all rules of the CPTPP and some of the USMCA, such as the one on open government data [43] (but not source code) ; some of the US-Japan DTA provisions, such as the one on ICT goods using cryptography, [44] have been included too. On the other hand, there are many other rules previously unknown to trade agreements that try to facilitate the functioning of the digital economy and enhance cooperation on key issues. [45] So, for instance, DEPA's Module 2 on business and trade facilitation includes, next to the standard CPTPP-like norms, [46] additional efforts " to establish or maintain a seamless, trusted, high-availability and secure interconnection of each Party's single window to facilitate the exchange of data relating to trade administration documents ". [47] Parties have also touched upon other important issues around digital trade facilitation, such as electronic invoicing ; express shipments and clearance times ; logistics and electronic payments. [48] Module 8 of the DEPA on emerging trends and technologies is also interesting to mention, as it highlights a range of key topics that demand attention by policymakers, such as in the areas of fintech and AI, and discusses the adoption of ethical and governance frameworks that support the trusted, safe, and responsible use of AI technologies. [49] Again going beyond economic issues, the DEPA also deals with the importance of a rich and accessible public domain [50] and digital inclusion. [51] Above all, DEAs provide a flexible platform for cooperation on a number of issues pertinent to the data-driven economy, including also matters that are not necessarily " treaty-ready ".

While the above enquiries do point to substantial CPTPP-plus developments, this is not true for all stakeholders involved. The EU, for instance, and despite its proactive and comprehensive domestic rulemaking in the digital domain, has been a relatively late mover on digital trade issues. [52] Now that it has defined its template, [53] this differs in important aspects from the provisions described above. On the one hand, the EU digital trade chapters converge with the CPTPP/USMCA model to cover issues such as software source code, [54] facilitation of electronic commerce, [55] online consumer protection, [56] spam [57] and open government data. [58] On the other hand, they do not include provisions on non-discrimination of digital products and, in reflection of the EU stance on trade and culture, consistently exclude audiovisual services from the scope of the application of the digital trade chapter. [59] Beyond this and critically for the regulation of the data-driven economy, the EU is willing to permit data flows only if coupled with the high data protection standards of its General Data Protection Regulation (GDPR). So while the EU and its partners subscribe to a ban on data localization measures, these commitments are conditioned : first, by a dedicated article on data protection, which clearly states that : " Each Party recognises that the protection of personal data and privacy is a *fundamental right* and that high standards in this regard contribute to trust in the digital economy and to the development of trade ", [60] followed by a paragraph on data

29. The USMCA follows the same broad scope of application (Article 19.2), bans customs duties on electronic transmissions /Article 19.3) and binds the parties for non-discriminatory treatment of digital products (Article 19.4). Furthermore, it provides for a domestic regulatory framework that facilitates online trade by enabling electronic contracts (Article 19.5), electronic authentication and signatures (Article 19.6) and paperless trading (Article 19.9).
30. Articles 19.11 and 19.12 USMCA.
31. Article 19.16 USMCA. On the expansion of the scope of the source code provision, see New Zealand's Waitangi Tribunal, supra note 28, at 104-112.
32. Article 19.17(2) USMCA.
33. See e.g., M. Burri, " Fake News in Times of Pandemic and Beyond : An Enquiry into the Rationales for Regulating Information Platforms ", in K. Mathis and A. Tor (eds), *Law and Economics of the Coronavirus Crisis* (Springer, 2022), 31-58.
34. Article 19.18 USMCA.
35. Article 19.18(2) USMCA.
36. Article 7 : Customs Duties ; Article 8 : Non-Discriminatory Treatment of Digital Products ; Article 9 : Domestic Electronic Transactions Framework ; Article 10 : Electronic Authentication and Electronic Signatures ; Article 14 : Online Consumer Protection ; Article 11 : Cross-Border Transfer of Information ; Article 12 : Location of Computing Facilities ; Article 16 : Unsolicited Commercial Electronic Messages ; Article 19 : Cybersecurity US-Japan DTA.
37. Article 20 US-Japan DTA.
38. Article 17 US-Japan DTA.
39. Article 18 US-Japan DTA.
40. Article 21 US-Japan DTA. This rule is similar to Annex 8-B, Section A.3 of the CPTPP Chapter on technical barriers to trade.
41. With Canada, South Korea and China seeking to join.
42. It should be noted that the DEAs are in most cases linked to an existing or in parallel adopted trade agreement ; in contrast, DEPA is a stand-alone agreement.
43. Article 9.4 DEPA.
44. Article 3.4 DEPA.
45. For a comparison of the DEPA with existing PTAs, see M. Soprana, " The Digital Economy Partnership Agreement (DEPA) : Assessing the Significance of the New Trade Agreement on the Block ", *Trade, Law and Development* 13 (2021), 143-169.
46. See e.g., Article 2.2 : Paperless Trading ; Article 2.3 : Domestic Electronic Transactions Framework.
47. Article 2.2(5) DEPA.
48. Respectively Articles 2.5, 2.6, 2.4 and 2.7 DEPA.
49. Article 8.2(2) and (3) DEPA.
50. Article 9.2 DEPA.
51. Article 11.2 DEPA.
52. For overview of this development, see e.g., Burri (2022), supra note 11.
53. Representative of the new EU approach are the adopted agreements with the United Kingdom (Trade and Cooperation Agreement, TCA) and with New Zealand, as well as the draft digital trade chapters of the negotiated deals with Australia and Tunisia.
54. See e.g., Article 207 EU-UK TCA. The commitment comes with a number of exceptions.
55. See e.g., Articles 205 and 206 EU-UK TCA.
56. See e.g., Article 208 EU-UK TCA.
57. See e.g., Article 209 EU-UK TCA.
58. See e.g., Article 210 EU-UK TCA. The FTA with New Zealand curiously has no provision on open government data.
59. See e.g., Article 197(2) TCA.
60. See e.g., Article 6(1) draft EU-Australia FTA (emphasis added). The same wording is found in the EU-New Zealand FTA. The EU-UK TCA does not however refer to privacy as fundamental right ; this can be however presumed, since

sovereignty. [61] A number of other safeguards are included too – such as a review possibility that can be linked to new restrictions, [62] as well as a broad carve-out under the " right to regulate ", which essentially gives the EU leeway to restrict data flows " to achieve legitimate policy objectives, such as the protection of public health, social services, public education, safety, the environment including climate change, public morals, social or consumer protection, privacy and data protection, or the promotion and protection of cultural diversity ". [63]

C. - The Asian Regionalism Model of Digital Trade Rulemaking

5 - Despite the fact that selected Asian countries are also members of western-led initiatives, such as the CPTPP and more recently, the Indo-Pacific Economic Framework (IPEF), and that Singapore has become the most prominent legal entrepreneur in digital trade governance with the DEAs, the Asian regionalism model of digital trade rulemaking comes with some specificities. In particular, if one looks carefully at the Regional Comprehensive Economic Partnership (RCEP) and the ASEAN E-Commerce Agreement, one sees a more flexible and pragmatic framework that allows developments at different speeds that well reflect varieties and sensibilities across the different countries. [64] For instance, while the RCEP includes many of the issues around the facilitation of digital trade, its language is more cautious on data governance issues. The RCEP electronic commerce chapter includes a ban on localization measures, [65] as well as a commitment to free data flows, [66] but there are clarifications that protect the RCEP parties " policy space. For instance, the necessity of the implementation of a legitimate public policy measure is to be decided by the implementing party. [67] In addition, a party can take " any measure that it considers necessary for the protection of its essential security interests. Such measures shall not be disputed by other Parties ". [68] In this sense, the RCEP parties " policy space remains well protected. It has been argued that this pragmatic and incremental approach should not be viewed as inferior but rather as one that addresses well the existing variations in digital development levels across countries, " eventually leading to meaningful consensus-building and long-term engagement in complex areas of digital regulation ". [69]

Keeping in mind these advanced FTA rule-frameworks, as well as their specificities, the following section asks whether we can go (back) to the multilateral forum of the WTO.

3. Can Digital Trade Law be Multilateralized ?

6 - In the midst of the stalemate at the WTO, the Joint Initiative (JI) on Electronic Commerce [70] has been a much-welcomed revigoration of the WTO negotiation arm in general and in particular of its effort to address contemporary digital trade. [71] The JI negotiations can be directly linked to the advanced rulemaking on digital trade in FTAs. This comes with both advantages and a number of setbacks. In the former sense, it appears that FTAs as well as the DEAs have worked as regulatory laboratories – not only in terms of mapping the relevant issues but also in terms of treaty language. Yet, the stakeholder positioning, as reflected in the discussed treaties, has also been translated in the JI negotiations. This has been helpful with regard to agreeing on multiple digital trade facilitation issues and progress has been made in particular on online consumer protection ; electronic signatures and authentication ; e-invoicing ; single windows ; spam ; open government data ; electronic contracts ; transparency ; internet access ; cybersecurity cooperation ; and paperless trading. Still discussed (as doable) are e-payments ; technical assistance and capacity building. Somewhat uncertain are : levels of market access commitments ; customs duty moratorium ; source code ; ICT products using cryptography ; scope and general provisions. And of course, the provisions on cross-border data flows and the related exception, including the privacy-related provisions, remain highly contested. Whether commitments on data flows materialize appears in the current geopolitical context unlikely, as there has been a shift in the negotiation position of one of the most proactive data flows supporters, the US, as it recently announced not to further pursue provisions on data flows, data localization and source code, so as to safeguard " policy space " for a digital trade rethink. [72]

The next months will show whether the JI on e-commerce can be brought to successful end and whether its results can be incorporated into the WTO architecture. [73] At least equally important will be the next WTO Ministerial Conference (26-29 February 2024), which will decide the fate of the WTO moratorium on customs duties on electronic transmission and thus also test the willingness of the entire WTO membership for cooperation on digital trade issues.

Concluding Remarks

7 - This article's enquiry reveals the critical importance of digital trade as a negotiation topic in both preferential and multilateral forums and the substantial efforts made, in particular in recent years, to create an adequate rule-framework. The achievements made in some FTAs and the DEAs are remarkable and there is a strand of legal innovation that seeks to tackle not only the " old " issues raised under the WTO Electronic Commerce Programme but also the newer issues in the context of a global data-driven economy. Yet, although all major stakeholders have become active in digital trade rulemaking, there are different approaches across

the UK incorporates the European Convention on Human Rights (ECHR) through the Human Rights Act of 1998 into its domestic law.

61. See e.g., Article 6(2) draft EU-Australia FTA. The same wording is found in the EU-New Zealand FTA and the EU-UK TCA.
62. See e.g., Article 5(2) draft EU-Australia FTA. The same wording is found in the EU-New Zealand FTA and the EU-UK TCA.
63. See e.g., Article 2 draft EU--Australia FTA. The same wording is found in the EU-New Zealand and the EU-UK TCA ; also S. Yakovleva, " Privacy Protection(ism) : The Latest Wave of Trade Constraints on Regulatory Autonomy ", *University of Miami Law Review* 74 (2020), 416-519, at 496.
64. See N. Mishra & A. M. Palacio Valencia, " Digital Services and Digital Trade in the Asia Pacific : An Alternative Model for Digital Integration ? ", *Asia Pacific Law Review* 31 (2023), 489-513.
65. Article 12.14 RCEP.
66. Article 12.15 RCEP.
67. Article 12.14.3(a) RCEP.
68. Article 12.14.3(b) RCEP.
69. Mishra & Palacio Valencia, supra note 64.
70. WTO, Joint Statement on Electronic Commerce, WT/MIN(17)/60 (13 December 2017) ; WTO, Joint Statement on Electronic Commerce, WT/L/1056 (25 January 2019) ; WTO, WTO Electronic Commerce Negotiations, Consolidated Negotiating Text, INF/ECOM/62/Rev.1 (14 December 2020) (the more recent consolidated negotiating text circulated in November 2023 is not public). The JI negotiations are co-convened by Australia, Japan and Singapore. Currently, 90 WTO Members representing over 90% of global trade, all major geographical regions and levels of development are participating in these negotiations.
71. On the development of the JI negotiations, see e.g., M. Burri, " A WTO Agreement on Electronic Commerce : An Enquiry into its Substance and Viability ", *Georgetown Journal of International Law* 53 (2023), 565-625 ; Y. Ismail, " The Evolving Context and Dynamics of the WTO Joint Initiative on E-commerce : The Fifth-Year Stocktake and Prospects for 2023 ", *International Institute for Sustainable Development and CUTS International* (Geneva, 2023).
72. See Inside US Trade, " US to End Support for WTO E-commerce Proposals, Wants 'Policy Space' for Digital Trade Rethink ", 24 October 2023.
73. For an overview of the debates, see e.g., Burri, supra note 71 ; also F. Angeles, R. Roy & Y. Yarina, *Shifting from Consensus Decision-Making to Joint Statement Initiatives* (Graduate Institute Geneva, 2020) ; B. Hoekman & C. Sabel, " Plurilateral Cooperation as an Alternative to Trade Agreements : Innovating One Domain at a Time ", *Global Policy* 12 (2021), 49-60 ; A.B. Zampetti, P. Low & P.C. Mavroidis, " Consensus Decision-Making and Legislative Inertia at the WTO : Can International Law Help ", *Journal of World Trade* 56 (2022), 1-26.

stakeholders. The issues around cross-border data flows remain highly contentious, as they impact states ″ policy space and the ability to adopt a variety of measures, particularly in the areas of national security and privacy protection. In this context, the venues of FTAs and in particular the more flexible model of the DEAs provide a good platform for experimentation and evidence-gathering on the economic but also, and perhaps importantly, on the broader societal effects of such commitments. Whereas enhanced regulatory cooperation in striving to attain a seamless global data-driven economy is needed, there must be safeguards for the protection of non-economic interests and values, as well as consideration of the varying levels of development and regulatory capacities across countries. Until we reach a state of digital trade law that properly interfaces international and national regimes and can operate in a fluid technological environment, more " learning " time is needed.■

9 Ensuring a Fair Remuneration to Authors and Performers in Music Streaming

Séverine DUSOLLIER,

Professor at Sciences Po Law School and Senior Chair of the Institut Universitaire de France

Introduction – The revolution of Music streaming

1 - Music is constantly flowing from our smartphones, in public transportation, at homes, when walking or running. For a monthly fee of less than the price of one album, or even for free, anyone, at least in richer economies, can listen to K-pop, New Orleans blues, French variété, drum and bass, gangsta rap, Arabic rock, Indian classical music from Taylor Swift to Prokofiev, from Ali Farka Touré to PJ Harvey. The technology of streaming [1] has materialised the celestial jukebox Paul Goldstein predicted in the very early advent of the web. [2] Its rapidity, volume and simultaneity of transmission of digital content have irrevocably revolutionised the cultural economy and consumption practices. [3]

After several years of peer-to-peer file-sharing and websites providing music and films without any authorisation, copyright-compliant [4] music streaming services, such as Spotify, Deezer, Apple, Tidal or SoundCloud, have brought back revenues and a recovered health to the music industry. Copyright royalties from streaming in the musical field have drastically increased in the last years and now surpass the revenues from physical sales. In 2022, streaming yielded 67% of the global music revenues and an astounding amount of 17,5 billion dollars, still on the rise. [5]

However, while both the volume of consumption of music in streaming mode and the revenues of the music industry keep on increasing, the remuneration of creators and musicians do not follow. Despite the massive transfer of consumption of culture and entertainment towards Netflix, Spotify and the like during the covid-19 pandemic, artists and creators are still struggling to earn a living, which is troublesome.

This short article will consist of two parts : the first one will address the distribution of revenues amongst the many holders of rights in music and explain its unfairness to authors and performers (I) ; a second part will explore the different legal initiatives that sought to address the issue and provide new modes of remuneration to artists (II).

1. THE DISTRIBUTION OF STREAMING REVENUES TO AUTHORS AND PERFORMERS

2 - Rights holders in recorded music are diverse and many : author(s) of the musical composition and of the lyrics own copyright in the musical work, that they usually transfer to a music publisher, while performers (musicians and singers) and the phonogram producer – who have turned the creation into a sound recording – own related rights (also called neighbouring rights) in the recording, referred to as phonogram in copyright law. [6]

The distribution of the revenues pie is approximately the following : the music streaming platforms transfer 70% of their revenues to rights holders. [7] Yet, the breakdown of the royalties is largely unequal : out of the 70% paid by the streaming platforms, approximately 55-58% go to the sound recording owners, i.e. the phonogram producers, 5% to publishers and 10% to songwriters, and 15% (taken from the amount going to producers) go to the performers (to be divided between all performers who have intervened in a recording, including studio musicians), depending on the contract they have with producers. [8] The share of authors (of the musical composition and of the lyrics) in the 10% perceived from the platforms also vary according to their contract with their publisher.

It is difficult to approximate the average remuneration allocated to authors and performers as the mode of calculation of royalties differs from one platform to another, and the royalties paid to creators and performers at the end of the chain depend upon their respective contracts with their publisher and producer, older contracts tending to be less generous to creators and musicians,

1. The technology of streaming can be defined as a mode of transmission of digital audio and/or video data on online networks that allows for simultaneous and synchronized reception and playback.
2. P. Goldstein, *Copyright's Highway. From Gutenberg to the Celestial Jukebox*, New York, 1994.
3. R. Leung, M. Kretschmer, B. Meletti, *Streaming Culture*, CREATe research report, April 2020, https ://www.create.ac.uk/blog/2020/06/02/new-working-paper-streaming-culture-2/.
4. Streaming musical or audiovisual works constitutes an act or making available to the public and also implies an act of reproduction of such works, hence requiring a license from copyright holders (i.e. composers and lyricists and music publishers) and from related rights owners (i.e. phonogram producers and performers).
5. see IFPI Global Music Report, 2023, https ://globalmusicreport.ifpi.org/. In the US, streaming surpassed both physical sales and digital downloads of music for the first time in 2015. For comparison, in 2012, streaming revenues were only one billion dollars out of a global revenue of 14 billion.
6. On the chain of rights in the music industry, see Susan Butler, *Inside the Global Digital Music Market*, World Intellectual Property Organization, 2021, https ://www.wipo.int/edocs/mdocs/copyright/en/sccr_41/sccr_41_2.pdf.
7. For Spotify, the leader of the market with 172 million premium subscribers and 381 million active users in 2021, it amounted to 7 billion dollars in 2021.For some information the allocation of revenues, see GESAC Report, *Study on the place and role of authors and composers in the European music streaming market*, September 2022, p.27.
8. It should be kept in mind that many performers, such as the background or session musicians who are hired to perform for a specific recording, are paid a lump sum for their work during the recording session and do not get more remuneration from producers on the further exploitation of the record. For a good explanation of the practices of remuneration and diverse model of contracts applying to music performer, see CMU Insights, *Performers Payments from Streaming*, available at https ://cmuinsights.com/performerpaymentsfromstreaming/.

except for music stars who have been enjoying a stronger negotiation leverage. [9]

According to a study of Aepo-Artis, the European association of performers, only 1% of European music performers earn more than the minimum wage from streaming revenues and 90% earn less than one thousand euros per year, even if their sound recordings are listened to one hundred thousand times. [10] A UK parliamentary report mentions that 8 out of 10 songwriters earn less than two hundred pounds a year from streaming. [11]

It is estimated that each stream generates a royalty of 0.0034$ (all rightholders together) on Spotify, of 0.0056$ on Deezer, and of 0.0067$ on Apple Music. Spotify pays between 0.003 and 0.005$ for each stream, which means that a song needs to reach three hundred thousand plays on the streaming platform for an artist to get roughly one thousand dollars in streaming royalties.

This low level of revenues of authors and performers is aggravated by a significant disproportion amongst artists. 1% of the artists whose music is available on streaming platforms captures 90% of the streams, and 10% concentrate 99,4% of the music listened to. [12] It is well known that the music industry is a winner-take-all market, where the superstar artists and " hit " songs seize a disproportionate share of the revenues leaving very little to the remaining players. Spotify has for instance reported that one thousand artists have won more than one million dollars from their streams and 130 artists more than five million, [13] a positive outcome for the major streaming operator, but that leaves invisible the mass of other artists who earn far less. Very recently, the leading music streaming platform has announced that a minimum one thousand streams within the preceding 12 months would be required to be eligible to copyright royalties. That restriction, arguably justified by the disproportionate transaction costs occurred by such micro payments, is said to account to only 0,5% of royalties distributed by Spotify. This seemingly negligible amount – that still represents forty million dollars per year – will be redistributed to major rightholders to the detriment of less streamed indie artists.

This disproportion of revenues between the average artist and the superstar has always existed in the music industry but might be intensified by other factors of the streaming model. Some models of calculation of remuneration adopted by the platforms are more inclined to concentrate the revenues yielded by the streaming service on the heads of a few artists, [14] and the recommendation systems and playlists put in place by platforms, particularly when algorithmically based, decisively impact what titles are included in playlists and prioritised in the recommendations made to platform users, ultimately deciding what music is listened to. [15]

Collectives of artists have started to protest against their low levels of remuneration through campaigns and petitions such as Justice at Spotify in the US, #BrokenRecord or #FixStreaming in the UK. [16]

Individual renowned artists have tried to put the issue in the spotlight as well, with some success and governments, particularly in countries with a wealthy music industry, such as the US, UK and France, have launched studies and initiatives to tackle the issue and provide for a better remuneration of artists. [17]

2. LEGAL SOLUTIONS FOR A BETTER REMUNERATION

3 - In order to increase the streaming remuneration of artists, two avenues have been mostly explored : the fixation of minimal tariffs and remuneration or the provision of an unwaivable right of remuneration that authors and performers directly collect from streaming operators.

In the US, the Music Modernization Act enacted in 2021 created the Mechanical Licensing Collective (MLC) that can grant license in musical works, based on tariffs overseen by a Copyright Royalty Board and negotiated with the streaming platforms. Such fixed percentage of remuneration has led to an increase of copyright royalties of 44% for songwriters. [18] After many years of negotiations, an agreement has been reached in France in 2022 to ensure a minimal remuneration of main performers of 10% of revenues (that can even go up to 28% in some cases) perceived by their producers from streaming exploitation. In addition, session performers, who have been paid a one-off fee for the recording time, are entitled to a further amount per sound recording, depending on the volume of streams. More recently the French government decided to impose a tax on revenues of music platforms to fund the National Council of Music, that aims at supporting emerging artists.

Beyond such statutory rates or percentages of remuneration, an equitable and unwaivable right of remuneration has been claimed by authors " and performers " representatives. [19] Such a right would consist in collecting the remuneration for streaming directly from the platform and irrespectively of the transfer of copyright or performers' right to the music publishers or producers. The latter would still negotiate with streaming platforms the required licence to stream the music and receive revenues for such exploitation, but the authors and performers would get their revenues from a collective management organisation that would negotiate and administer the conditions of the right. The added value of such an unwaivable right of remuneration is precisely its independence from the individual contracts agreed upon between authors and performers and their economic counterparts, where they are generally in a weaker negotiating position, as well as its collective mandate and representation. However, the distribution of revenues would still be determined by the number of streams of each artist.

Belgium and Croatia have set up such a right of remuneration for authors and/or performers. [20] The UK official inquiry into the Economics of streaming also recommended to adopt legislation on equitable remuneration, though the Government decided to carry out more research before legislating in that direction. In the Fall 2023, Uruguay has announced the enactment of a right to remuneration for streaming which led Spotify to announce its with-

9. GESAC Report, *Study on the place and role of authors and composers in the European music streaming market*, September 2022, p.25.
10. AEPO-ARTIS, *Performers' rights in International and European Legislation – Situation and Elements for Improvement*, 2018, https ://www.aepo-artis.org/wp-content/uploads/2022/07/AEPO-ARTIS-Study-2018-Performers-Rights-in-International-and-European-_20181161711.pdf
11. DCMS Committee, *Economics of music streaming : Second Report of Session 2021-22*, https ://committees.parliament.uk/work/646/economics-of-music-streaming/.
12. Those numbers dates back from a 2020 survey, but might largely be the same today. See https ://themusicnetwork.com/few-artists-generate-most-streams/.
13. Spotify Loud and Clear Transparency Report, available at https ://loudandclear-.byspotify.com/.
14. Different models apply, such as the Market Centric Payment System (Spotify), the User-Centric Payment Model SoundCloud and Deezer) or the Artist-Centric Model (Deezer), see S. Butler, *op. cit.*, note 34, p. 24-25 ; Survey of the French Conseil National de la Musique, available at https ://cnm.fr/en/studies/impact-of-online-music-streaming-services-adopting-the-ucps/
15. GESAC Report, *op. cit.*, p.23-24 ; DCMS Committee, Economics of music streaming : Second Report of Session 2021-22, *op. cit.*
16. See also, GESAC Report, *Study on the place and role of authors and composers in the European music streaming market*, September 2022.
17. See mostly in the UK, DCMS Committee, *Economics of music streaming : Second Report of Session 2021-22*, https ://committees.parliament.uk/work/646/economics-of-music-streaming/ ; Competition and Markets Authority, *Music streaming – Final Report*, 29 November 2022, https ://www.gov.uk/cma-cases/music-and-streaming-market-study#final-report.
18. The system does not cover performers.
19. Pleading for the introduction of such a right for audiovisual authors, see R. Xalabarder, The equitable remuneration of audiovisual authors : a proposal of unwaivable remuneration rights under collective management, *R.I.D.A.*, 2018, n° 256 ; SAA, *White Paper – Audiovisual Authors' Rights and Remuneration in Europe*, 2015, https ://www.saa-authors.eu/en/publications/55-saa-white-paper-2nd-edition.
20. Article XI.228/11 of the Belgian Code of Economic Law ; Art. 149 Croatian Copyright Act. Spain already has such a right of unwaivable remuneration that might be extended to streaming exploitation.

drawal from the Uruguayan market and spurred the Government to reach and deal and retract from its initial plan.

Streaming platforms have challenged the Belgian legal provision before the Constitutional Court [21] based on discrete grounds and the case is closely followed in Europe as it could result in a referral before the CJEU.

The opponents to this unwaivable remuneration right first argue that it stands in contradiction with the article 18 of the CDSM directive of 2019 that imposes a fair and proportionate remuneration of authors and performers when authors and performers contractually transfer or license their rights, [22] which would exclude any extra-contractual solution to provide for some remuneration. However, the directive itself allows Member States to implement the principle of appropriate and proportionate remuneration through different existing or newly introduced mechanisms. [23] The text of article 18 states that " *Member States* shall ensure " a principle of adequate remuneration, which can be construed as meaning that such remuneration does not necessarily only come from the transferees or licensees.

Another argument relates to the principle of exclusivity that should be vested in copyright and related rights, as reasserted by the CJEU. [24] Yet, statutory rights of remuneration are not foreign to EU copyright framework. They particularly benefit performers for some secondary uses of their fixations and mitigate their weaker bargaining position in contractual dealings or the low remuneration they might effectively get against a transfer of their exclusive rights. [25]

Moreover, the unwaivable remuneration right applied to streaming exploitations, in comparison to the remuneration right granted to related rights holders for broadcasting, does not substitute to an exclusive right but only " secures a remuneration retained upon the transfer of the exclusive right ". [26] It does not deprive in any way the authors and performers of their exclusive right, but guarantees rather an effective remuneration against the licensing of their right. R. Xalabarder qualifies it as a residual remuneration right, that is separated from the transferred or licensed exclusive right. Combining the exclusivity of exploitation with a right to a fair remuneration is for that reason not contrary to the principle of an absolute and undivided property, another argument held by streaming platforms against the proposed regime. They argue indeed that when the right has been transferred by contract to music publishers and producers, authors and performers do not enjoy such rights and the platforms need only to remunerate the publishers and producers who are the sole legitimate owners of copyright. Otherwise, so they say, they would pay twice for the same right.

Envisaging copyright as a property right does not necessarily transform its several economic rights into a monolithic whole. Copyright, as property, can be conceived as a bundle of rights that assembles several entitlements applying to separate economic activities, either in the form of exclusive rights that can be transferred or assigned to others and enable them to carry out exploitation of the works, or in the form of rights to remuneration that the authors could exercise to be associated in a more permanent and on-going manner to the overall exploitation of works and the financial flows they generate. [27] Under the regime of an unwaivable remuneration right, creators and musicians would only assign by contract their exclusive right of control to publishers or producers, amputated from a right to perceive a remuneration granted by law. [28] A similar division of different exploitation or remuneration rights is regularly applied in copyright contracts or in collective management mandates. [29]

Conclusion

4 - Streaming music platforms have radically changed our modes of consumption of music and generate today billions of dollars of revenues for the music industry. Yet, earnings of most creators, musicians and artists remain disproportionately low despite the successful commercial uptake of streaming.

Now that the market of streaming is thriving in most economies of the world, and appears to steadily expand in poorer countries, this is a challenge that lawmakers know that they need to embrace. Internationally known and already tested legal mechanisms such as the right of equitable remuneration, currently considered or implemented in some Western economies, could be of some help in restoring fairness in the streaming industry.

It will not be easy. Streaming platforms will not hesitate to show off some corporate muscle. Spotify, the dominant player of the market, has decided in an interval of a few months to demonetise the less streamed music, to withdraw from the Uruguayan market if an unwaivable remuneration right is enacted and to stop funding French music festivals in retribution for the 1,2 % tax imposed on its revenues. The dominant position of the Swedish platform could call for an intervention of competition law. However a recent survey of the Competition authority in the UK has declined to see the meagre revenues of authors and performers as an issue, as far as consumers would benefit from a huge diversity of content at a very low price. [30] Maybe it is time to acknowledge that consumer welfare cannot be the only compass to regulate an unfair market and that a fair remuneration of the creators and artists equally justifies legislative interventions. Isn't it time also to ask the question of the fair price users should pay to access the ongoing and voluminous flow of music delivered by streaming platforms ?■

21. The Belgian law also provides for an unwaivable right to remuneration against online content-sharing services providers, which is not discussed here.
22. For an analysis of this legal provision see, S. Dusollier, " The 2019 Directive on Copyright in the Digital Single Market : Some progress, a few bad choices, and an overall failed ambition ", [2020] 57 *Common Market Law Review*, 979-1030. On the compatibility of a solution of an equitable right of remuneration with the art. 18 of the directive, see the Opinion of the European Copyright Society Comment of the European Copyright Society, *Addressing Selected Aspects of the Implementation of Articles 18 to 22 of the Directive (EU) 2019/790 on Copyright in the Digital Single Market*, https ://europeancopyrightsocietydotorg.files.wordpress.com/2020/06/ecs_comment_art_18-22_contracts_20200611.pdf.
23. See recital 73 of the directive 2019/790.
24. CJEU, 16 November 2016, *Soulier & Doke*, C-301/15, ECLI :EU :C :2016 :878 ; CJEU, 14 November 2019, *Spedidam c. INA*, C-484/18, ECLI :EU :C :2019 :970.
25. See B. Hugenholtz, " Is Spotify the New Radio ? The Scope of the Right to Remuneration for 'Secondary Uses' in respect of Audio Streaming Services ", in *Festschrift für Thomas Dreier*, *forthcoming* (who pleads for the extension of the right of remuneration for performers in broadcasting to streaming when it is mostly based on playlists).
26. Xalabarder, *op. cit.*, p.58.
27. For more on this argument, see S. Dusollier, " Intellectual property and the bundle-of-rights metaphor ", *Kritika – Essays in Intellectual Property*, Vol.3, 2020, p.146-179.
28. Xalabarder, *op. cit.*, p.31.
29. The possibility of fragmenting rights entrusted with a CMO is provided for by the Directive 2014/26 on collective management, article 5.7 and even postulated by the CJEU : CJCE, 21 March 1974, SABAM, C-127/73, ECLI :EU :C :1974 :25.
30. Competition and Markets Authority, *Music streaming – Final Report*, *op. cit.*

10 Regulating for Asymmetric Market Power : Beyond the Consumer Sovereignty Model

Olivier SYLVAIN [1],

Professor of Law at Fordham University School of Law, New York

1 - Consumer data protection law and policy in the European Union (EU) and the United States (US) have much in common, even as different as their respective legal regimes appear to be. Both, in the end, arise from an abiding commitment to a consumer sovereignty model of commercial surveillance regulation. The EU's General Data Protection Regulation (GDPR), for example, aims in large measure to protect " data subject's rights and freedoms and legitimate interests ". [2] In the US, the prevailing legal conventions presume that companies are best able to provide products and services that satisfy each consumer's respective interests. The first is a rights-based approach. The second is a " laissez-faire " approach. Under both, however, regulators assume that, whether exercised as a positive right or a consensual commercial transaction, individual data subjects or consumers are best situated to manage how companies process or use their personal information.

Recent policy developments suggest, however, that consumer sovereignty models of regulation have substantial, if not fatal, limitations. Binding decisions by the European Data Protection Board in 2023, [3] as well as other recent public law enactments in the EU and the US, overtly reject the assumption that individuals are best situated to manage how companies process or use their personal information. Prevalent online practices are too opaque and the conditional or " take it or leave it " services that companies provide render individuals' rights and commercial choices effectively meaningless. In short, the relative power of consumers as compared to the companies that collect, process, and monetize personal information belies the normative conceit that consumers are in fact sovereign.

Existing restrictions on collection and use, including rules concerning data minimization, purpose limitations, and transparency are the way forward. In this regard, also consider the EU's new AI Act's flat prohibition on certain commercial practices like facial recognition and biometric identification as well as its imposition of heightened duties on companies that collect and process consumer data in high-risk sectors. [4] These developments, this essay argues, are evidence that policymakers in the EU and US are contemplating models of consumer data protection law and policy that are better suited to prevalent commercial surveillance practices today.

*

***

2 - The European Union's General Data Protection Regulation is arguably the single most influential public law concerning commercial surveillance practices. Chapter 3 in particular stands out to the extent that it establishes that each individual " data subject " has sovereign control over the ways in which " data controllers, " " processors, " and other companies use their " personal information ". [5] These include, among others, the right to : information about data collection practices, [6] access to the personal information that covered entities collect and share, [7] rectification of inaccurate personal information processed by those entities, [8] erasure of personal information, [9] data portability, [10] and objection of the processing of personal information. [11]

Consider, moreover, Article 22, which provides that consumers may opt out of automated decisions that are solely or mostly responsible for a legally significant outcome. This right is especially illustrative of the EU's commitment to the individual rights-based model given the opacity and complexity of the automated systems on which companies rely to deliver products and services. Article 22 also enumerates three exceptions to the opt-out right, all of which prioritize data subjects' individual rights. The first sounds in contract. It provides that companies' use of an automated system is lawful as long as it is " necessary for entering into, or the performance of, a contract between the data subject and a data controller ". [12] Here, the drafters overtly rest on the view that individuals are best positioned to make decisions about their commercial rela-

1. Fordham University School of Law, New York, New York. Professor Sylvain was Senior Advisor to the Chair of the Federal Trade Commission from 2021 to 2023. This essay reflects solely his views. He is grateful for productive conversations with Beatriz Botero Arcila, Rebecca Mignot-Mahdavi, Sibylle Pouillaude, and participants in the Sciences Po Law and Technology Workshop. All errors here are his own.
2. *See* Art. 14 (" Information to be provided where personal data have not been obtained from the data subject ") of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1, Art. 12- 23 [hereinafter GDPR].
3. *See* e.g. European Data Protection Board, *Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR)*, (adopted Oct.27, 2023 ; published Dec. 7, 2023).
4. European Parliament, *Artificial Intelligence Act : deal on comprehensive rules for trustworthy AI* (Dec. 9 2023), Press Release, https ://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai.
5. *See* Art. 12 (" Transparent information, communication and modalities for the exercise of the rights of the data subject. "). See also Art. 12- 13 of the GDPR.
6. *See* Art. 13 (" Information to be provided where personal data are collected from the data subject. ").
7. *See* Art. 15 (" Right of access by the data subject. ").
8. *See* Art. 16 (" Right to rectification. ").
9. *See* Art. 17 (" Right to erasure (" right to be forgotten ") "). See also Art 19 (" Notification obligation regarding rectification or erasure of personal data or restriction of processing. ").
10. *See* Art. 20 (" Right to data portability. ").
11. *See* Art. 21 (" Right to object "). To be clear, the EU did not invent these concepts. With perhaps the exception of the Chapter 3 rights to data portability and objection to data practices, they are just restatements of the 1973 Fair Information Practice Principles, which themselves the Council of Europe adopted in 1980. See Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, European Treaty Series 108 (CETS No. 108) [1981].
12. Art. 22(2)(a).

tionships, no matter how daunting the task of understanding online commercial practices is. The second exception defers to the applicable " Union or Member State law to which the controller is subject, " provided those protections " safeguard the data subject's rights and freedoms and legitimate interests ". [13] The third turns on the consent of the data subject, a legal mechanism whose roots in the classical liberal tradition are as deep as any other.

Other jurisdictions have promulgated laws and policies that overtly draw on the GDPR's consumer sovereignty model. [14]

*

***

3 - Since its passage, commentors have regarded the GDPR's rights-based model in contrast to the ostensibly " laissez-faire " approach to regulation in the United States. [15] It is important to note, however, that, in the US, privacy regulators have abided by the rights-based model in a variety of settings since the 1970s, if not earlier. [16] Pursuant to its organic statute's injunction against " unfair or deceptive acts or practice ", the Federal Trade Commission (FTC), for example, has brought enforcement actions against companies that fail to obtain consumer consent or " affirmative express consent " for data practices ". [17] Other sector-specific statutes and regulations that the FTC and other federal agencies enforce, moreover, enumerate, for example, consumer rights to verify and contest the accuracy of personal information, [18] as well as rights to information about data practices. [19] In the context of contemporary commercial surveillance practices, moreover, the US Congress in 2022 came very close to passing legislation that would have adopted much of the rights-based approach of the GDPR. [20] And the White House's Office of Science and Technology Policy in October 2022 published a " Blueprint for an AI Bill of Rights " that sets out many of these same rights. [21] That document, however, does not have the binding effect of law.

We could attribute the absence of binding comprehensive federal data protection law in the US to the longstanding skepticism of government regulation of information markets, particularly those concerning the internet. [22] Proponents of this " laissez-faire " approach contend that companies and other private actors are more capable than government regulators of realizing consumer demand. [23] Consider, after all, the ways in which, over the past two or so decades, companies have developed and marketed a wide range of privacy-enhancing technologies that have demonstrably won over consumers, including end-to-end encryption, the Global Privacy Control, [24] ephemeral messaging, and restrictions on third-party access to persistent identifiers. [25] These innovative commercial practices have directly empowered consumers to manage the collection, retention, and distribution of their personal information.

Courts, moreover, reflect this deep skepticism to government regulation of information flows in constitutional First Amendment doctrine. US courts have invalidated data protection laws on free speech grounds, even when those laws mean to protect consumers in their commercial transactions. [26] This " laissez-faire " approach has defined regulation of networked information in the US at least since the commercial deployment of the internet in the 1990s, [27] and arguably even before. [28]

*

***

4 - As different as the GDPR and US approaches to data protection appear to be, however, they both articulate an abiding commitment to the individual. The EU, for example, frames the GDPR as a law geared to actualizing " data subject's rights and freedoms and legitimate interests. " Pursuant to the prevailing US approach, companies in a mostly unregulated market are best positioned to abide by and meet each marginal consumer's demand. Ultimately, the individual is the direct beneficiary under both approaches.

Consumer sovereignty models, however, are not the only potential forms of government regulation of commercial data practices. Consider China's distinctly statist approach. Its aims are plainly to protect against domestic and foreign threats. In this vein, China has, at once, established impressive protections against abusive commercial data practices [29] but also made a nearly absolute exception for government surveillance. [30] Its trade policy is also unapologetically protectionist, privileging domestic development of technologies at the expense of foreign imports. [31]

But statism is also not the only alternative to consumer sovereignty models. Today, jurisdictions around the world, including the

13. Art. 22(2)(b).
14. See Brazil : " Law 13.709/2018 – Lei Geral de Proteção de Dados Pessoais " (General Law for the Protection of Personal Data, abbreviated by the Portuguese name), http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm ; California : California Consumer Privacy Act, 2018 Cal. Legis. Serv. Ch. 55 (A.B.375) (WEST).
15. Bradford, Anu, *Digital Empires : The Global Battle to Regulate Technology*. Oxford University Press. (1st ed. 2023).
16. US scholars and activists have advocated for EU-like rights-based regulation. See Aziz Z. Huq, A Right to a Human Decision, 106 Va. L. Rev. 611, 686 (2020) (arguing for a " right to a well-calibrated machine decision ") ; Kate Crawford & Jason Schultz, *Big Data & Due Process : Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. Rev. 93 (2014) ; Danielle Citron & Frank Pasquale, *The Scored Society : Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014) (calling for system reforms as well as due process rights protections).
17. *See* Complaint for Permanent Injunction and Other Equitable and Monetary Relief, *In re Vizio, Inc*., F.T.C. File No. 2 :17-cv-00758 (D.N.J. filed Feb 6, 2017), https ://www.ftc.gov/?system/?files/?documents/?cases/?170206_?vizio_?2017.02.06_?complaint.pdf ; Complaint, *In re Support King, LLC*, F.T.C. File No. 192-3003 (Dec. 20, 2021), https ://www.ftc.gov/?system/?files/?documents/?cases/?1923003c4756spyfonecomplaint_?0.pdf. These cases arise from an implicit consumer right to notice and consent. Cf. Advisory Committee on Automated Personal Data Systems, Transmittal Letter to Secretary of Health, Education, and Welfare on " Fair Information Practice Principles (1973), https ://aspe.hhs.gov/reports/records-computers-rights-citizens.
18. *See* Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x (enacted 1970) ; Equal Credit Opportunity Act, 15 U.S.C. 1691-1691f (enacted 1974) ; Children's Online Privacy Protection Act, 15 U.S.C. 6501-6506 (enacted 1998).
19. *See* Health Breach Notification Rule, 16 CFR part 318 ; Graham-Leach-Bliley Act (" Financial Services Modernization Act "), Public Law 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of titles 12 and 15 of the US Code).
20. *See* H.R.8152 – 117th Congress (2021-2022) : American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022), https ://www.congress.gov/bill/117th-congress/house-bill/8152.
21. White House, *Blueprint for an AI Bill of Rights : Making Automated Systems Work for the American People* (Oct. 4, 2022), https ://www.whitehouse.gov/ostp/ai-bill-of-rights/.
22. *See* John Perry Barlow, *A Declaration of the Independence of Cyberspace* (1996), https ://www.eff.org/cyberspace-independence. *See generally* Olivier Sylvain, *Platform Realism, Informational Inequality, and Section 230 Reform*, 131 Yale. L. J. Forum 475, 485-89 (2021) (outlining the incentives and positive theory for the prevailing laissez-faire approach).
23. *See* Avi Goldfarb & Catherine Tucker, *Privacy and Innovation*, in Innovation Policy and the Economy, Vol. 12, pp. 65-90 (2012), https ://doi.org/10.1086/663156.
24. *See* Russell Brandom, *Global Privacy Control wants to succeed where Do Not Track failed*, The Verge (Jan. 28, 2021), https ://www.theverge.com/2021/1/28/22252935/global-privacy-control-personal-data-tracking-ccpa-cpra-gdpr-duckduckgo.
25. *See* Sam Schechner, *Google Pursues Plan to Remove Third-Party Cookies*, Wall. St. J. (Jan. 25, 2021), https ://www.wsj.com/articles/google-progresses-plan-to-remove-third-party-cookies-11611581604.
26. *See*, e.g., Sorrell v IMS Health, 564 US 552 (2011) (holding that limits on sale, disclosure, and use of physician prescribing history by pharmaceutical companies violate the First Amendment) ; NetChoice v. Bonta, 2023 WL 6135551 (N.D. Cal., Sept. 18, 2023) (holding that limits on collection and use of children's personal information by operators of websites and services directed at children violate the First Amendment).
27. *See generally* Olivier Sylvain, *Platform Realism, Informational Inequality, and Section 230 Reform*, 131 Yale L.J. Forum 475 (2023).
28. *See* Ithiel de Sola Pool, Technologies of Freedom (1993).
29. *See* National Governance Committee for the New Generation Artificial Intelligence, *Governance Principles for the New Generation Artificial Intelligence--Developing Responsible Artificial Intelligence*, China Daily (June 17, 2019), https ://www.chinadaily.com.cn/a/201906/17/WS5d07486ba3103dbf14328ab7.html. See also Bradford, supra note 12 at 92.
30. Bradford, *supra* note 12 at 78.
31. Bradford, *supra* note 12 at 72.

E.U., Brazil, and California, have promulgated public law interventions that do not fit easily under consumer sovereignty models. Consider that, under Article 6 of the GDPR, companies may only rely on one of six lawful bases for processing personal information. Some of these rely on the consumer sovereignty model : to wit, covered entities may process personal information when either (1) they obtain the data subject's consent to process personal information for specific purposes [32] or (2) " processing is necessary for the performance of a contract to which the data subject is a party ". [33] And the last of the six asserts that companies may process personal information as long their " legitimate interests " do not conflict with the " fundamental rights and freedoms of the data subject ". [34]

Even as these " lawful bases " ostensibly abide by the consumer sovereignty model, recent binding decisions from the European Data Protection Board (EDPB) suggest that something more is necessary given that most consumers do not understand how companies use their data, even when companies elicit user consent. Data subjects in certain circumstances, the EDPB has announced, are sometimes in no position to negotiate the terms of their access to such services given the glaring asymmetry between them and the companies that process their personal information.

Consider the EDPB's decision, published in January 2023, that Article 6 does not allow Whats-App to process a user's personal information to implement " service improvements " and new security measures just because the user clicks " Accept " when the company unilaterally presents the Terms of Service. [35] Service improvements and security may be routine and even nominally mentioned in the company's Terms of Service, the EDPB acknowledged, but it is not obvious that processing is " objectively necessary for the performance of the contract with the user ". [36] Rather, the " exact rationale of the contract " must be clear and the processing must be " objectively necessary " for that purpose. [37] This is also to say that a company may not process information if " realistic, less intrusive alternatives " exist. [38] The Whats-App Terms of Service, however, required data subjects to agree to use the service " to communicate with others " on the condition that the company could process their personal information. [39] In this way, the company, the EDPB held, had relied on its users' " forced consent " in violation of Article 6(1)(b) when it processed all of its users' personal information to perform these functions. [40]

Article 6, the EDPB elaborated, requires data processors to make data subjects aware of " possible adverse consequences " that " processing may have on them, and having regard to the relationship and potential effects of imbalance between them and the controller ". [41] Importantly, however,

> an average user cannot fully grasp what is meant by processing for service improvement and security features, be aware of its consequences and impact on their rights to privacy and data protection, and reasonably expect it solely based on Whats-App IE's Terms of Service. [42]

Moreover, the company gives users a " take it or leave it choice, " which is no choice at all. [43]

> They may either contract away their right to freely determine the processing of their personal data and submit to its processing for service improvements or security features, which they can neither expect, nor fully understand based on the insufficient information Whats-App IE provides to them. Alternatively, they may decline accepting Whats-App IE's Terms of Service and thus be excluded from a service that enables them to communicate with millions of users. [44]

Finally, the EDPB also relied on the Article 5 principles of fairness, purpose limitation, and data minimization to reject Whats-App's claim to lawfully processing personal information. Those principles, it explained, protect against the kind of " power imbalance " in " the controller-data subject relationship " at work in that case. [45] This must be especially true " in the context of online services provided without monetary payment, where users are often not aware of the ways and extent to which their personal data is being processed ". [46] Here, the EDPB relied on the Article 6 to protect " data subjects " who generally cannot " determine what is done with their personal data, " irrespective of their ostensible agreement to the contract. [47] This conclusion is obviously " in contrast " to the idea that data subjects have the " autonomy " to " control " how companies process their personal information. [48] The purpose limitation principle in particular requires that Whats-App only process as much as is necessary to provide the service to which data subjects ostensibly agreed. Here, users agreed to processing but were likely confused with regard to " the type of data processes, the legal basis used, and the purposes of the processing, which ultimately restricts... users " possibility to exercise their' rights. [49] Thus, to make it plain, the EDPB concluded that :

> the unbalanced relationship between Whats-App IE and its users, combined with the " take it or leave it " situation that they are facing due to the lack of alternative services in the market and the lack of options allowing them to adjust or opt out from a particular processing under their contract with Whats-App IE, systematically disadvantages them, limits their control over the processing of their personal data and undermines the exercise of their rights under Chapter III GDPR. [50]

This would not be the last word from the EDPB on the point. In December 2023, it published another binding decision that invoked the same logic. This time, it rejected Meta's claim that, pursuant to Article 6(1)(f), it could rely on its " legitimate interest " as well as the performance of its contract to engage in behavioral targeting – a specific but extremely high-stakes form of data processing in the networked information economy. [51]

Evidently, at least according to the EDPB, the consumer sovereignty model of regulation has its limits. That is, even when consumers ostensibly agree to a service, Article 6's " lawful bases " provisions still require scrupulous engagement and oversight by government regulators (here, the Irish data protection authority

32. *See* Art. 6(1)(a). *See also* Recital 40.
33. *See* Art. 6(1)(b).
34. *See* Art. 6(1)(f). The other three lawful bases for data processing under Article 6 serve public policy priorities that do not turn on consumer sovereignty at all. In short, these permit companies to process personal information if doing so is necessary, first, to comply with other statutory and common law obligations involving, for example, employment, insurance, or banking laws, *see* Art. 6(1)(c) ; *See also* Recital 41 ; or, second, to protect the life and health of " the data subject or of another person, " *see* Art. 6(1)(d) ; *see also* Recital 46 ; or, third, to perform an official government or quasi-government function, *see* Art. 6(1)(e).
35. *See* European Data Protection Board, *Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding Whats-App Ireland Limited (Art. 65 GDPR)* (adopted Dec. 5, 2022 ; published Jan. 24, 2023), [para][para] 90, 114, 152.
36. Id. at [para][para] 112, 121.
37. Id. at [para] 105.
38. Id. at [para] 112.
39. Id. at [para] 118.
40. Id. at [para] 152.
41. Id. at [para] 99. *See also* id. at [para] 149.
42. Id. at [para] 111.
43. Id. at [para] 119.
44. Id. at [para] 119.
45. Id. at [para] 149.
46. Id. at [para] 149.
47. Id. at [para] 149.
48. Id. at [para] 149.
49. Id. at [para] 153.
50. Id. at [para] 156.
51. EDPB, Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR) (adopted Oct. 23, 2023 ; published Dec. 7, 2023), https ://edpb.europa.eu/our-work-tools/our-documents/urgent-binding-decision-board-art-66/urgent-binding-decision-012023_en.

and, in turn, the EDPB through the one-stop-shop mechanism) to evaluate the " specificities of the " service at issue and the power asymmetry between the controller and data subjects. [52]

The EDPB's interventions arguably reflect an emergent administrative " risk-based " approach to regulation in the EU, as opposed to a rights-based one. Consider, for example, provisions of the Digital Services Act (DSA). Article 25 in particular addresses " online interface design and organization " in recognition that some consumer-facing features are too opaque or confusing, rendering consumers vulnerable to manipulation. [53] Existing EU consumer protection law already ostensibly forbade such practices, [54] but the DSA does so far more explicitly now. Meanwhile, the EDPB and the FTC have intensified their policymaking and enforcement resources to protect against " dark patterns " in online consumer-facing interfaces. [55] Concerns about information and market power asymmetries animate these interventions.

Finally, consider the AI Act, which classifies AI systems into four categories that reflect their relative risk to consumers depending on the specific context of their application. [56] It explicitly prohibits (without regard to whether data subjects exercise rights or choose to consent) companies from employing systems that, among other things, process sensitive characteristics like political beliefs or sexual orientation, collect facial images from certain sources to create facial recognition databases, and engage in certain forms of biometric identification. It also requires companies to conduct impact assessments when they apply AI systems in high-risk sectors, including those involving health, safety, insurance, and banking. [57]

*

***

5 - Given these new legal authorities, the binding EDPB decisions arguably reflect an important inflection point in the evolution of government regulation of commercial data practices. At bottom, they reflect the view that consumers cannot adjudicate their consent or agreement to use an online service when the companies administer opaque data practices and provide online services under conditional or " take it or leave it " terms. [58] The implications of these decisions are potentially far reaching to the extent that they recognize, perhaps more directly than before, that information and power asymmetries define today's networked information economy. They suggest that legal authorities are adapting their regulatory approach to the ways in which companies currently process information.

To put it more starkly : today, consumer sovereignty models for legislation and regulation are insufficient, if not altogether inapposite. This is not to say that rights are not productive, at least perhaps as aspirational tropes. [59] They evoke politically and culturally salient commitments to due process and human dignity. [60] In terms of consumer protection, however, the consumer sovereignty model is insufficiently definite about the legal or normative constraints on opaque commercial practices and " take it or leave it " online services. Companies should continue to be alert to fairness, data minimization, purpose limitations, transparency, and accuracy. But those duties, as the EDPB has made clear, do not necessarily arise from the specific commercial relationship that a company has with any given data subject or consumer. They flow instead from the power and information asymmetries that define the relationship between consumers and the companies that collect their personal information or provide them services.■

52. Id. at [para] 151.
53. *See* Digital Services Act, Article 25.
54. This conclusion echoes the way in which European private law generally redresses " information asymmetry, unfairness, product risks, and [consumer] apathy when enforcing their rights " across professional and personal services. See generally Joasia Luzak, *Consumers in European Private Law* at 5, Uncovering European Private Law, Research Paper No. 2 (2022), https ://papers.ssrn-.com/sol3/papers.cfm ?abstract_id=4304778.
55. *See* European Data Protection Board, *Guidelines 3/2022 on Dark patterns in social media platform interfaces : How to recognise and avoid them* (adopted March 14, 2022) ; Federal Trade Commission, *Complaint, In re Epic Games*, FTC File No. 1923203 (Dec. 19, 2022), https ://www.ftc.gov/system/files/ftc-_gov/pdf/1923203EpicGamesComplaint.pdf. *See also* Organisation for Economic Co-operation and Development, *Dark Commercial Patterns* (Oct. 2022), https ://www.oecd.org/digital/dark-commercial-patterns-44f5°846-en.htm.
56. AI Act enumerating (1) unacceptable-risk (2) high-risk (3) limited-risk, (4) minimal/no-risk. *See* European Commission, Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM/2021/206 final.
57. *Ibid*.
58. See Daniel Solove, *The Limitations of Rights to Privacy*, 98 Notre Dame L. Rev. 975 (2023) ; Daniel Solove & Woodrow Hartzog, Breached ! : Why Data Security Law Fails and How to Improve It (2022) ; Ari Waldman, Industry Unbound : The Inside Story of Privacy, Data, and Corporate Power (2021) ; Aziz Z. Huq, *Constitutional Rights in the Machine-Learning State*, 105 Cornell L. Rev. 1875 (2020) ; Deven R. Desai & Joshua A. Kroll, *Trust but Verify : A Guide to Algorithms and the Law*, 31 Harv. J. L. & Tech. 1, 43 (2018).
59. The critique of rights is as old as rights themselves. Cf. Duncan Kennedy, *The Critique of Rights in Critical Legal Studies Edmund Burke* in Left Legalism/Left Critique (2002) ; Reflections on the Revolution in France (1790). Nothing in this essay means to directly engage this debate in political or moral theory. Nor does it take up the eternal questions about human free will, *see* James Gleick, *The Fate of Free Will*, N.Y. Rev. of Books (Jan. 18, 2024) (reviewing Kevin Mitchell, Free Agents : How Evolution Gave Us Free Will (2023), although the issues it raises of course invoke them. *Cf*. Jaron Lanier, You Are Not a Gadget (2011).
60. *See* Margot Kaminski, *The Right to Contest AI*, 121 Colum. L. Rev. 1957, 1990-91 (2021) ((arguing that the right to contestation, for example, promotes accuracy, the rule of law (i.e., " fair consistent, predictable, and rational across different individuals "), and human dignity). *See also* Danielle Citron & Ryan Calo, *The Automated Administrative State : A Crisis of Legitimacy*, 70 Emory L. J. 797 (2021) ; Danielle Citron, *Technological Due Process*, 85 Wash. U. L. Rev. 1249 (2008).

Technology and the digital rule of law

11

Taking Technical Standardization of Fundamental Rights Seriously for Trustworthy Artificial Intelligence

Gregory LEWKOWICZ,

Professor at Université Libre de Bruxelles, Perelman Centre & Director of the Smart Law Hub

Ritha SARF,

Research Assistant at HEC-Paris, Member of the Smart Law Hub

1 - In a seminal essay, E. Bruton Swanson explains that information systems have come to rule the world for a long time " by the rules they actually embody (...) mostly without drama as infrastructure that comes to our attention only when something goes awry ". [1] In recent years, the rapid digitization of society and the widespread deployment of artificial intelligence (AI) systems have only made this state of affairs more evident, and the glitches often more dramatic. The implementation of AI systems across various sectors, including education, justice, social welfare, migration, policing, and healthcare, often justified by enhanced efficiency, has been marred by a multitude of scandals and breaches of fundamental rights. [2] These incidents have revealed the risks associated with the unregulated adoption and deployment of these systems, prompting regulatory actions across the globe. In this context, technical standards have emerged as a promising tool for ensuring the trustworthiness of AI systems and their conformity with fundamental rights.

In this paper, we critically examine the emerging paradigm of technical standardization of fundamental rights for AI systems and explore potential solutions for advancing ongoing efforts. Firstly, we briefly present the current trends in AI regulation and fundamental rights, and the role envisioned for technical standards in this context, especially within the AI Act, the European Union (EU)'s flagship legislative initiative (I). Secondly, the paper discusses the main benefits and limitations of incorporating fundamental rights into AI technical standards (II). Finally, we critically examine the current landscape of AI technical standards and propose some methodological insights that may contribute to take fundamental rights seriously in the context of AI technical standardization (III).

1. Fundamental rights in AI regulation and the role of technical standards

2 - For a long time, discussions on AI regulation and the impacts of AI systems on fundamental rights were primarily confined to data and privacy issues. As a result, data protection dominated the global regulatory agenda, at least until 2020, leading to the first wave of regulations targeting these aspects worldwide. [3] Meanwhile, the extensive deployment of AI systems has revealed a broad spectrum of rights and freedoms that may be impacted by them, [4] impacts that cannot be solely addressed or encompassed by data protection alone, [5] especially when following the traditional approach to privacy. [6]

Therefore, while data regulation remains crucial and continues to evolve dynamically, the regulatory focus has shifted towards a more comprehensive approach that targets software and AI systems themselves. This new regulatory trend aims to address the ever-growing array of risks arising from AI systems at various governance levels, relying on a diverse set of instruments. These include guidelines, ethical norms, and legal measures at local, national, or regional levels, as well as initiatives like the Council of Europe's project for an international convention on artificial intelligence, human rights, democracy, and the rule of law. [7]

For instance, various multilateral organizations have published their own principles, such as the OECD's " Principles on Artificial Intelligence ", [8] the EU's " Ethics Guidelines for Trustworthy AI ", [9] and UNESCO's " Recommendations on the Ethics of Artificial Intelligence ". [10] The rise of generative AI has led to new initiatives, including the G7 " Hiroshima Guiding Principles " and its " Code of Conduct " on artificial intelligence. [11] In December 2023, the newly appointed UN AI advisory board released an interim report outlining key principles to guide the formation of new global AI governance institutions. [12] All these instruments extend beyond data regulation and aim to address the various dimensions of fundamental rights and values potentially put at risk by AI systems.

1. E. Burton Swanson, *How Information Systems Came to Rule the World and Other Essays*, New York/London, Routledge, 2022, p.66.
2. For an overview of various problematic use cases in these sectors across European countries see – European Digital Rights (EDRi), Uses cases : Impermissible AI and fundamental rights breaches, August 2020, 29 p.
3. See J. Huang, " Applicable Law to Transnational Personal Data : Trends and Dynamics ", *German Law Journal*, vol. 21, 6, 2020, pp. 1283-1308 ; G. Kapar, " Global Regulatory Competition on Digital Rights and Data Protection : A Novel and Contractive form of Eurocentrism ? ", Global Constitutionalism, 2022, pp. 1-29.
4. See e.g., A. Quintavalla & J. Temperman (eds.), *Artificial Intelligence and Human Rights*, Oxford, Oxford University Press, 2023 ; European Union Agency for Fundamental Rights, Getting the Future Right : Artificial Intelligence and Fundamental Rights, Report, 2020, 108 p.
5. See A. Mantelero, *Beyond Data : Human Rights, Ethical and Social Impact Assessment in AI*, The Hague, T.M.C. Asser Press 2022.
6. For a critical perspective, see I. Cofone, *The Privacy Fallacy : Harm and Power in the Information Economy*, Cambridge, CUP, 2024.
7. Council of Europe, Committee on Artificial Intelligence (CAI), Consolidated Working Draft of the Framework Convention on Artificial Intelligence, Human rights, Democracy and the Rule of Law, CAI (2023)18, 7 July 2023.
8. OECD, Recommendation of the Council on Artificial Intelligence, Adopted on May 22, 2019, and amended on November 8th, 2023.
9. High-Level Expert Group on AI, Ethics Guidelines for Trustworthy AI, Publications Office, 2019.
10. UNESCO, Recommendation on the Ethics of Artificial Intelligence, 2022.
11. G7, Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI Systems, 2023 and G7, Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems, 2023.
12. UN AI Advisory Body, Interim Report : Governing AI for Humanity, December 2023.

With the same comprehensive approach to risks, the surge in local, national, and regional laws specifically aimed at regulating AI systems is also remarkable and confirms the hypothesis of a race to regulate AI, indicative of a global battle to regulate technology. [13] Notable examples include China's Interim Administrative Measures for the Management of Generative AI Services [14] and Algorithmic Recommendation systems, [15] the US's AI Executive Order (EO), [16] the draft Canadian Artificial Intelligence Data Act, [17] and the Brazilian Bill No. 2338, which introduces a risk-based approach to AI regulation similar to the (almost) finalized EU AI Act. [18]

Despite their significant diversity in content and objectives, these various initiatives assign a role to technical standards in ensuring that AI systems either respect fundamental rights or uphold fundamental values. [19] As Voker Türk, the UN High Commissioner for Human Rights, remarked at the World Standards Cooperation, " the world of technological expertise, long the domain of standard-developing organizations, and the world of human rights, are moving closer" . [20]

This closer connection is particularly evident in the upcoming EU AI Act, which draws inspiration from traditional European product safety regulations. The Act imposes obligations on AI systems based on their associated risks and introduces specific responsibilities for both producers and operators of AI systems. [21] Specifically, producers of AI systems classified as high risk must perform a conformity assessment to affix the CE marking on the system they introduce to the market or put into service. [22] When harmonized standards developed by recognized European Standards Organizations (CEN, CENELEC, ETSI) exist, adherence to them grants a presumption of conformity with the regulation. [23] Producers may also demonstrate compliance by referring to other technical standards or their own specifications, but they must explain in that case how these meet the legal requirements.

At first glance, this approach appears to align with the longstanding " New Approach " principles within the European single market. However, it diverges by integrating, for AI systems, fundamental rights alongside conventional health and safety requirements. This innovation reflects a broader trend within the digital single market, where compliance with fundamental rights is becoming an integral aspect of product and service regulation. This move is also reflected in the Digital Services Act (DSA) [24] or the upcoming Health Data Space regulation, which underscores the importance of common specifications for " *interoperability, security, safety or fundamental right concern* ". [25]

The EU AI Act will introduce fundamental rights conformity assessment for high-risk AI systems. [26] In doing so, it significantly expands the traditional scope of technical standards and harmonized standards and positions the European Union at the forefront of the global movement towards the technical standardization of fundamental rights and values.

2. AI technical standards and fundamental rights protection

3 - The incorporation of fundamental rights into risk management and their inclusion in technical standards is not an entirely new concept. For example, the ISO 26000 :2010 standard on social responsibility has become an international framework for companies to comply with fundamental principles and rights at work. [27] However, with AI systems, this movement takes a significant step further. In this case, technical standards will be a crucial part of the conformity assessment process – unlike ISO 26000 :2010, which is not certifiable [28] – and intimately linked to market access. Moreover, the range of fundamental rights potentially affected by AI systems is limited only by the imagination. Given that ongoing global efforts to align AI with fundamental rights will largely depend on the technical standards ultimately developed, it is crucial to critically assess this approach on its merits. Understanding its advantages and limitations is especially important in the context of the upcoming EU AI Act.

Arguably, the most compelling argument in favor of using technical standards to ensure AI systems comply with fundamental rights is their proven track record in regulating technologies. Legal historians have illustrated that, since its inception in the 19th century, technical standardization has developed as a form of " engineer-made law, " often in competition with " lawyer-made law. " [29] This approach has been notably successful in setting global standards, a success that could be envied by many international lawyers. [30] By incorporating fundamental rights into these standards, a bridge can be created to facilitate communication with technical communities, such as engineers and data scientists. These professionals, for instance, might find it easier to work with fairness metrics integrated into technical standards than to navigate non-discrimination law and the case law of the European Court of

13. See N.A. Smuha, " From a " Race to AI " to a " Race to AI Regulation " : Regulatory Competition for Artificial Intelligence ", *Law, Innovation and Technology*, 13, 1, 2021, pp. 57-84 and A. Bradford, *Digital Empires : The Global Battle to Regulate Technology*, Oxford, Oxford University Press, 2023.
For an overview of the global AI regulatory landscape see – Stanford University, AI Index 2023 Annual Report, AI Index Steering Committee, Institute for Human-Centered AI, 2022, 386 p.
14. Interim Measures for the Management of Generative Artificial Intelligence Services, July 10, 2023.
15. Internet Information Service Algorithmic Recommendation Management Provisions – Effective March 1, 2022.
16. The White House, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, October 30, 2023. (Executive Order)
17. Government of Canada, The Artificial Intelligence and Data Act (AIDA), June 2022.
18. Proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on artificial intelligence and amending certain Union legislative acts, COM (2021)0206 – C9-0146/2021 – 2021/0106(COD) (AI Act). At the time of writing, the AI Act trilogue has ended but the final text adopted is yet to be released. The reference made to the AI Act in this paper refers to the European Parliament amended position being the most recent draft to date.
19. See Internet Information Service Algorithmic Recommendation Management Provisions art. 5 & art. 9 ; A. Hilliard, How is Brazil Leading South America's AI Legislation Efforts ? *Holistic AI*, November 20, 2023 ; Executive Order, Section 11 (b) ; UN AI Interim report, supra note 11, see institutional function number 2 on interoperability and number 3 on mediating standards and safety frameworks, p.21.
The interplay between technical standard setting and human rights was also discussed in the UN Human Rights Council 53rd session, see Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/53/42.
20. Volker Türk addresses World Standards Cooperation Meeting on Human Rights and Digital Technology, February 24, 2023 (accessible at https ://www.ohchr.org/en/statements/2023/02/turk-addresses-world-standards-cooperation-meeting-human-rights-and-digital).
21. AI Act, supra note 18, title III, chapter 2.
22. *Ibid*, art. 16.
23. *Ibid*, art. 40.
24. See G. Lewkowicz, " La liberté d'expression en algorithmes : un droit SMART de la liberté d'expression en ligne est-il inévitable ? " in J. Englebert (ed.), *La régulation des contenus haineux sur les réseaux sociaux*, Bruxelles, Anthemis, 2022, pp. 119-138.
25. Proposal for a regulation of the European Parliament and of the Council on the European Health Data Space, COM (2022) 197/2, article 10(h).
26. AI Act, supra note 18, art. 43.
27. See B. Frydman & A. Van Waeyenberge, *Gouverner par les standards et les indicateurs. De Hume aux rankings*, Bruxelles, Bruylant, 2013, chap. 4 and P. Lequet, " Loi " devoir de vigilance " : de l'intérêt des normes de management des risques ", *Revue juridique de l'environnement*, vol. 41, 2017/4, pp. 705-725.
28. International Standards Organization, ISO 26000, Guidance on social responsibility.
29. M. Vec, *Recht und Normierung in der Industriellen Revolution : Neue Strukturen der Normsetzung in Völkerrecht, staatlicher Gesetzgebung und gesellschaftlicher Selbstnormierung*, Nomos Verlag, 2006.
30. J. Yates & C.N. Murphy, *Engineering Rules : Global Standard Setting since 1880*, Baltimore, John Hopkins University Press, 2019.

Justice. [31] Generally, standards are already recognized as vital markers of market conformity across various industries, [32] making them a suitable medium for integrating fundamental rights considerations in AI systems.

Secondly, since standards are integral to upstream product development, linking AI system conformity with market entry standards enables direct intervention in their design. Addressing one of the main challenges of AI regulation – the limitations of *ex post* regulation – technical standards can be particularly effective. By setting *ex ante* requirements, they essentially establish a form of licensing, [33] that promotes a " compliance by design " approach, influencing both the " proxies " and back-end " choice architectures " of AI systems. [34] In this dynamic, while standards prompt a rethinking of traditional modes of fundamental rights protections, fundamental rights can concurrently transform the process through which technologies are developed.

On the other hand, several arguments question the suitability of technical standards for ensuring respect for fundamental rights. Some are based on the inherent nature of fundamental rights and technical standards. Others are entrenched in more contextual reasons regarding the functioning of standardization bodies.

Among the first category of arguments are those challenging the feasibility of translating fundamental rights into technical standards due to the context-dependency of these rights. [35] Fundamental rights exhibit a complex interplay that requires competitive balancing against each other. Such a balancing act is typically the domain of courts, which consider each case individually. This process necessitates a degree of discretion and an *ad hoc* approach to adequately weigh the rights involved, acknowledging the situational nature of fundamental rights. The inherent complexity and case-specific nuances of fundamental rights might, therefore, resist a one-size-fits-all standardization approach.

This consideration also raises crucial questions regarding the nature and the scope of standards being developed for the AI Act and similar initiatives. [36] Given their potential global impact, these standards could lead to a " regionalization of standards " [37] that reflect the values and norms of the countries and regions from which they originate. This regionalization may become more pronounced as standards move from embodying universal values to more specific and codified criteria. The risk of divergence becomes particularly evident in the realm of fundamental rights protection, such as the stark contrast in how freedom of expression is safeguarded in the United States, Europe, and China. [38] As technical standards become more involved in encoding fundamental rights, their universality may be fragmented, drawing attention to the international differences in interpreting the breadth and scope of *universal* rights. [39]

Certain authors argue that technical standards are also grossly inadequate to address fundamental rights concerns due to their unique conception of risk. [40] In the realm of technical standards, risk management is primarily about meeting market access criteria, following a logic of satisfaction. [41] Therefore, it is irrelevant whether a given system barely achieves or significantly surpasses the relevant standards. [42] Whereas the legal approach to fundamental rights is rooted in a principle of optimization : they should be safeguarded and advanced to the highest degree. This perspective thus advocates for a parallel system : one preserving health and safety via harmonized standards, and another one to address fundamental rights concerns framing risk differently. [43]

Other limits to fundamental rights technical standardization are more contextual and concern the legitimacy and ability of standardization bodies to undertake such a task. [44] This issue is partly linked to the type of stakeholders involved. Standardization bodies are dominated by industry actors and have been criticized for their vulnerability to industrial lobbying. [45] Such influence may have a negative impact on the protection of fundamental rights. [46] This was illustrated by the controversy over the exclusion of ETSI from the draft standardization request of the Commission for the AI Act. [47] ETSI's " pay-to-play " [48] governance model assigns more votes in meetings to members who pay higher subscription fees, leading to perceptions of heavy influence from foreign corporations. As a consequence, there is a risk that interested private parties might shape norms and values that ought to be democratically debated, particularly when these concern fundamental rights.

Also, the business model behind standardization bodies raises the questions of access to technical standards. [49] Paywalls standing between copy-righted standards and interested stakeholders have proven to be a challenge for small actors such as NGOs. [50] This difficulty becomes all the more pressing under the EU system, where harmonized standards are often " indispensable " when

31. See the interesting discussion of fairness metrics in S. Wachter *et al.*, " Why Fairness Cannot Be Automated : Bridging the Gap Between EU Non-Discrimination Law and AI ", *Computer Law & Security Review*, vol.41, July 2021.
32. P. Cihon, *Standards for AI Governance : International Standards to Enable Global Coordination in AI Research & Development*, Technical Report, Future of Humanity Institute, Oxford University, April 2019, p.7.
33. G. Malgieri & F. Pasquale, " Licensing high-risk artificial intelligence : Toward ex ante justification for a disruptive technology ", *Computer Law & Security Review*, Volume 52, 2024.
34. M. Hildebrand, " The issue of proxies and choice architectures : Why EU law matters for recommender systems ", *Frontiers in Artificial Intelligence*, 5, 789076, 2022, pp. 1-17.
35. M. Gornet, " The European approach to regulating AI through technical standards ", HAL Open Science – 04254949, 2023 and M. Almada & N. Petit, " The EU AI Act : A Medley of Product Safety and Fundamental Rights ? " ; *RSC Working Paper*, EUI, 2023, 27 p.
36. C. Perarnaud, " With the AI Act, we need to mind the standards gap ", *CEPS*, April 2023. (https ://www.ceps.eu/with-the-ai-act-we-need-to-mind-the-standards-gap/)
37. *Ibid*.
38. Malgieri & Pasquale, *supra* note 33, p.15.
39. The UN Interim Report (see *supra* note 11, p.19.) also notes that while " several important initiatives to develop technical and normative standards, safety, and risk management frameworks for AI are underway, there is a lack of global harmonization and alignment ".
40. M. Almada & N. Petit, *supra* note 35, p.20.
41. *Ibid*.
42. *Ibid*.
43. *Ibid*. p.26.
44. H. Fraser, J-M. Bello y Villarino, " Acceptable Risks in Europe's Proposed AI Act : Reasonableness and Other Principles for Deciding How Much Risk Management Is Enough ", *European Journal of Risk Regulation*, Published online 2023, pp.1-16 p.13.
45. M. McFadden, K. Jones, E. Taylor, G. Osborn, " Harmonizing Artificial Intelligence : The role of standards in the EU AI Regulation " ; *Oxford Information Labs*, 2021, 42 p, p.20.
46. C. Castets-Renard, & P. Besse, Ex ante Accountability of the AI Act : Between Certification and Standardization, in Pursuit of Fundamental Rights in the Country of Compliance. *Artificial Intelligence Law : Between Sectoral Rules and Comprehensive Regime. Comparative Law Perspectives*, C. Castets-Renard & J. Eynard (eds), Bruylant, 2023, 23 p, p.20.
47. L. Bertuzzi, Commission leaves the European standardization body out of AI standard-setting. Euractiv, December 7, 2022.
48. I. Rashid & S. Simpson, " The struggle for coexistence : communication policy by private technical standards making and its limits in unlicensed spectrum ", *Information, Communication & Society*, vol 24, 4, 2022, pp. 576-593, p.581.
49. Gornet, *supra* note 35, p.7 and R. Ducato, Why Harmonised Standards Should Be Open, 2023,IIC 54, pp.1173-1178, p.1173.
50. This is illustrated by the In Public.Resource.Org Case T-185/19., in which two non-profit organizations requested access to several harmonized standards listed in the EU official journal but whose full text stood behind a paywall. The Commission refused to grant access on the basis of the Article 4(2) of Regulation 1049/2001 arguing that such disclosure would undermine the protection of commercial interests including intellectual properties of standardization bodies. A first judgment was issued by the General Court in July 2021 in favor of the Commission. In their appeal, the organizations argued that the Court of First Instance wrongly assessed the copyright protection of HS, as HS are part of the law and cannot be copyrighted. See – Judgment of the General Court (Fifth Chamber, Extended Composition) of 14 July 2021. Public.Resource.Org, Inc. and Right to Know CLG v European Commission. Case T-185/19 ; Appeal brought on 23 September 2021 by Public.Resource.Org, Inc., Right to Know CLG against the judgment of the General Court (Fifth Chamber, Extended Composition) delivered on 14 July 2021 in Case T-185/19, Public.Resource.Org, Inc. and Right to Know CLG v European Commission.

complying with a given EU regulation. [51] As harmonized standards have grown to become part of EU law, [52] concerns over intellectual property protections clash with the rooted principle of free access to the law. [53] This principle seems all the more essential when it is fundamental rights, and not the dimensions of containers, that are the object of technical standardization.

Furthermore, beyond the question of legitimacy, there is a critical issue whether the process of standardization bodies " lend themselves to discussion of fundamental rights and their jurisprudence ". [54] Typically, these bodies focus on technical features and engineering processes, rather than discuss trade-offs between conflicting rights and interests in complex socio-political contexts. Standardization bodies have so far made minimal provision for the participation of civil society and other relevant stakeholders, [55] raising doubts about their capacity for meaningful integration of diverse perspectives. [56] For instance, while the current EU draft standardization request for the AI Act calls for a consultation with a broad array of stakeholders, [57] it remains uncertain how standardization bodies will develop the necessary expertise to engage with core legal aspects of fundamental rights protection. [58] Additionally, it is unclear whether the EU strategy on standardization, published by the Commission in February 2022, will fulfill its long-term objectives regarding the enhancement of " openness, transparency, and inclusiveness " [59] of the standardization process.

3. Taking Standardization of Fundamental Rights Seriously

4 - The technical standardization of fundamental rights in AI regulation is both profoundly problematic and inevitable. The problematic aspect arises from legitimate criticisms it faces. Indeed, contextual challenges may be addressed by reforming standardization bodies, their membership, and business models. Transforming these entities into multistakeholder and multidisciplinary deliberative forums, which adopt technical standards subject to judicial review under the rule of law, could be a viable, though a revolutionary, and complex technocratic solution. Yet, the challenges entrenched in the inherent nature of fundamental rights and technical standards are, by definition, not amenable to an easy solution.

Nevertheless, some form of technical standardization of fundamental rights appears inevitable, given that an increasing portion of our behaviors are mediated by digital technologies and interfaces. It is challenging to advocate for *de facto* adherence to the rules embedded in these often black-box technologies, solely to preserve the purity of fundamental rights in their *ex-post* application. Yet, at the same time, while technical standards can introduce meaningful fundamental rights safeguards in the AI-system development process, as they do so, *it matters how*. [60]

In the European Union, the draft standardization request from the European Commission for CEN and CENELEC falls short in providing clear guidance on how to address the legal dimensions of fundamental rights. [61] The AI Act only makes vague references to European values, treaties, and the need for stakeholder diversity, without offering concrete directives. [62] This ambiguity is compounded by the numerous, yet unspecific, mentions of fundamental rights, failing to establish a well-defined policy outlining the interaction between binding legal requirements and harmonized technical standards. [63] Even if standardization bodies strive to incorporate fundamental rights considerations and expertise into their processes, there remains significant uncertainty about the specific actions they should undertake and which rights they should consider. [64]

A closer examination of broader AI standardization endeavors reveals that most standards developed or in development primarily focus on ethics and fairness. [65] While fundamental rights do intersect with ethical values to some extent, these two notions should not be confused. The current landscape of technical standards for trustworthy AI falls short in providing the rights-based approach envisioned by the AI Act. [66] Relying predominantly on ethics to build a fundamental rights-based approach risks regressing to a time, nearly three-quarters of a century ago, before the development of international and regional human rights law, leaving us with frameworks that are, at best, vague. This concern is amplified by critiques from scholars who warn of " ethics washing ", [67] where ethical guidelines are perceived as mere facades to circumvent or delay the implementation of effective regulation.

The ISO/IEC 42001 :2023 technical standard on AI management systems, published in December 2023, exemplifies the limitations of the current approach of fundamental rights in AI standardization. This standard, likely to be endorsed by European standardization organizations, does establish a risk assessment step to evaluate significant impacts of AI systems on individuals and groups, specifically references areas such as physical and psychological well-being and *" universal human rights "*. [68] However, the standard leaves the responsibility for making design choices to mitigate such risks and for determining the appropriate metrics to evaluate the contextualized application of an AI system solely to its providers. In our view, current standards like ISO/IEC 42001 :2023 fall short

51. Gornet, *supra* note 35, p.7 ; Opinion of Advocate General Medina delivered on 22 June 2023. Case C-588/21 P. Public.Resource.Org, Inc., Right to Know CLG v European Commission, para 33.
52. Judgment of the Court (Third Chamber) of 27 October 2016. James Elliott Construction Limited v Irish Asphalt Limited. Request for a preliminary ruling from the Supreme Court (Ireland). Case C-613/14, para 40.
53. Opinion of Advocate General Medina, *supra* note 57, para 72.
54. McFadden and al., *supra* note 45, p.19.
55. See C. Galvagna, " Discussion Paper : Inclusive AI Governance ", *Ada Lovelace Institute*, 2023, 65 p, p.9. ; McFadden and al, supra note 45, p.20. ; H. Pouget, " The EU's AI Act Is Barreling toward AI Standards That Do Not Exist ", *Lawfare*, January 12, 2023.
56. *Ibid*.
57. European Commission, Draft standardization request to the European Standardization Organizations in support of safe and trustworthy artificial intelligence, recital (14). (Draft standardization request)
58. One challenge that comes with the cost of attending standardization process meetings and making contributions is the demand for capital and human intensive resources which are generally available to private companies. One suggestion that has been formulated is amending the EU Standardization Regulation to reform the funding and governance of European Standardization Bodies to support diverse participation. See " H.W. Micklitz, " The Role of Standards in Future EU Digital Policy Legislation : A Consumer Perspective ", Commissioned by ANEC and BEUC, July 2023, 196 p, p.171.
59. European Commission, Communication from the Commission – An EU Strategy on Standardization : Setting Global Standards in Support of a Resilient, Green and Digital EU Single Market, COM (2022) 31 final, February 2, 2022, p.4.
60. As concluded by K.J.M. Matus and M. Veale in their assessment of certification systems for machine learning " if there is an acceptance that standards are a required approach, sustainability shows us that the question of what kind of standard is not inconsequential, and that there may be a trade-off between what it is possible to standardize, and the desired outcomes of the standard ". See K.J.M Matus & M. Veale, " Certification systems for machine learning : Lessons from sustainability ", *Regulation & Governance*, vol. 16, 2022, pp. 177-196, p.187.
61. Draft standardization request, *supra* note 52, recital (14). ; AI Act, *supra* note 18, recital 61(a), recital 72(b), recital 85, article 9 para 4-1.
62. AI Act, *supra* note 18, recital 61(a), recital 72(b), recital 85, article 9 para 4-1.
63. Micklitz, *supra* note 52, p.70.
64. *Ibid*.
65. See ibid p.114-153, and McFadden, *supra* note 45, p.29-40 for an overview of existing and developing AI standards by various Standard Setting Organizations.
66. Garrido, J.O., Tolan, S., Hupont Torres, I., Fernandez Llorca, D., Charisi, V., Gomez Gutierrez, E., Junklewitz, H., Hamon, R., Fano Yela, D., & Panigutti, *AI Watch : Artificial Intelligence Standardisation Landscape Update*. EUR 31343 EN. Report, Publications Office of the European Union. 2023, 44 p, p.11.
67. B. Wagner, " Ethics as an Escape from Regulation : From Ethics-Washing to Ethics-Shopping ", in Hildebrandt, M. (Ed.), *Being Profiling. Cogitas ergo sum*, Amsterdam University Press, 2018, pp. 86-90.
68. ISO / IEC 42001, Information technology Artificial intelligence Management system, 2023, section 6.1, 8.2 read conjointly with Annex B (normative), section B5.

of fulfilling the aspirations of technical standardization of fundamental rights because they do not take fundamental rights seriously.

From a methodological perspective, taking fundamental rights seriously involves bridging the rights/standard gap to pave the way for the development of more robust socio-technical standards. In the context of the AI Act, this would involve operationalizing the risk identification process to map the most relevant fundamental rights to the high-risk areas defined by the legislation. [69] For each high-risk use case, the potentially affected fundamental rights should be contextually analyzed and broken down into their various dimensions based on existing law and jurisprudence. This approach aims to create a more precise mapping of the various rights and freedoms relevant to each high-risk area, moving beyond broad concepts like " universal human rights ", " fairness " or " bias-free systems. " Instead, it provides a nuanced understanding tailored to the specific rights most relevant to application cases.

Consider the instance of AI systems used by judicial authorities for interpreting law and facts. [70] The right to a fair trial is undoubtedly a relevant fundamental right in this use case. However, the risks associated with using an AI system in this context must be assessed across the various dimensions of this right. It is therefore essential to dissect the right to a fair trial into its distinct components : judicial independence, impartiality, motivation, publicity, adversarial principle, equality of arms, presumption of innocence and access to justice. This breakdown facilitates a detailed evaluation of how each aspect of the right to a fair trial might be impacted by a given AI system.

The next step involves developing risk assessment methods to evaluate the significance of the impact of such a system on each component of the right to a fair trial. This method should incorporate the elements of risk significance as outlined in the AI Act, including the intensity, duration, severity, and probability of occurrence, as well as the exposure of individuals versus groups. [71] Once the relevant rights are identified and their risk significance is quantified, the findings can be visually represented using radial graphs plotting the different rights and components to show their associated risk for a given use case, as illustrated below. [72]

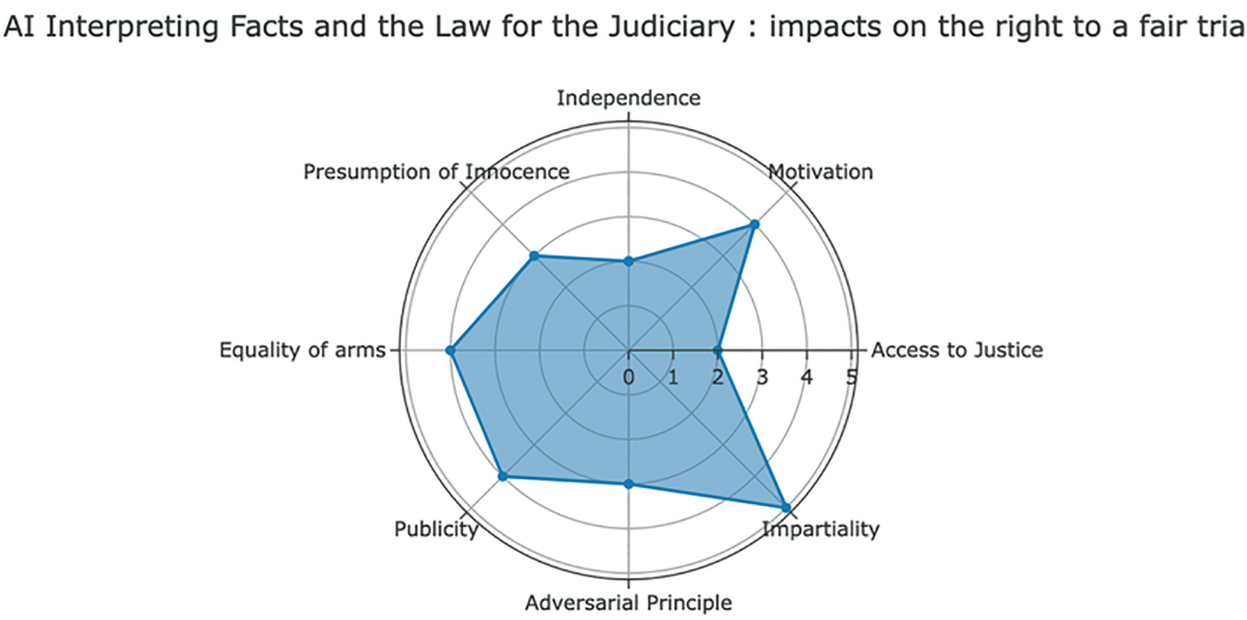

Figure 1. Mapping of the right to a fair trial

For each dimension of the right to fair trial, it becomes feasible to evaluate the effectiveness of existing metrics, performance standards, or process standards in mitigating these risks. This mapping process facilitates a comprehensive understanding of the interplay between technical tools and legal requirements and helps identify existing gaps. Such an approach would offer guidance, firmly grounded in law and jurisprudence, to AI providers. It may also aid ongoing standardization efforts that aim to tackle the complex challenge of fundamental rights standardization.

This methodological approach describes a way to take fundamental rights seriously in the context of the technical standardization of AI. It aims to translate the legal concept of fundamental rights into actionable parameters in a technical setting, potentially leading to the development of " new machine-readable variables " [73] that represent relevant rights-based features and targets. If the technical standardization of fundamental rights is indeed inevitable, it is imperative that we focus on upholding these rights rigorously, rather than settling for vaguely defined ethical guidelines.■

69. AI Act, *supra* note 18, art. 6, annex III.
The Annex lists 8 high-risk domains including AI used for administration of justice and democratic processes with a list of associated use cases subject to review.
70. AI Act, *supra* note 18, annex III, para 8, point a.
71. *Ibid*, art.3.
72. The radial graph presents the different dimensions of the rights to a fair trial and their respective level of risk in the context of the use of an AI system. This graph is a visual example and does not represent the final result proposed by the methodology. Generated from Radar Chart Creator, Copyright © 2024 All Rights Reserved Barcelona Field Studies Centre S.L.
73. Hildebrandt, *supra* note 34.

12

Going Deep : EU Copyright, Generative AI and the Competition Rationale Underlying Originality

Julien CABAY,

Professor and Director of JurisLab at Université Libre de Bruxelles,
Associate Professor at Université de Liège

In the current debate on the copyrightability of artificial intelligence [AI] production, several arguments were brought in relation to the foundations and rationales of copyright law. Against this theoretical background, a clear line was drawn between AI-generated and AI-assisted production. Whereas it seems now generally admitted that copyright will not vest with the former because of its complete lack of authorship, the latter seems eligible to such protection as there is here room for human intervention. Though human authorship is a bedrock requirement of copyright, it does not however suffice to conclude in general that AI-assisted productions would fall within its realm. Other rationales justify the grant or denying of this protection. Amongst those, the one underlying the US merger doctrine, and that can be found in the CJEU case law (Copyright, Design, Trademark), shows that copyright protection is probably not fit for AI-assisted productions per se. This idea, that connects the competition foundations of copyright and the basic technical features of Generative AI, was apparently left unexplored. Enshrined in Intellectual Property theory, it exemplifies that the New Digital Rule of Law is not simply a New Rule of Law in the Digital.

1 - In recent times, the greatest advancement of artificial intelligence [AI] was made possible thanks to deep learning. The multilayer architecture that characterizes deep learning inspired me the structure of the analysis I propose here of the possibility for an AI output to qualify for copyright protection.

Indeed, between the input (AI production) and the output (copyright status) layers, I think there are many hidden layers (copyright architecture), some of which remained unveiled in the literature.

In the current debate on the copyrightability of AI production, several arguments were brought in relation to the foundations and rationales of copyright law. Against this theoretical background, a clear line was apparently drawn between AI-generated and AI-assisted production.

Whereas it seems now generally admitted that copyright will not vest with the former because of its complete lack of authorship, the latter seems eligible to such protection as there is here room for human intervention. Though human authorship is a bedrock requirement of copyright, it does not however suffice to conclude in general that AI-assisted productions would fall within its realm. Other rationales justify the grant or denying of this protection.

Amongst those, the one underlying the US *merger doctrine*, and that can be found in the CJEU case law (Copyright, Design, Trademark), shows that copyright protection is probably not fit for AI-assisted productions per se. This idea, that connects the competition foundations of copyright and the basic technical features of Generative AI, was apparently left unexplored.

The aim of this contribution is to raise awareness of this inner competition rationale and its application, through diving into the EU copyright foundations. Somewhat of a deep learning of AI and EU Copyright.

1. Looking at the Surface : Deep Learning, Generative AI and EU Copyright

2 - Deep Learning methods have dramatically improved the state-of-the-art in various tasks traditionally addressed by AI technologies. As LeCun, Bengio & Hinton emphasizes, " it has turned out to be very good at discovering intricate structures in high-dimensional data and is therefore applicable to many domains of science, business and government " [1].

Deep learning as a machine learning process and architecture can be described as such :

> Representation learning is a set of methods that allows a machine to be fed with raw data and to automatically discover the representations needed for detection or classification. Deep-learning methods are representation-learning methods with multiple levels of representation, obtained by composing simple but non-linear modules that each transform the representation at one level (starting with the raw input) into a representation at a higher, slightly more abstract level. With the composition of enough such transformations, very complex functions can be learned [2].
>
> (...)
>
> A deep-learning architecture is a multilayer stack of simple modules, all (or most) of which are subject to learning, and many of which compute non-linear input-output mappings. Each module in the stack transforms its input to increase both the selectivity and the invariance of the representation [3].

As Goodfellow *et al.* mentioned :

1. Y. LeCun et al., *Deep learning*, Nature, 2015, Vol. 521, p. 436.
2. *Ibid.*
3. *Ibid.*, p. 438.

> The promise of deep learning is to discover rich, hierarchical models that represent probability distributions over the kinds of data encountered in artificial intelligence applications, such as natural images, audio waveforms containing speech, and symbols in natural language corpora [4].

Still according to Goodfellow *et al.*, deep generative models have however had less of an impact due to several difficulties, which led those authors to propose a new generative model called Generative Adversial Networks (GANs). GANs had impressive results in various applications [5] and eventually drew general public attention in 2018 when the portrait of Edmond de Bellamy [6], created by the French collective Obvious with the use of GANs, was auctioned at Christie's and sold 432.500 $. Since then, interest from the general public has grown even more for Generative AI, with the releasing of applications based on Large Language Models such as ChatGPT, Dall-E, Midjourney, Stable Diffusion, etc. In the art (and copyright) community, Midjourney attracted special attention in 2022 after a picture it generated, entitled *Théâtre d'opéra spatial*, won a prize at the Colorado State Fair's annual art competition [7].

Generative models have actually a long history in AI. But core advancements in the field were recently made possible thanks to " training more sophisticated generative models on larger datasets, using larger foundation model architectures, and having access to extensive computational resources (...) [in addition to researchers] exploring ways to integrate new technologies with [Generative AI] algorithms " [8]. According to Cao *et al.*, the nowadays " dominant backbone for many generative models in various domains " is the " transformer architecture ", that was first introduced for Natural Language Processing tasks in 2017, and later applied in Computer Vision [9].

The flourishing of Generative AI impressive achievements and user-friendly applications did not only attract the attention of the public in general, but became an object of great interest for many copyright scholars and practitioners as well. Over the past years, countless of scientific and position papers have been published over the copyrightability of AI generated products [10], and it seems the stream is not about to stop. Certainly not as long as the law will remain uncertain.

At the policy level, the EU institutions first approached the Generative AI through the lens of copyright law, in an evanescent suggestion made in a *Report with recommendations to the Commission on Civil Law Rules on Robotics* by the European Parliament. In the explanatory statement, the Parliament called on the Commission for the " elaboration of criteria for " own intellectual creation " for copyrightable works produced by computers or robots (...) " [11]. That demand was removed from the resolution finally adopted and the Commission never moved on, remaining silent in most of its subsequent communications [12]. It limited itself to stressing in very general terms the need to think of the interactions between AI and intellectual property [13], including a " reflection on how and what is to be protected " [14]. In particular, it emphasized that :

> AI technologies are creating new works and inventions. In some cases, for instance in the cultural sector, the use of inventive machines may become the norm. These developments raise the question of what protection should be given to products created with the help of AI technologies (...) [15].

Given those very few statements, it was not surprising that the AI Act Proposal [16] published in 2021 did not contain any provision related to the copyright status of such products. Amendments adopted by the Parliament did not add much to this, though Generative AI came under closer scrutiny (ChatGPT having been released in the meantime), eventually leading to more detailed obligations upon their providers [17].

The question of the copyright status of their products remains however fully open.

2. Beneath the Surface : The " Result " and " Process " Approaches to Artificial Intelligence and Copyright

3 - For those who are not skilled in the art – such as most of us, simple copyright lawyers –, understanding deep learning and AI is quite challenging, especially when confronted to the technical differences between all models. As a consequence, discussing the status of the output of an AI seems delicate.

There are, however, essentially two ways to address this difficulty.

On the one hand, our inability to cope with the underpinnings of the technology might be completely disregarded. We could consider the " technological neutrality " [18] or the " one size fits all " [19] principles that govern copyright law as appropriate answers to this problem, the technical features being irrelevant and therefore left out of the discussion.

Following this reasoning, only the result would matter. In other words, if the AI output resembles the subject matter of copyright

4. I. Goodfellow *et al., " Generative adversarial nets "*, in Advances in neural information processing systems, 2014, Vol.27 (pp. 2672-2680), arXiv :1406.2661v1 [stat.ML] (at p. 1).
5. Y. Cao *et al., A Comprehensive Survey of AI-Generated Content (AIGC) : A History of Generative AI from GAN to ChatGPT*, 2023, arXiv :2303.04226v1 [cs.AI] (at p. 4).
6. GANs Algorithm, Inkjet printed on Canvas, 70x70cm [https ://obvious-art.com/portfolio/edmond-de-belamy/].
7. K. Roose, *An A.I.-Generated Picture Won an Art Prize. Artists Aren't Happy*, The New York Times, September 2nd 2022 [https ://www.nytimes.com/2022/09/02/technology/ai-artificial-intelligence-artists.html].
8. Y. Cao *et al., op. cit.*, p. 2.
9. *Ibid.*, p. 4.
10. I do not intent here to carry out the impossible task to cover this very broad literature and will in part rely on previous work of mine (and supporting references), J. Cabay, *Droit d'auteur et intelligence artificielle : comparaison n'est pas raison*, Entertainment & Law, 2019, 307-325 ; J. Cabay, *Mort ou résurrection de l'auteur ? A propos de l'intelligence artificielle et de la propriété intellectuelle*, Revue de la Faculté de Droit de l'Université de Liège, 2019, pp. 179-190. In addition, I would suggest reading as a great overview of the current state of the art (and providing additional and more recent references) G. Frosio, " Four theories in search of an A(I) Author ", *in* R. Abbott (ed.), *Research Handbook on Intellectual Property and Artificial Intelligence*, Cheltenham, Edward Elgar, 2022, pp. 155-177.
11. Report with recommendations to the Commission on Civil Law Rules on Robotics, European Parliament, 2017, 2015/2103(INL).
12. EU Commission White Paper, *On Artificial Intelligence – A European Approach to Excellence and Trust*, 2020, COM(2020) 65 final ; EU Commission Communication, *A European strategy for data*, 2020, COM(2020) 66 final ; EU Commission Communication, *Shaping Europe's digital future*, 2020, COM(2020) 67 final ; EU Commission Communication, *Fostering a European Approach to Artificial Intelligence*, 2021, COM(2021) 205 final.
13. EU Commission Communication, *Artificial Intelligence for Europe*, 2018, COM(2018) 237 : *" Reflection will be needed on interactions between AI and intellectual property rights, from the perspective of both intellectual property offices and users, with a view to fostering innovation and legal certainty in a balanced way "*.
14. EU Commission Communication, *Making the most of the EU's innovative potential – An intellectual property action plan to support the EU's recoverty and resilience*, 2020, COM(2020) 760 final.
15. *Ibid*.
16. Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, European Commission, 2021, COM(2021) 206 final.
17. *See* Article 28(b)(4) of the version of the Artificial Intelligence Act adopted on 14 June 2023 by the European Parliament.
18. *See* for example, interpreting the private copying exception in light (to encompass saving in a cloud computing services) of this principle : CJEU, *Austro-Mechana Gesellschaft zur Wahrnehmung mechanisch-musikalischer Urheberrechte Gesellschaft mbH v Strato* AG, C-433/20, 24 March 2022, § 27.
19. *See* for example, clarifying that objects that qualify for design protection are subject to the same copyright requirement of protection that applies to all works : CJEU, *Cofemel – Sociedade de Vestuário SA v G-Star Raw* CV, C-683/17, 12 September 2019.

law, then it could attract copyright law protection. Accordingly, even an output entirely generated by an AI could qualify for protection [20]. Though this radical view is in a very minority because of the complete lack of authorship, it seems widely admitted that an AI generated output could be protected when there is at least some human intervention in the process [21]. It is true that this second view takes into account the fact that human intervention is in the loop. Yet, the focus remains on the result.

On the other hand, one could try to alleviate the burden of entering into the complexities of the technology through focusing on a low rather than a high level of granularity. Whatever type of AI we consider, the models are entrenched in mathematics, statistics and probabilities [22]. And this is by no means irrelevant. Following this approach, the focus would not be on the specific result anymore. It would consider instead the basic technical features of the process to achieve that type of results.

The place we give to the human intervention in the production of a hypothetical " work " with the assistance of a Generative AI appears differently according to each of those two approaches.

If we consider the human intervention in relation to the result (first approach), the situation of AI is actually very similar to that, for instance, of photography, where one can find room for " free and creative choices " in the preparation phase, the setting up or the editing stage [23]. The question then is whether the author, by making those choices, could stamp the result with his " personal touch ", making it a " work " that is " original " [24]. That is, the typical copyright question.

But if we consider the human intervention in relation to the process (second approach), then we should probably address the question differently. According to its usual meaning, a " choice " is " an act of choosing between two or more possibilities " [25]. A camera does certainly not make such choices, in particular the type of camera that were in use in the late 19th century and triggered the copyrightability issue of photographs, back in the times [26]. It is however less clear with an AI, since its output stem from a machine learning process based on mathematical, statistical and probability rules. Then, one can wonder whether the application of those rules is not, to some extent, comparable to making a choice between two or more possibilities.

In such context, it is not much a matter of the choices made by the human being that we should address, but rather of the " choices " that can be made by the AI. The relevant question would be then whether the human being, by making choices, has produced a result that could or could not have been generated by the AI. Indeed, if the maths, statistics and probabilities underlying the model could trigger an identical or similar result, it is questionable whether the result achieved (only in part) by the human being can be deemed the " author's own intellectual creation " bearing his " personal touch ".

To address this question, we must deepen our analysis of copyright law.

3. Shallow Copyright : The First Layers (Human Authorship)

4 - Much has been written about what I call here the " first layers " of the analysis and it is not the purpose of this contribution to describe the state of the art [27]. We can however shortly summarize the main arguments and opinions. Basically, they all revolve around the " human authorship " requirement, which importance can be evidenced by the recent refusal by the US Copyright Office to register as a copyrighted work the *Théâtre d'opéra spatial* mentioned above [28]. In support of that rejection, it put emphasis on the fact that " human authorship is a bedrock requirement of copyright " [29].

In short [30], firstly, the justifications for copyright protection are not met with AI generated contents. The AI must not be incentivized to produce outputs and there is no personality to be rewarded for its work.

Secondly, copyright protection is subject to the requirement of an author, being a natural person involved in the creation of the work. Absent this person, there is no room for copyright protection.

Thirdly, the originality requirement supposes that the author expresses his personality in the work. With no human being originating the output, then it can be found no traces of originality therein.

Obviously, those arguments are true only if we consider a result entirely generated by an AI. The problem remains with the vast array of outputs that were not entirely generated by AI.

With regard to those outputs, several proposals were made but they seem to mostly conclude the same way : copyright protection is likely when there is room left to the human intervention, making the contribution possibly original [31].

If we try to frame those arguments and opinions into the two approaches I identified in the previous section, we see that they mostly relate to the first one. The problem with this " first layers " analysis is its assumption that the distinction between AI-generated and assisted works is a dichotomy [32], whereas it should be rather

20. *See* in particular R. C. Denicola, *Ex Machina : Copyright Protection for Computer-Generated Works*, Rutgers University Law Review, 2016, Vol. 69, pp. 251-287.
21. *See* for example the AIPPI Resolution on Copyright in artificially generated works adopted on 18 September, 2019 at AIPPI World Congress in London [https ://www.aippi.org/content/uploads/2022/11/Resolution_Copyright_in_artificially_generated_works_English.pdf]. See also recently for examples in the EU the answers in national reports (available here : https://www.alai.org/en/assets/files/2023-congress-paris.zip) to question 4.2 of the questionnaire for the ALAI 2023 Paris Congress on *Copyright, Related Rights and Artificial Intelligence* by Germany of Greece.
22. *See* in general A. Gelman & A. Vehtar, " *What are the most important statistical ideas of the past 50 years ?* ", 2021, arXiv :2012.00174v5.
23. CJEU, *Eva-Maria Painer v Standard VerlagsGmbH and Others*, C-145/10, 1 December 2011, § 91 : " *In the preparation phase, the photographer can choose the background, the subject's pose and the lighting. When taking a portrait photograph, he can choose the framing, the angle of view and the atmosphere created. Finally, when selecting the snapshot, the photographer may choose from a variety of developing techniques the one he wishes to adopt or, where appropriate, use computer software* ".
24. *Ibid.*, § 92.
25. Oxford Learner's Dictionary of Academic English, [https ://www.oxfordlearnersdictionaries.com/definition/academic/choice].
26. The arguments at the time were somewhat related to the contemporary discussion and are worth the comparison. On this debate, see in particular E. Pouillet, *Traité théorique et pratique de la propriété littéraire et artistique et du droit de représentation*, Paris, Marchal, Billard et C[ie], 1879, pp. 91-99. It must also be emphasized that the United States Supreme Court decision that upheld the power of Congress to extend copyright protection to photography (*Burrow-Giles Lithographic Co. v. Sarony*, United States Supreme Court, 111 US 53, 1884) has proved an important precedent in support of rejecting copyright protection for AI-generated works. *See also Thaler v. Perlmutter*, United States District Court, District of Columbia, 2023 WL 5333236, 2023, §§10-11.
27. *See* recently for a good overview G. Frosio, *Four theories in search of an A(I) Author, in* R. Abbott (ed.), Research Handbook on Intellectual Property and Artificial Intelligence, 2022, pp. 155-177.
28. *See* the Letter of the U.S. Copyright Office Review Board, 5 September, 2023 [https ://acrobat.adobe.com/link/review ?uri=urn%3Aaaid%3Ascds%3AUS%3Aea3099df-32e2-3767-b953-58cc252de9be].
29. As it was stated in another recent decisions by the District Court of Columbia involving another AI-generated work entitled *A Recent Entrance to Paradise* (*Thaler v. Perlmutter, op. cit.*, § 4).
30. *See* for an easy access to the basic arguments that have been further developed in the subsequent literature, A. Ramalho, *Will Robots Rule the (Artistic) World ? : A Proposed Model for the Legal Status of Creations by Artificial Intelligence Systems*, Journal of Internet Law, 2017, Vol. 21, pp. 12-26.
31. AIPPI Resolution on Copyright in artificially generated works, *op. cit.*
32. *See* for examples in the EU, the answers in national reports (available here : https ://www.alai.org/en/assets/files/2023-congress-paris.zip) to question 4.3 of the questionnaire for the ALAI 2023 Paris Congress on *Copyright, Related Righs and Artificial Intelligence* (" How can we distinguish between AI-assisted

considered a *continuum* [33] [34]. It therefore fails to take into account the fact that the risks associated with undesirable outcomes of a protection for AI-generated outputs might be equally present in case of a protection given to some AI-assisted outputs. For that reason, I already suggested that this approach was flawed [35].

To overcome this flaw, I consider necessary to adopt the second approach identified in the previous section, which supposes to deepen the analysis of the subject matter and requirements for protection of copyright.

Indeed, from an EU normative standpoint, this " first layers " analysis is exclusively based on a literal interpretation of those subject matter and requirements for protection according to EU law. Yet, the CJEU has consistently held that the meaning and scope of a term must be determined not only by considering its usual meaning in everyday language, but also by taking into account the context in which it occurs and the purposes of the rules of which it is part [36].

Since all those terms related to " work " and " originality " were pulled out from the EU directives by the CJEU itself, starting with *Infopaq* [37], a correct understanding thereof should take into consideration its broader case law.

4. Deep Copyright : The Bottom Hidden Layers (Competition Rationale)

5 - At the EU level, it is settled case-law that the concept of " work " is :

> An autonomous concept of EU law which must be interpreted and applied uniformly, requiring two cumulative conditions to be satisfied. First, that concept entails that there exist an original subject matter, in the sense of being the author's own intellectual creation. Second, classification as a work is reserved to the elements that are the expression of such creation [38].

Besides the endorsement of the personalist approach [39], those two requirements for protection have been refined by the CJEU, through the development of the " free and creative choices " criteria for assessing originality [40], and the precision that the expression shall make the subject matter " identifiable with sufficient precision and objectivity " [41].

Though the CJEU did not adopt an explicit normative approach to support those interpretation, careful scrutiny seems to evidence an underlying rationale.

Three cases in particular exemplify this rationale.

First, in *Football Dataco*, the CJEU explicitly stated that neither the " significant labour and skill of its author " in the creation, selection or arrangement of data, nor the fact " that selection or arrangement includes " adding important significance " to that data " are relevant for that creation, selection or arrangement of data to be considered original [42]. In other words, the " added value " of the output with regards to the input does not justify, as such, copyright protection. As the facts of this case were concerned with a database, one can certainly trace back the underlying rationale in the *Magil* [43] and *IMS Health* [44] cases. In *Magil*, the CJEU found that, under particular circumstances, the use of exclusive rights which are entitled to the copyright holder on the data of which he is the sole source (*Magil*) would constitute an abuse of dominant position. In *IMS Health*, the CJEU further constructed the law to reach the same conclusion with regards to an arrangement of data that has become a *de facto* standard. Putting it simply, in those two cases competition law was used as a redress mechanism of copyright law to limit exclusive appropriation of the added value associated with the creation, selection or arrangement of data. As it appears in *Football Dataco*, competition law concerns are somehow internalized to strike an appropriate balance within copyright law through the interpretation of its requirements for protection.

Second, in *Levola*, the CJEU explicitly justified the exigence of " sufficient precision and objectivity " of the expression on the basis of competition concerns. Especially, the CJEU explained that :

> Individuals, in particular economic operators (...) must be able to identify, clearly and precisely, what is the subject matter of protection which third parties, especially competitors, enjoy [45].

In other words, the output must be clearly outlined, in order to ensure " legal certainty " [46]. The borrowing by the CJEU to the *Sieckman* [47] case in trademark law is evident [48]. And when one reminds that following numerous decisions of the CJUE, trademark has an " essential role in the system of undistorted competition which the EC Treaty seeks to establish " [49], it seems then clear that the underlying rationale *Levola* is similarly a balancing of copyright law through internalization of competition concerns. This is even more obvious when we have in mind the *SAS Institute* case, in which the CJEU stated that " ideas " (as opposed to " expression ") cannot be protected since it would be " to the detriment of technological progress and industrial development " [50], the promotion of which is traditionally devoted to competition.

Third and foremost, in *Brompton*, the CJEU made clear that not every " choice ", even being " free ", triggers originality. In this case, the CJEU rejected the so-called " multiplicity of forms " doctrine [51], through stating that :

> Even though there remains a possibility of choice as to the shape of a subject matter, it cannot be concluded that the subject

outputs and outputs generated by an AI ? ") by Croatia, Germany, Greece or Portugal. *See* also the more nuanced answers by France or Poland.

33. J. McCutcheon, *The Vanishing Author in Computer-Generated Works : A Critical Analysis of Recent Australian Case Law*, Melbourne University Law Review, 2013, Vol. 36, p. 929.
34. *See* for examples in the EU, the answers in national reports to question 4.3 of the questionnaire for the ALAI 2023 Paris Congress on *Copyright, Related Righs and Artificial Intelligence* (mentioned above) by Belgium (envisaging a " spectrum " with at the one extreme " AI systems that function as a tool to assist and/or enhance human creativity " and at the other extreme " more autonomous AI, having transcended its role as an instrumentality and having independently created a work that exhibits the requisite creativity, which experts and non-experts alike cannot distinguish from a work generated by a human "). *See also* the answer by the Netherlands (considering " it is a matter of degree ").
35. J. Cabay, *Droit d'auteur et intelligence artificielle : comparaison n'est pas raison, op. cit.*, p. 325.
36. *See* for one copyright example CJEU, *Johan Deckmyn and Vrijheidsfonds VZW v Helena Vandersteen and Others*, C-201/13, 3 September 2014, § 19.
37. CJEU, *Infopaq International A/S v Danske Dagblades Forening*, C-5/08, 16 July 2009.
38. *See* for example CJEU, *Cofemel – Sociedade de Vestuário SA v G-Star Raw CV, op. cit.*, § 29.
39. CJEU, *Eva-Maria Painer v Standard VerlagsGmbH and Others, op. cit.*, § 92.
40. *Ibid*., §§ 87-94. *See also* CJEU, *Football Association Premier League Ltd and Others v QC Leisure and Others / Karen Murphy v Media Protection Services Ltd*, joined cases C-403/08 and C-429/08, 4 October 2011, §§96-99.
41. CJEU, *Levola Hengelo BV v Smilde Foods BV*, C-310/17, 13 November 2018, § 40.
42. CJEU, *Football Dataco Ltd and Others v Yahoo ! UK Ltd and Others*, C-604/10, 1 March 2012, §§ 41-42.
43. ECJ, *Radio Telefis Eireann (RTE) and Independent Television Publications Ltd (ITP) v Commission of the European Communities*, joined cases C-241/91 P and C-242/91, 6 April 1995.
44. ECJ, *IMS Health GmbH & Co. OHG v NDC Health GmbH & Co. KG*, C-418/01, 29 April 2004.
45. CJEU, *Levola Hengelo BV v Smilde Foods BV*, op. cit., § 41.
46. *Ibid*.
47. ECJ, *Ralf Sieckmann v Deutsches Patent– und Markenamt*, C-273/00, 12 December 2002, § 37 and § 51.
48. *See* for further details J. Cabay & F. Gotzen, *Une saveur n'est pas une œuvre : " Cette leçon vaut bien un fromage, sans doute "*, Revue de Droit Commercial Belge, 2019, Vol. 6, pp. 793-811.
49. *See for example* ECJ, *Ralf Sieckmann v Deutsches Patent– und Markenamt, op. cit.*, § 35.
50. CJEU, *SAS Institute Inc. v World Programming Ltd*, C-406/10, 2 May 2012, § 40.
51. CJEU, *SI and Brompton Bicycle Ltd v Chedech / Get2Get*, C-833/18, 11 June 2020, § 32.

matter is necessarily covered by the concept of " work " within the meaning of Directive 2001/29 [52].

The justification is clear, and reflects that of *SAS Institute* :

> The criterion of originality cannot be met by the components of a subject matter which are differentiated only by their technical function (...) [because stating otherwise] would amount to making it possible to monopolise ideas, to the detriment, in particular, of technical progress and industrial development [53].

In other words, not every output can qualify for copyright protection, despite being the result of a free choice (and therefore entailing some " added value "). It is also in line with the justification of the rejection of the same " multiplicity of forms " doctrine in the CJEU case law on the exclusion of technical shapes under design [54] (*DOCERAM* [55]) and trademark [56] laws (*Philipps* [57]). Under those two laws, the CJEU excluded the said doctrine in light of the aim to preserve competition as to the features dictated solely by the technical function of a product, for the sake of " technological innovation " [58]. Only the granting of a patent, subject to stringer requirements and shorter duration, would allow an economic operator to capture the added value of such technical shape on a proprietary basis [59].

As it appears clearly from those cases, the extent of copyright subject matter and requirements for protection is actually defined in consideration of the potential impact on competition, which preservation operates as an underlying rationale. Therefore, the question of the copyrightability of AI-generated or AI-assisted output should certainly be addressed in light of competition concerns. Indeed, competition concerns can arise in relation to both equally.

Frosio recently suggested that " legal incentives for AI-generated creativity should be dealt with care for the potential disruption it may bring to the creative market " [60]. And the DG Competition of the European Commission recently acknowledged that potential competition issues may arise in the field of Generative AI, that hence will be subject to further inquiry [61].

But next to this external approach, an analysis of the inner balance of copyright shall be performed as well. Indeed, in light of the systematic and teleological interpretation of the subject matter and requirements for protection of copyright in *Football Dataco*, *Levola* and *Brompton*, one would certainly understand that the literal interpretation or originality that underpins the " first layers " analysis referred to in previous section comes a bit short. Yet, the analysis we carried out so far is not decisive for answering my main question. To do so, we need to deepen even more our understanding of the originality criterion.

5. Deepest Copyright : The Top Hidden Layers (*Merger Doctrine*)

6 - *Brompton* is of significant importance to answer the question whether the choices made by a human being assisted by an AI can qualify as " free and creative ", and so original, in the event this AI could generate an identical or similar result (through assisting this human being, or any other).

Indeed, the CJEU stated in that case that there can be no originality " where the realisation of a subject matter has been dictated by technical considerations, rules or other constraints which have left no room for creative freedom or room so limited that the idea and its expression become indissociable " [62].

That last part, that was to be found in previous cases [63], borrows from the *merger doctrine* under US copyright law [64]. Following the seminal case *Herbert Rosenthal Jewelry Corp. v. Kalpakian* (9th Cir.) :

> When the " idea " and its " expression " are thus inseparable, copying the " expression " will not be barred, since protecting the " expression " in such circumstances would confer a monopoly of the " idea " upon the copyright owner free of the conditions and limitations imposed by the patent law [65].

And as emphasized in this case, the *merger doctrine* precisely internalizes " the preservation of the balance between competition and protection reflected in the patent and copyright laws " [66]. The competition law rationale envisaged in previous section is blatant.

It is even truer when one considers the further refinements of this doctrine. In particular, as Samuelson suggested, whereas a minority view in the US merger case law would strictly " reserve merger for circumstances in which there is a true unity of expression and ideas (...) the now prevalent, event if not universally accepted, view is that merger can and should be found when there are some, albeit a limited number, of alternative ways to express certain ideas, facts, of functions " [67]. As a matter of fact, only such a broad understanding of the *merger doctrine* would strike the appropriate " balance between competition and protection " which it aims.

This broader conception of the *merger doctrine* is rooted in *Morrissey v. Procter & Gamble Co.* (1st Cir.), in which the Court held that :

> When the uncopyrightable subject matter is very narrow, so that " the topic necessarily requires, " if not only one form of expression, at best only a limited number, to permit copyrighting would mean that a party or parties, by copyrighting a mere handful of forms, could exhaust all possibilities of future use of the substance. In such circumstances it does not seem accurate to say that any particular form of expression comes from the subject matter. However, it is necessary to say that the subject matter would be appropriated by permitting the copyri-

52. *Ibid.*
53. *Ibid.*, § 27.
54. Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs, Art. 8(1) ; Directive 98/71/EC of the European Parliament and of the Council of 13 October 1998 on the legal protection of designs, Art. 7(1).
55. CJEU, *DOCERAM GmbH v CeramTec GmbH*, C-395/16, 8 March 2018, § 29.
56. Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark (codification), Art. 7(1)(e)(ii) ; Directive (EU) 2015/2436 of the European Parliament and of the Council of 16 December 2015 to approximate the laws of the Member States relating to trade marks (recast), Art. 4(1)(e)(ii).
57. *See* originally CJEU, *Koninklijke Philips Electronics NV v Remington Consumer Products Ltd*, C-299/99, 18 June 2002, §§ 81-84. *See also* in particular CJEU, *Lego Juris A/S c. OHMI*, 14 September 2010, C-48/09 P, §§ 53-58.
58. CJEU, *DOCERAM GmbH v CeramTec GmbH, op. cit.*
59. *See* in particular the Opinion of Advocate General Saigmandsgaard Øe delivered on 19 October 2017 in the case *DOCERAM GmbH v CeramTec GmbH.*
60. G. Frosio, *Should We Ban Generative AI, Incentivise it or Make it a Medium for Inclusive Creativity ?, in* E. Bonadio & C. Sganga (eds.), A Research Agenda for EU Copyright Law, Cheltenham, Edward Elgar, 2024 (forthcoming), p. 15.
61. See the recent call for contribution on competition and generative AI : https ://competition-policy.ec.europa.eu/system/files/2024-01/20240109_call-for-contributions_virtual-worlds_and_generative-AI.pdf.
62. CJEU, *SI and Brompton Bicycle Ltd v Chedech / Get2Get, op. cit.*, § 31.
63. CJEU, *Bezpecnostní softwarová asociace – Svaz softwarové ochrany v Ministerstvo kultury*, C-393/09, 22 December 2010, § 49. See also CJEU, *Funke Medien NRW GmbH v Bundesrepublik Deutschland*, 29 July 2019, C-469/17, § 24.
64. See for further details J. Cabay, *L'originalité, entre merger doctrine et multiplicité des formes (ou : Quand la Cour de justice fait l'expérience de l'équilibre sur un vélo pliable)*, Revue de Droit Intellectuel – Ingénieur Conseil, 2020, Vol. 3, pp. 617-650.
65. United States Court of Appeals for the Ninth Circuit, *Herbert Rosenthal Jewelry Corp. v. Kalpakian*, 446 F.2d 738 (9th Cir. 1971), § 742.
66. *Ibid.* ; United States Court of Appeals for the Third Circuit, *Apple Computer, Inc. v. Franklin Computer Corp.*, 714 F.2d 1240 (3rd Cir. 1983), § 1253. Following Pamela Samuelson, " [t]he merger doctrine in U.S. copyright law performs a significant number of important functions. Foremost among them has been preservation of opportunities for meaningful competition ", see P. Samuelson, *Reconceptualizing Copyright's Merger Doctrine*, Journal of the Copyright Society of the USA, 2016, vol. 63, pp. 459-467.
67. *Ibid.*, pp. 425-426.

> ghting of its expression. We cannot recognize copyright as a game of chess in which the public can be checkmated [68].

It is clear from the wording in *Brompton* that the CJEU did adopt the *merger doctrine* under the originality requirement. It is also clear that the Court embraced the broad conception of the doctrine, since its application is not limited to the situation where there is " no room for creative freedom ", but also where the " room [is] so limited " [69].

Furthermore, reading *Brompton* in light of the previous CJEU case law on the exclusion of technical shapes under design and trademark laws comfort the idea of a borrowing from the broad US *merger doctrine*, for the sake of preserving competition. In particular in *DOCERAM*, the CJEU arguably adopted the same view that the 1st Cir. Court of Appeal in *Morrisey v. Procter & Gamble Co.*, holding that :

> If the existence of alternative designs fulfilling the same function as that of the product concerned was sufficient in itself to exclude the application of Article 8(1) of Regulation No 6/2002, a single economic operator would be able to obtain several registrations as a Community design of different possible forms of a product incorporating features of appearance of that product which are exclusively dictated by its technical function. That would enable such an operator to benefit, with regard to such a product, from exclusive protection which is, in practice, equivalent to that offered by a patent, but without being subject to the conditions applicable for obtaining the latter, which would prevent competitors offering a product incorporating certain functional features or limit the possible technical solutions, thereby depriving Article 8(1) of its full effectiveness [70].

Applied to the choices made by a human being, it derives clearly from this case law that they will not qualify as " original " when they are dictated by constraints that have left no or limited room for free and creative expression. To trigger originality, the amount of choices available shall therefore not be one only. Neither can it be two or three, probably. But what about five, ten, hundreds, thousands ? There is no correct (and general) answer as to the threshold, and this must be addressed through a case by case analysis.

What however seems clear is that the capabilities of a human being to explore the amount of choices available is not comparable to the capabilities of an AI. As Degli Esposti, Lagioia and Sartor emphasized :

> Extended automated reuse would affect authors to a greater extent than human reuse, given AI-generation of new creation based on a training set can be unleashed with little marginal costs, and can explore any kind of combinations and variations [71].

As a consequence, if we were to apply the *merger doctrine* rationale to the situation where the work has been created by a human being with the assistance of a Generative AI, arguably the hypothetical threshold would be much higher. Whereas imagining and exploring thousands of possibilities might be elusive for a human being in a lifetime, such an AI might be able to do so in a few minutes. What would then be the limits to the " choices " this AI can make, " with little marginal cost " : thousands, millions, billions ? If we were to leave this AI running " unleashed ", disclosing every generated output, would it exhaust all possibilities for human beings to express the same idea and enjoy copyright protection for their true creation ? If all the outputs (or the most interesting ones) could be appropriated by one single economic operator, claiming copyright protection (which, quite conveniently, is not subject to any registration requirement), what would be the consequences on competition and associated benefits, such as innovation ?

The functioning of GANs might serve exemplifying those concerns. As Goodfellow *et al.* explained, the basic idea underlying its functioning is the following :

> In the proposed adversarial nets framework, the generative model is pitted against an adversary : a discriminative model that learns to determine whether a sample is from the model distribution or the data distribution. The generative model can be thought of as analogous to a team of counterfeiters, trying to produce fake currency and use it without detection, while the discriminative model is analogous to the police, trying to detect the counterfeit currency. Competition in this game drives both teams to improve their methods until the counterfeits are indistinguishable from the genuine articles [72].

In a sense, all the attempts by the generative model to fool the discriminative model trough creating output mimicking the inputs are akin to " choices " made amongst a myriad of possibilities. Depending of the quantity/quality of the data and of the model, if all those attempts were to be appropriated to the benefit of one single operator though an exclusive right, there could be an exclusion of all competition on the same output market. And according to the settled CJEU case law, unless there are present exceptional circumstances (as already mentioned), " the exercise of such right, even if it is the act of an undertaking holding a dominant position, cannot in itself constitute an abuse of a dominant position " [73].

So, rather than entirely leaving the potential competition issues to competition law and the uneasy demonstration of exceptional circumstances, *ex post*, it could be concluded that those " choices ", despite being numerous, cannot give rise to originality, which factors competition concerns into copyright law, *ex ante*. This conclusion is strongly supported by the *merger doctrine* and must be general, whoever makes the choice, being the user of the AI or the AI itself. It is also a conclusion that might not be limited to the sole " *droit d'auteur* " EU law, but could apply to common law copyright, given the US origin of the doctrine. It seems however that so far, the argument was not brought in the US literature [74]. Actually, as far as I know, the *merger doctrine* argument was never discussed in the literature on AI and copyright.

So, turning to my initial question, I posit that in the context of AI-assisted production, it is not much a matter of the choices made by the human being, but rather of the " choices " that can be made by the AI. If the author assisted by a Generative AI has been making choices which could have been equally done by this AI, then the result cannot be deemed the " author's own intellectual creation ", bearing his " personal touch ". Such a conclusion is not based on a plain reading of the originality requirement, but is supported by its contextual and teleological interpretation, duly taking into account the competition underlying rationale.

68. United States Court of Appeals for the First Circuit, *Morrissey v. Procter & Gamble Co.*, 379 F.2d 675 (1st Cir. 1967), §§ 678-679.
69. CJEU, *SI and Brompton Bicycle Ltd v Chedech / Get2Get, op. cit.*, § 31.
70. CJEU, *DOCERAM GmbH v CeramTec GmbH, op. cit.*, § 30.
71. M. Degli Esposti *et al., The use of copyrighted works by AI systems : Art works in the data mill*, European Journal of Risk Regulation, 2020, Vol. 11, p. 67.
72. I. Goodfellow *et al., op. cit.*, p. 1.
73. See for example CJEU, *Huawei Technologies Co. Ltd v ZTE Corp. and ZTE Deutschland GmbH*, C-170/13, 16 July 2015, § 46.
74. The *merger doctrine* is not mentioned in the US national report to the questionnaire on *Copyright in artificially generated works* submitted to the AIPPI 2019 World Congress in London, nor in the US national report to the questionnaire on *Copyright, Related Rights and Artificial Intelligence*, submitted to the ALAI 2023 Congress in Paris.

6. Conclusion : Parrots and Copyright

7 - One basic assumption of mine is that the main reason why we started discussing copyright protection for Generative AI lies in the similarities between its production and works created by human beings [75].

It is true that it is sometimes hard to distinguish amongst the results brought by a human being and an AI. Yet, we should not overlook that despite those similarities, the underlying processes are completely different which, in turn, questions the relevance of those similarities and the conclusion we can draw from there.

In a paper discussing actual and potential risks of developing ever larger language models, Bender, Gebru, *et al*. suggested that some of the value we associate with the output (here the generated text) is biased " by our own linguistic competence and our predisposition to interpret communicative acts as conveying coherent meaning and intent, whether or not they do ". Such value (coherence here), they say, is " in the eye of the beholder " [76]. To raise awareness on this aspect, they coined the " stochastic parrot " metaphor to remind us what we are actually talking about :

> Contrary to how it may seem when we observe its output, an LM [Language Model] is a system for haphazardly stitching together sequences of linguistic forms it has observed in its vast training data, according to probabilistic information about how they combine, but without any reference to meaning : a stochastic parrot [77].

Confronted with such output, we should avoid parroting traditional and superficial copyright doctrine and wording to simply concluding that, provided there was so room for human choices, the way to get to that result does not make a change. It does make a change. Actually, it changes everything.

As suggested by Bender, Gebru, *et al.*, scaling up with language models is incurring new kind of risks of harmful behavior [78]. And Gugli, Henandez, Lovitt *et al*. emphasized that it can be difficult to study those risks on smaller models [79]. The same goes with copyright analysis. Copyright is anthropocentric, and its design is entirely based on the capabilities of a human being [80]. Applied equally to works created by human beings and generated or assisted by AI, it will not produce the same (possibly desirable) outcomes, because of the change of scale.

To put this idea in simple words and make my point clear, we can compare creation to water. Water does not behave the same way depending on the temperature. Below 0 °C, it is solid. Above 100 °C, it is gas. Within this range, it is liquid. If I want to encapsulate water at these different temperatures, I won't use the same container. It is true that the development of technologies since the early printing had already significantly " raised the temperature " (with the radio, television, satellite, internet, etc.). But creation remained " solid " or " liquid " and could be captured with the same type of copyright containers we used for decades. With the advent of Generative AI, creation became like gas and behaves a completely different way. The " copyright bottle " is certainly not appropriate to fully get it.

In my view, prompting to generate an output and tweaking it to make it resembles a work of art can by no means be considered equivalent to taking a pencil to write down a novel based on one's life experience, a chisel to carve out of marble an idealized representation of mankind, or sheet music paper to compose a symphony for posterity. Neither can it be compared to creating the so-called " small changes ", such as drafting contractual terms and conditions [81], designing a handbag [82], or playing a catchy melody on simple chords [83]. It is because it does not take the same amount of time, effort, or investment, nor supposes the skills, qualification, or education, from the human being originating the alleged work.

This is why we must distinguish.

The " one size fits all " approach of copyright does not discriminate against amongst human creations based on " quality ", " merit ", " aesthetics " or " purpose " [84], and accordingly protects equally the masterpieces and the " small changes ".

It does not imply however that we cannot distinguish between genuine human works, purely AI-generated outputs, and human productions assisted by an AI. As the CJEU stated in *Cofemel* :

> It is apparent from the wording of [Article 17(2) of the Charter of Fundamental Rights of the European Union] that subject matter constituting intellectual property qualifies for protection under EU law. However, it does not follow that such subject matter or categories of subject matter must all qualify for the same protection [85].

We must then consider the underlying technology, accept that it is not neutral and discriminate against accordingly to give the AI assisted productions another status. Concluding otherwise would run counter to the aim of the " technological neutrality " which, according to the CJEU, " requires that the interpretation of the provisions at issue does not hold back innovation and technological progress " [86].

Hence, even the " one size fits all " and " technological neutrality " principles that underpin what I referred to as the " result " approach, and that is prevalent in the literature, suggest that such approach is not appropriate. This is why I recommend adopting the " process " approach.

Following this approach, the underlying competition rationale of copyright law and its concrete inner application through the broad *merger doctrine* adopted by the CJEU seriously pleads against the copyrightability of such productions. It is also preferable because it goes beyond a literal interpretation of the originality requirement, and equally considers the contextual and teleological methods.

In my opinion, this is a deep argument that we should carefully consider. Certainly, it offers perspective for further research. We can always go deeper.■

75. See for further details on my opinion, J. Cabay, *Droit d'auteur et intelligence artificielle : comparaison n'est pas raison*, *op. cit.*, pp. 307-325 ; J. Cabay, *Mort ou résurrection de l'auteur ? A propos de l'intelligence artificielle et de la propriété intellectuelle*, *op. cit.*, pp. 179-190.
76. E. M. Bender *et al.*, *On the Dangers of Stochastic Parrots : Can Language Models Be Too Big ?*, *in* Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (FAccT " 21), Association for Computing Machinery, New York (NY, USA), 2021, p. 616, [https ://doi.org/10.1145/3442188.3445922].
77. *Ibid*., p. 617.
78. *Ibid*., p. 612.
79. D. Ganguli *et al., Predictability and Surprise in Large Generative Models, in* Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency (FAccT " 22), Association for Computing Machinery, New York (NY, USA), 2022, p. 1742 [https ://doi.org/10.1145/3531146.3533229].
80. As I suggested elsewhere, *see J. Cabay, Droit d'auteur et intelligence artificielle : comparaison n'est pas raison, op. cit.*, p. 315.
81. *See* for an example of copyright protection for such work in Belgium : Antwerp Court of Appeal, *Auteurs & Media*, 5 February 2007, p. 352.
82. *See* for an example of copyright protection for such work in Belgium : Brussels Court of Appeal, *Revue de droit intellectuel – Ingénieur conseil*, 26 July 2018, p. 488, *Intellectuele Rechten – Droits intellectuels*, 2019, p. 211.
83. *See* for an example of copyright protection for such work in Belgium : Brussels Court of Appeal, 18 December 2008, *Auteurs & Media*, 2010, p. 22.
84. *See* in general S. Van Gompel & E. Lavik, *Quality, merit, aesthetics and purpose : An inquiry into EU copyright law's eschewal of other criteria than originality*, Revue international du droit d'auteur, 2013, Vol. 236, pp. 100-295.
85. CJEU, *Cofemel – Sociedade de Vestuário SA v G-Star Raw CV*, *op. cit.*, § 38.
86. CJEU, E*utelsat SA v Autorité de régulation des communications électroniques et des postes (ARCEP) and Inmarsat Ventures SE*, C-515/19, 15 April 2021, § 48. *See* also the Opinion of Advocate General Hogan delivered on 23 September 2021, A*ustro-Mechana Gesellschaft zur Wahrnehmung mechanisch-musikalischer Urheberrechte Gesellschaft mbH v Strato*, *op. cit.*, footnote 13.

13 Le modèle européen de régulation de l'intelligence artificielle

Frédérique BERROD,
Chaire Jean Monnet « Narratifs européens de la frontière »,
Professeure à Sciences Po Strasbourg,
Membre du CEIE EA 7307,
Membre du centre d'excellence franco-allemand Jean Monnet

1 - L'intelligence artificielle (IA) déclenche des passions dans le débat citoyen autant que dans les cénacles de l'écriture des lois. Un système d'intelligence artificielle est décrit comme un « système algorithmique ou toute combinaison de tels systèmes utilisant des méthodes de calcul dérivées de statistiques ou d'autres techniques mathématiques et qui génère du texte, du son, une image ou un autre contenu ou soit assiste, soit remplace la prise de décision humaine » par le Conseil de l'Europe [1]. Cette définition cristallise les principaux enjeux. L'IA suppose des données et des systèmes puissants de calcul, ce qui renvoie à l'application de textes existants dans l'Union européenne (UE) pour protéger les données personnelles [2] ou la mise à disposition de données publiques [3], les assurer contre les cyberattaques [4], éviter leur capture par des plateformes dites cruciales [5]. Les IA produisent du texte, du son ou de l'image, ce qui suppose dans l'UE une responsabilité particulière pour ne pas diffuser par exemple des *fake news* ou des images pernicieuses à destination des mineurs [6]. Enfin, l'IA peut assister ou remplacer la décision humaine, ce qui pose la question de la place de l'humain et de sa capacité à ne pas être gouverné par la machine.

Pour comprendre les enjeux de la régulation de l'IA, il faut rappeler les bénéfices et les risques de cette mutation technologique ; les communications de 2018 [7] et 2021 [8] ont ainsi été construites sur ces deux considérations. La crise de la COVID a montré comment l'IA était à la fois omniprésente et nécessaire pour mieux soigner, un peu à l'image de la fée électricité ou des merveilleuses machines du dieu Hephaïstos [9]. L'irruption des IA génératives entraînées sur la base de données (comme ChatGPT), appelées aussi modèles fondationnels, a remis au centre des débats les risques de cette technologie pour l'humain, comme dans les romans de science-fiction de Asimov ou comme Ada [10], machine programmée pour écrire des romans à l'eau de rose qui échappe à ses concepteurs et risque de supplanter l'humanité par le règne de la machine.

C'est sur cette trame technique, sociale et culturelle que se dessine une réglementation européenne sur la chose, première « loi » au monde qui ambitionne de protéger l'humain par la norme. Le texte proposé par la Commission européenne en 2021 [11] a abouti à un accord politique entre le Parlement et le Conseil de l'UE après un trilogue de 37 heures début décembre 2023 [12]. Cet accord ouvre encore des débats sur les modalités techniques et le texte ne sera stabilisé définitivement que début 2024. Malgré cet accord volontiers décrit comme « historique » [13], des critiques demeurent, dont celle du Président Emmanuel Macron qui déclarait : « cette réglementation européenne fait qu'on est le premier endroit au monde où sur les modèles dits fondationnels d'IA [14], on va beaucoup plus réguler que les autres. Je ne pense pas que ce soit une bonne idée », le 11 décembre à Toulouse, lors d'un point d'étape du plan France 2030 [15].

Du point de vue juridique, cette tension est celle entre innovation et régulation, entre laisser-faire normatif et obligation juridique, entre autorégulation et obligations opposables aux entreprises et aux individus. Dans une note stratégique produite par l'Espagne au début de sa présidence du Conseil de l'UE, cette tension est exprimée entre l'innovation technologique et la protection des droits fondamentaux. Elle englobe aussi la protection environnementale. Elle suppose également de ne pas laisser pour compte les citoyens, parce qu'elle implique une attention au changement de contenu

1. Article 3 du projet de convention-cadre sur l'IA du Conseil de l'Europe dans sa version consolidée en juillet 2023. Les informations sont disponibles sur : Conseil de l'Europe, « Conseil de l'Europe et intelligence artificielle » [www.coe.int/fr/web/artificial-intelligence].
2. Règlement Général sur la Protection des Données personnelles (UE) 2016/679 du 27 avril 2016, JOUE 4 mai 2016, L 119, p. 1.
3. Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données), JOUE du 3 juin 2022, L 152, p. 1.
4. Règlement (UE) 2019/881 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, JOUE du 17 avril 2019, L 151, p. 15.
5. Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique dit Digital Market Act, JOUE du 12 octobre 2022, p. 1.
6. Règlement (UE) 2022/2065 relatif à un marché unique des services numériques dit DSA, JOUE du 27 octobre 2022 L 277, p. 1.
7. Communication de la Commission européenne : « L'intelligence artificielle pour l'Europe », 25 avril 2018, COM/2018/237 final.
8. Communication de la Commission européenne : « Favoriser une approche européenne en matière d'intelligence artificielle », 21 avril 2021, COM(2021)205 final.
9. A. Marcinkowski et J. Wilgaux, « Automates et créatures artificielles d'Héphaïstos : entre science et fiction », *Techniques & Culture*, 2004, 43-44.
10. Roman de A. Bello, *Ada*, Gallimard, 2018.
11. Proposition de règlement de la Commission européenne du 21 avril 2021, COM(2021)206 final.
12. Les informations sur ce dernier trilogue sont celles de l'Agence Europe du 11 décembre 2023. Le texte final ne sera disponible qu'après la négociation sur les détails techniques.
13. Pour reprendre les termes du commissaire Thierry Breton sur X (anciennement Twitter).
14. Jusqu'à récemment, les systèmes d'intelligence artificielle (IA) étaient des outils spécialisés. Il était donc courant d'entraîner un modèle d'AA pour une application ou un cas d'utilisation spécifique. La notion de modèle de fondation, aussi appelé modèle de base, a intégré notre jargon lorsque des spécialistes ont observé les deux tendances suivantes dans le domaine de l'apprentissage automatique : un petit nombre d'architectures d'apprentissage profond étaient utilisées afin d'obtenir des résultats pour des tâches très diverses ; et de nouveaux concepts peuvent émerger à partir d'un modèle d'intelligence artificielle (IA), qui n'étaient pas prévus à l'origine dans l'entraînement de ce dernier.
Red Hat, « IA : un modèle de foundation qu'est-ce que c'est ? », 14 septembre 2023 [https ://www.redhat.com/fr/topics/cloud-computing/foundation-models].
15. Voir sa déclaration sur « 'Ce n'est pas une bonne idée' : Macron réservé sur le fait que l'Europe encadre l'IA 'plus que les autres' », *Le Parisien*, 11 décembre 2023 (https ://www.leparisien.fr/high-tech/ce-nest-pas-une-bonne-idee-macron-reserve-sur-le-fait-que-leurope-encadre-lia-plus-que-les-autres-11-12-2023-BCSMXSPSYBBZNFMNJVITDWVMWU.php).

des emplois ou l'acquisition de nouvelles compétences tout au long de la vie [16]. Elle est exprimée un peu différemment sous forme de trilemme par Milo Rignell : « Comment rester à la pointe d'une technologie hautement stratégique, et en même temps fixer des règles de gouvernance qui régiront ces systèmes dans le monde, et en même temps éviter de développer des systèmes imprévisibles qui, en cas de défaillance, pourraient poser un réel risque systémique pour son propre pays, voire pour le monde ? » [17].

L'auteur rappelle que, sur le plan chronologique, le monde et les États ont d'abord lancé une course technologique. La Commission rappelle les atouts de l'UE de ce point de vue, dont sa puissance de calcul [18]. La course qui se joue depuis 2021 est celle de la régulation et de la gouvernance de l'IA, tant au niveau mondial, que national ou européen. C'est sur ce plan que se situera notre analyse, pour évaluer comment l'Union défend un modèle européen de régulation de l'IA.

1. Une régulation fondée sur la place de l'humain

2 - L'idée de réguler l'intelligence artificielle est née en Europe de la volonté de protéger l'humain et ses droits, face à une machine qui pourrait devenir « décidante ». Le Conseil de l'Europe a été pionnier de cette approche, conscient aussi des abus possibles de l'IA pour manipuler la démocratie et l'État de droit. Il négocie aujourd'hui une convention-cadre qui serait ouverte aux pays tiers. Dans la version consolidée en juillet 2023, l'objet de la convention est d'énoncer « des principes et des obligations visant à garantir que la conception, le développement, l'utilisation et la mise hors service des systèmes d'intelligence artificielle sont pleinement compatibles avec le respect de la dignité humaine et de l'autonomie individuelle, les droits de l'homme et les libertés fondamentales, le fonctionnement de la démocratie et le respect de l'État de droit ».

Les techniques juridiques garantissant l'éthique de l'IA sont la transparence en fonction du risque encouru et la responsabilisation (comprenant à la fois l'*accountability* et la responsabilité juridique) tout au long de la chaîne menant de la conception de l'IA à sa mise à disposition pour le citoyen. Les parties à la future convention devront aussi garantir l'application des principes d'égalité, de non-discrimination et de vie privée. De manière spécifique pour l'IA, le projet d'article 11 vise la robustesse, la sûreté et la sécurité des données qui nourrissent l'IA tout au long de son cycle de vie, ce qui vise la « conception, le développement, l'utilisation et la mise hors service des systèmes d'intelligence artificielle ».

Le projet d'article 12 permet de comprendre pourquoi la régulation de l'IA doit aller au-delà du respect de ces seuls principes. L'équilibre, à ce stade, entre innovation et régulation est exprimé de cette manière : « Lorsque des systèmes d'intelligence artificielle sont testés à des fins de recherche et d'innovation, chaque Partie met en place un environnement réglementaire contrôlé pour tester les systèmes d'intelligence artificielle sous la supervision de ses autorités compétentes, en vue d'éviter tout impact négatif sur les droits de l'homme, la démocratie et l'État de droit dans le cadre du test ». La régulation est donc envisagée comme un élément d'une innovation éthique parce que conçue dans le respect des valeurs européennes. Elle induit logiquement une approche par le risque, pour que les parties soient mises en capacité d'« identifier, évaluer, prévenir et atténuer les risques et les impacts sur les droits de l'homme, la démocratie et l'État de droit découlant de la conception, du développement, de l'utilisation et de la mise hors service des systèmes d'intelligence artificielle » (article 15).

L'UE reprend ce même narratif, dans une logique pourtant plus économique. Depuis sa communication d'avril 2018, elle mise sur l'élaboration d'un cadre pour une IA de confiance. La Commission estime déjà à cette époque que « l'UE doit dès lors veiller à ce que l'IA soit développée et appliquée dans un cadre approprié qui favorise l'innovation et respecte les valeurs et les droits fondamentaux de l'Union ainsi que les principes éthiques tels que la responsabilité et la transparence. L'UE est également bien placée pour diriger ce débat sur la scène mondiale ». Elle appuie ses travaux préparatoires du règlement sur l'IA sur un groupe d'experts, composé de 52 membres et qui fait connaître ses lignes directrices au printemps 2019. Au début de l'année 2020, à la veille de la pandémie, la Commission avait publié son Livre Blanc pour une approche européenne en matière d'IA basée sur l'excellence et la confiance [19].

La proposition de règlement d'avril 2021 s'appuie sur ce corpus éthique pour élaborer un cadrage fondé sur le risque. Cette proposition va plus loin que le projet du Conseil de l'Europe en ce qu'elle impose des obligations directement applicables dans l'ensemble des États membres, qui varient en fonction de catégories de risques prédéfinies dans le règlement. Le principe est l'évaluation des systèmes d'IA différenciés en fonction de leur niveau de risque, pour les fournisseurs et les utilisateurs.

La négociation s'est tendue depuis la fin de l'été 2023 avec l'ambition de construire des champions européens de ces IA génératives ou fondationnelles. Certains États, dont la France, l'Italie et l'Allemagne, et des lobbies d'entreprises européennes spécialisées dans ces développements de l'IA, ont plaidé pour un contrôle *a minima*, par le biais de codes de conduite. Ces codes sont, dans l'accord politique de décembre 2023, réduits à de l'appui pour les fournisseurs de systèmes et modèles représentant des risques systémiques afin qu'ils puissent se conformer aux futures règles. Derrière les revendications françaises, italiennes et allemandes sont reposées les questions de l'opportunité de la réglementation par l'UE pour l'innovation. Le commissaire Breton, qui a beaucoup poussé pour cette réglementation qu'il considère comme un succès de son mandat, répond à ces arguments que les IA doivent répondre à un modèle européen si elles veulent accéder au plus grand marché du monde qu'est le marché intérieur [20].

2. Un modèle européen leader de la régulation mondiale

3 - Dans l'idée de Thierry Breton, la régulation de l'IA est une question de protection des valeurs de l'UE et des droits de la personne humaine qui doit être le fondement de l'IA prétendant à pouvoir accéder au marché intérieur. Ce marché numérique est en effet unifié en un écosystème de règles sur la protection des données personnelles et la libre circulation des données non personnelles. L'important règlement sur la gouvernance des données, entré en application en septembre 2023, constitue un avantage compétitif pour nourrir des IA à partir des données publiques, largement ouvertes et réutilisables. Enfin, le Digital Markets Act (DMA) [21] et le Digital Services Act (DSA) commencent à produire leurs effets, en imposant déjà un modèle européen de

16. Cette dimension sociale est soulignée dès la communication de 2018, *ibid.*.
17. M. Rignell, « IA, l'ambivalence entre course technologique et gouvernance mondiale », Institut Montaigne, 20 juillet 2023 (https ://www.institutmontaigne.org/expressions/ia-lambivalence-entre-course-technologique-et-gouvernance-mondiale).
18. L'entreprise commune EuroHPC, mettant en réseaux des supercalculateurs permet d'installer la plus grosse puissance de calcul au monde.
19. Livre Blanc de la Commission européenne : « Intelligence artificielle – Une approche européenne basée sur l'excellence et la confiance », 19 février 2020, COM(2020)65 final.
20. « Intelligence artificielle : 'les Gafam et la startup Mistral ne défendent pas l'intérêt général' (Thierry Breton) », *La Tribune*, 24 novembre 2023 (www.latribune.fr/technos-medias/informatique/intelligence-artificielle-les-gafam-et-la-startup-mistral-ne-defendent-pas-l-interet-general-thierry-breton-984046.html).
21. F. Berrod, « Introduction au DMA : un esprit pionnier de la régulation des plateformes numériques », *Dalloz IP/IT : droit de la propriété intellectuelle et du numérique*, N° 5, 2023, p. 266.

régulation des grandes plateformes. Cet écosystème plaide pour une régulation de l'IA, en complément logique des autres textes existants. Le temps n'est donc pas à ce titre à la pause réglementaire.

Le modèle de régulation à l'européenne repose sur l'excellence technologique de l'UE et sa capacité à fédérer la recherche universitaire, les entreprises et des investissements substantiels dans ce secteur. L'UE a donc intérêt à poursuivre le développement de ses investissements normatifs par la régulation de l'IA. C'est à la fois la protection de ses valeurs et de son modèle économique qui sont en jeu. Accéder au marché intérieur numérique suppose donc de se mettre au niveau des standards de l'UE, ce qui conditionne ensuite l'innovation. Un dernier argument fait pencher dans le sens de la régulation : la régulation de l'IA permet à l'UE de protéger son autonomie stratégique ou sa souveraineté. Elle protège par ses standards normatifs son innovation technologique, sur la base de données massives, traitables par une puissance de calcul inégalée dans le monde. Cet ensemble permet de renforcer l'Europe en tant que puissance dans la géopolitique mondiale de l'IA.

Cela explique le choix de déterminer dans le règlement sur l'IA quatre catégories de risque, avec des obligations correspondantes. Pour les risques inacceptables parce qu'ils sont considérés comme des menaces pour les personnes, la sécurité ou les moyens de subsistance, le principe du règlement est l'interdiction pure et simple. Sont visées les manipulations cognitivo-comportementales de personnes ou de groupes vulnérables (par exemple jouets activés par la voix qui encouragent les comportements dangereux chez les enfants), les pratiques de score social et les systèmes d'identification biométrique en temps réel et à distance (reconnaissance faciale). Pour les risques élevés, à savoir les IA qui ont un impact négatif sur la sécurité (telles les infrastructures critiques) ou les droits fondamentaux (médecine assistée par robot, logiciel de tri de CV ou d'évaluation de la fiabilité des preuves...), le principe est l'évaluation de la conformité au règlement avant leur mise sur le marché et tout au long de leur cycle de vie et lors de changements substantiels de la technologie. Cette évaluation par un organisme notifié extérieur au producteur de l'IA ressemble au niveau d'exigences des dispositifs médicaux les plus dangereux pour la santé, qui n'ont accès au marché qu'après examen de la conformité par des organismes notifiés [22]. Les systèmes d'IA relevant de huit domaines devront être enregistrés dans une base de données de l'UE (identification biométrique, éducation et formation professionnelle, emploi, migration, forces de l'ordre...). L'évaluation préalable a pour objectif de faire baisser les risques (en incorporant aussi des contrôles par l'humain), de garantir une haute qualité des ensembles de données utilisés pour l'IA (données qui doivent présenter un haut niveau de robustesse, de sécurité et de prévision), enregistrer les activités, tracer les résultats et informer les consommateurs sur le niveau de risque. Les IA de risque faible ne sont soumises qu'à des obligations de transparence. Les consommateurs doivent par exemple savoir qu'ils conversent avec un robot afin de leur garantir une prise de recul suffisante. L'IA à risque nul peut circuler librement sans obligations préalables à la commercialisation.

Toute la question a été de savoir où classer les IA génératives dans cette taxinomie. Le risque semblait faible jusqu'à l'arrivée de Chat GPT à l'automne 2022 (pour sa version gratuite grand public). Finalement, elles ont été classées comme IA de risque faible mais avec une obligation d'information des consommateurs, la publication des résumés des données protégées par le droit d'auteur et surtout la preuve que la conception empêche l'IA de générer du contenu illégal. En outre, les systèmes d'IA et les modèles sur lesquels ils sont basés représentant des risques systémiques devraient quant à eux appliquer des règles plus strictes, notamment l'évaluation des modèles, l'évaluation et l'atténuation des risques systémiques ou encore la réalisation de tests contradictoires. Ces IA sont mises sous surveillance si elles représentent un risque « systémique » trop importants pour l'humain. Il est vrai que les performances des IA génératives ont remis sur le devant de la scène leurs risques dans le monde de l'éducation, du journalisme, de la démocratie et, au fond, de la place de l'humain. Le projet de règlement intègre l'idée qu'à des grands pouvoirs correspondent de grandes responsabilités. Cette approche fonde également le DSA, ce qui a déjà mené la Commission européenne à distinguer 22 plateformes qualifiées de systémiques ; leur taille induit un risque systémique justifiant leur mise sous surveillance pour qu'ils aient accès au marché intérieur. C'est ce qui explique l'ouverture d'enquêtes préliminaires et d'une première enquête formelle contre le réseau X pour diffusion de contenus illégaux et désinformation [23]. Les systèmes d'IA à risque systémique devront aussi faire la preuve de leurs efforts pour assurer une IA de confiance. Des rapports devraient donc être rendus à la Commission pour les incidents graves et des mesures devraient aussi être prises pour assurer la cyber sécurité. En outre, des comptes-rendus quant à l'efficacité énergétique des modèles devraient être réalisés ; la consommation énergétique de l'IA s'est invitée dans le débat, particulièrement suite à la crise énergétique découlant de la guerre en Ukraine, parce que ces grands modèles d'IA supposent une prise électrique...

3. Un difficile équilibre entre régulation et innovation

4 - La tension entre innovation et régulation redevient importante à l'automne 2023, quand la proposition de règlement entre dans les dernières phases de trilogue. Il faudra 37 heures, dans la nuit du 8 au 9 décembre 2023, pour trouver un accord politique sur le texte. Les États comme la France, qui critiquent l'équilibre retenu, misent encore sur la mise au point des détails techniques, après l'accord politique et jusqu'à janvier, après le vote du texte par le Parlement européen et le Conseil de l'UE.

Les positions du Parlement européen ont été reprises dans le compromis pour assurer une protection maximale des droits de personne humaine, y compris par l'introduction de la prise en compte des risques systémiques découlant de la puissance de calcul des systèmes et modèles. Les États ont en revanche réussi à imposer leur point de vue sur les questions de sécurité, en obtenant de nombreuses exemptions des obligations des IA dans le domaine militaire, pour la lutte contre le terrorisme ou des crimes graves. L'identification en temps réel par l'IA est par exemple possible pour localiser les victimes potentielles, mais après autorisation préalable et évaluation du risque sur les droits fondamentaux. L'accord comprend aussi une procédure d'urgence afin de permettre aux services répressifs de déployer en cas d'urgence un outil d'IA à haut risque qui n'a pas passé la procédure d'évaluation de la conformité. Le texte préserve la liberté totale de la recherche et développement et les modèles dits ouverts.

Le trilogue permet de préciser également la gouvernance de cette régulation et les sanctions en cas de violation des obligations posées par la proposition de règlement. Cela vise à assurer une approche normative basée sur la science et suffisamment ductile, de façon à ne pas brider abusivement l'innovation. Dans cette optique, un Office européen de l'IA est créé pour superviser la mise en œuvre du texte et contribuer à l'élaboration des normes et des pratiques d'essai, ainsi que l'élaboration des codes de pratique pour les modèles de fondation. Il est composé de représentants des États membres et est assisté par un groupe d'experts indépendants,

22. Règlement (UE) 2017/745 relatif aux dispositifs médicaux, JOUE du 5 avril 2017, L 117, p. 1.

23. Voir pour une première analyse C. Félix, « La commission européenne déclenche une 'enquête formelle' contre le réseau social X, une procédure inédite », *France Inter*, 18 décembre 2023 (www.radiofrance.fr/franceinter/la-commission-europeenne-declenche-une-enquete-formelle-contre-le-reseau-social-x-une-procedure-inedite-1162802).

qui l'aidera à concevoir les normes et repérer l'émergence de modèles de fondation à fort impact.

Comme pour le DMA et le DSA, l'effectivité du texte est assurée par des sanctions, qui s'élèveraient au maximum à 35 millions d'euros (ou 7% du chiffre d'affaires annuel mondial de l'entreprise) pour les violations des applications d'IA interdites. Le montant de l'amende est dégressif pour les autres violations, se montant à 15 millions d'euros (3% du chiffre d'affaires mondial annuel). Si les informations fournies en application du futur règlement sur l'IA sont inexactes, le montant de l'amende pourrait s'élever à 7,5 millions d'euros (1,5% du chiffre d'affaires). Les individus peuvent aussi déposer plainte auprès de l'autorité de surveillance du marché dans les États membres pour assurer le respect du texte.

Le texte est soumis à une entrée en vigueur différée, soit six mois après la publication au JOUE, ce qui est peu habituel [24] et démontre la volonté de préparer les administrations et les entreprises à ce cadrage. Comme pour beaucoup de règlements, l'unification des règles est concédée contre une mise en application échelonnée dans le temps des obligations : six mois après l'entrée en vigueur, les règles relatives aux modèles de fondation et aux organismes d'évaluation de la conformité seront effectives, et un an est encore prévu avant que le texte doive être entièrement appliqué. Cette mise en œuvre progressive est aussi une concession à la France, l'Italie et l'Allemagne, pour permettre l'innovation tout en garantissant un cadre unifié d'obligations en Europe.

Restera à évaluer combien la mise au point des détails techniques font bouger en 2024 la version finale du règlement. Si ce dernier permet d'imposer un modèle européen de régulation dans la course mondiale à la norme, il pose aussi la question du poids de celle-ci pour l'économie européenne et de manière ultime de sa compétitivité. Ce thème sera à n'en pas douter un sujet des prochaines élections au Parlement européen.■

24. Le délai de mise en œuvre est presque systématique depuis quelques années mais les règlements entrent en principe en vigueur du jour de leur publication au JOUE.

14 Unveiling the Digital Side of Journalism: Exploring the European Media Freedom Act's Opportunities and Challenges

Oreste POLLICINO,

Professor of Constitutional Law and Media Law at Bocconi University, Senior Emile Noele Global Fellow at the New York University

Federica PAOLUCCI,

Ph.D. Candidate at Bocconi University

Introduction

1 - Journalists today face continuous challenges amid the digital landscape. The pressures extend beyond the ubiquitous influence of social media on information dissemination ; they also encompass the integration of cutting-edge technologies like Artificial Intelligence (AI) systems into the journalist profession. With respect to the first aspect, it is no news that social media play a central role in the curation of content, design and control exposure of political and democratic discourse, exercising a *de facto* editorial role over the public reaching of a certain new or opinion. Since the Israeli-Palestinian conflict spread in 2023, social media, especially platforms such as TikTok, have played a significant role in reporting and covering the escalation of violence. As of 10 October 2023, the hashtag #Palestine has some 27.8 billion views, and the hashtag #Israel has 23 billion on TikTok [1]. The decision to make a piece of content go viral ultimately rests with the service provider, exercising editorial control over the content delivered to user groups [2]. This aspect might trigger the protection of freedom of expression and media pluralism [3] – which is a precondition for enjoying most democratic freedoms, such as the electoral vote [4] – and by orienting editorial choices and news coverage.

Concerning the second aspect, namely the integration of technological tools, such as AI, in the journalist job, this is something that certainly eases the creation and the editing of a piece of news [5] ; it is, however, to be handled with care, even though many newsrooms have already started to approach generative AI and integration in the editorial job [6]. Moreover, the Council of Europe has recently published practical guidelines aimed at guiding journalists in the implementation of AI systems [7]. This includes the duty to use AI systems in ways that are compatible with human rights and public values, promote society's interests in being informed and function the media as a forum for public discourse [8].

The novelties summarised here show how the pervasiveness of technology constantly triggers the practice of journalism in the digital environment and raises serious questions about the relationship between journalists, public information, and digital media, moving towards a quadrangular formation of digital powers [9]. One of the issues at stake is, in fact, how to ensure an adequate balance between opposing interests : freedom of expression and information, independence and market business, which, in the European context, translates into control of the internal market.

Hence, in this context, a new geometry of digital powers is emerging, and it can be described as involving a renovated space – the digital one – triggered by transnational stances, highly influenced by the value-based approach of the European matrix. The last relevant aspect refers to the potentiation of procedural remedies that can counter the aforementioned balance between different interests.

Despite the identified drawbacks, private actors have already demonstrated that they are capable of enforcing regulation effectively. This results in co-regulatory attempts, such as the Strengthened Code of Practice on Disinformation [10], where critical providers agreed to sign a code of conduct on disinformation. On the other hand, journalists are one of the categories tangentially interested

1. *Oreste Pollicino is a Professor of Constitutional Law and Media Law at Bocconi University. He is a Senior Emile Noele Global Fellow at the New York University.
   ** Federica Paolucci is Ph.D. Candidate at Bocconi University.
   Taylor Lorenz, *Why TikTok videos on the Israel-Hamas war have drawn billions of views*, Washington Post, 10 October 2023.
2. The Oversight Board, the independent organisation that reviews Meta's decisions on content removal, decides on two cases of videos initially removed by Meta and then reinstated with a warning screen. See the OB press release (2023) <https ://www.oversightboard.com/news/318968857762747-oversight-board-announces-new-cases-on-israel-hamas-conflict-for-expedited-review/>.
3. Maria Luisa Stasi and Pier Luigi Parcu, *Disinformation and misinformation : the EU response*, in E. Brogi, P. Parcu (eds.), Research Handbook on EU Media Law and Policy, Edward Elgar Publishing (2021), pp. 407-426.
4. Roberto Mastroianni, *Freedom of pluralism of the media : an European value waiting to be discovered ?*, Rivista di Diritto dei Media, 1 (2022), pp. 100-110.
5. As in the case of Newsquest, where the paper created an in-house AI tool which is trained by professional journalists, and which is then edited and tweaked, if necessary, by a news editor, as reported by Alexandra Topping, *How one of the world's oldest newspapers is using AI to reinvent journalism*, The Guardian, 28 December 2023.
6. David Caswell, *AI and journalism : What's next ?*, Reuter Institute (2023).
7. Council of Europe (CoE), *Guidelines on the responsible implementation of artificial intelligence systems in journalism*, Adopted by the Steering Committee on Media and Information Society (CDMSI) on 30 November 2023, CDMSI(2023)014.
8. The guidelines provide the journalists with concrete and hands-on perspectives on procurement and using AI systems in their jobs. It is interesting to observe that, in line with the guidelines already shared by the CAI (Committee on Artificial Intelligence), news organisations should have procedures in place to recognise and, where feasible, assess and mitigate risks that result from the way journalistic AI systems are implemented, including any risks to the rights of third parties (such as data protection, copyright, and non-discrimination) or dangers to the environment, internal and external workers' rights or rights of subjects, copyright holders and affected communities. Risk assessment procedures should include ways to integrate the experiences and perspectives of affected individuals and communities. It should be recognised that procuring AI systems can carry risks associated with not completely controlling data, methods and processes.
9. Oreste Pollicino, *Potere digitale*, in M. Cartabia and M. Ruotolo (eds.), Enciclopedia del Diritto Potere e Costituzione, Giuffrè (2023), pp. 409-446 ; Oreste Pollicino, *The quadrangular shape of the geometry of digital power (s) and the move towards a procedural digital constitutionalism*, European Law Journal (2023).
10. Strengthened Code of Practice on Disinformation (June 2022) https ://digital–strategy.ec.europa.eu/en/ policies/code-practice-disinformation.

in the European Union " campaign " of re-balancing rights in the digital realm through hard law regulations, *i.e.* 1. the Digital Services Act (DSA) [11], that pursue harmonisation of providers responsibility and a stricter consideration of the notion of unlawful content ; 2. the Digital Markets Act (DMA), that aims at ensuring competition in markets where gatekeepers are present, and, as an effect, can ensure media diversity and respect for consumer autonomy and choices ; 3. the Digital Single Market Directive (DSM) [12], through which copyright protected contents are tackled by platform liability.

This scenario will be complemented by a Regulation that directly focuses on the protection of the independence of journalists and media pluralism against external influences, both at the political level and " digital " level : the newly agreed proposal of the European Media Freedom Act (EMFA) [13] on which EU institutions found an agreement in December 2023 [14]. In other words, the EMFA aims to establish " EU-wide harmonised rules to tackle these issues and overcome fragmentations in the national frameworks identified by the Commission " [15]. This paper aims to evaluate the potential benefits and obstacles associated with the EMFA, particularly within the context of the complex and intricate regulatory framework as described. To achieve this objective, the discussion will focus on the influence of private entities in driving a transformative regulatory landscape, wherein they wield significant influence over public discourse, as has been exemplified above through the role of social media within the Israeli-Palestinian conflict.

1. Dealing with (private) actors

2 - The are two reasons for the significance of private power within the new digital world. The first reason is " quantitative " : the pervasiveness of the process of digitalisation, mechanisms for algorithmic automation and the enormous volumes of data available in order to conduct processing and also to pre-empt users' preferences have endowed the major multinationals operating within the digital sector with unprecedented influence and a global reach. The second novelty is " qualitative ". It concerns the breadth, pluralism and freedom of public debate. In fact, we have never witnessed in the past what is currently happening within the digital domain. Specifically, private operators exert such significant dominance over this special type of market, namely the free marketplace of ideas – to paraphrase the legendary metaphor used by Holmes [16]– that they are capable of so effectively conditioning public debate. As a matter of fact, it has recently been argued that " fostering a large community – similar to a public sphere – is key to the business model " of the major platforms.

From this perspective, for instance, and with particular reference to a specific jurisdiction, the parallel that has been drawn within the case law of the Supreme Court of the United States between the space controlled by private online operators and the classical public forum, as the cradle of public discourse within the analogical domain, is extremely delicate and in many ways controversial, especially if a prescriptive and not only descriptive force must be attributed to that metaphorical language [17]. The aspects pointed out above are undoubtedly emblematic of the radical transformation triggered by the new digital world over the last two decades both on society as well as on the private " gatekeepers " of cyberspace, which have *de facto* " transformed " from economic operators into authorities in a technical sense, often exercising paraconstitutional functions. In the light of these preliminary reflections, it is proposed that we conceptualise digital power in terms of a quadrangular geometry, also with reference to the shift from a vertical dimension to a horizontal dimension.

Against this background, the structure of cyberspace and the physiognomy of the problematic issues that have been sketched out above represent the result of a series of legislative choices that lawmakers embraced, above all in the USA and the EU, around the turn of the millennium. As the illusion of a web that was free from potential state interference proved to be short-lived, a need arose for regulation that was consistent with the special nature of the digital ecosystem, which was satisfied both in Europe and in the US by a minimalist approach aimed at promoting the wide circulation of content. It should be recalled that the context within which lawmakers took their first steps was radically different from today, which explains why reform projects such as the DSA and the DMA are regarded as epic reforms, almost revolutionary in tone. The dominant concern within the minds of not only the US but also European lawmakers was to establish rules that could guide the actions of service providers (which had not yet emerged as full-blown gatekeepers, or at least as platforms) in order not to impede the circulation of content online.

The structure underpinning these legislative acts reflects, above all, the openness to freedom of expression that is inherent to US constitutionalism. As was also confirmed by the US Supreme Court's interpretation of freedom of expression in *Reno v. ACLU*, during those years, the Internet was regarded as a forum for exchanging ideas and giving effect to the free marketplace of ideas prophesied by Justice Holmes (although that had perhaps never previously been realised). Against a scenery of mistrust in regulation, and in particular a marked hostility to any form of content regulation that distinguished between content that was legitimately available online and content that could be accessed in the real world (moreover, the Supreme Court itself had held that there was no evidence of any increased benefit resulting from regulation, compared to an absence of regulation [18], US lawmakers chose a paradigm, set out in Section 230 of the Communications Decency Act, which is still an object of debate. This Act, which is still in force, gives effect to that libertarian fervour embodied in the First Amendment, which was celebrated at the dawn of the Internet [19]. The legislation exempts service providers from any responsibility for any moderation of defamatory content : irrespective of whether the service provider has chosen to remove content or to leave it online, that choice cannot result in any liability for it, save under exceptional circumstances. The reason for this choice, which massively favoured service providers, was to avoid any room for doubt regarding the legal classification of service providers. This, hence, solved the dilemma within US case law over whether to classify them as

11. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC.
12. Directive (EU) 2019/970 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market, OJ L 130/92.
13. Proposal for Regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market, 1 December 2022, COM (222) final.
14. It is set to enter into force in 2025.
15. Institute of European Media Law, *European Media Freedom Act* (2023).
16. *Abrams v. United States*, 250 U.S. 616 (1919). See, most notably, Justice Holmes' dissenting opinion, 624 ff.
17. Milan Kundera had already understood the sensitiveness of metaphorical language when, describing the main character of his most famous book, he highlighted *Tomàs' unawareness of the dangers entailed by metaphors and stated that it is best not to play with metaphors.* M. Kundera, *The Unbearable Lightness of Being* (Faber, 1984).
18. See *Reno v ACLU*, see n. 14 : " The dramatic expansion of this new marketplace of ideas contradicts the factual basis of this contention. The record demonstrates that the growth of the Internet has been and continues to be phenomenal. As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship ".
19. J. Kosseff, *The Twenty-Six Words That Created the Internet*, Cornell University Press (2017).

" distributors " or " publishers ". It has been noted that the choice made, which moreover resulted in an enhancement of the protection provided for under the First Amendment, resulted from the need to avoid virtuous forms of content moderation and policing by websites based on appropriate implementation mechanisms : this would have entailed a regime of editorial responsibility, which would have been excessively penalising for operators that were not formally involved in content control, especially on an *ex ante* basis.

As has been stressed by the literature, Section 230 CDA – which was nonetheless subject to some (unrealistic and ultimately unsuccessful) attempts at reform also during the Trump presidency [20] and was at the centre of the recent US Supreme Court's decision [21] in the *Gonzalez v. Google* case, concerning the existence of a liability of the search engine for the promotion of ISIS-sponsored content which led to the terrorist attacks and killings in Paris of November 2015 [22] – resulted from a bipartisan initiative aimed at avoiding the paradox, as is clearly apparent in the *Stratton Oakmont v. Prodigy* judgment [23] of the Supreme Court of New York, that the efforts made by a platform to carry out content policing in good faith could subject the operator of such a site to a more severe liability standard, such as that applicable to publishers and content providers [24]. The need to maintain separate liability standards flowed from the need to favour as far as possible the spread of new " virtual *agorà* " that could host and retransmit third party content, including content created by individual users themselves. Within this perspective, considering platforms as equivalent to content creators would have severely penalised the aim of favouring the exercise of freedom of speech in cyberspace. It was considered that this aim could be most readily achieved by providing that service providers should not incur any liability. Besides, the imposition of " direct " liability for content published by third parties would have significantly undermined the business models of content-sharing platforms.

That freedom of action was also needed for a contingent reason : there was a conviction that minimalist legislation inspired by a digital liberalist vocation [25] would leave greater freedom to the new actors that were starting to operate online to promote the new technology by spreading content on the Internet without any fear of subsequent sanctions, thereby engaging a process of collateral censorship [26].

This idea of digital liberalism readily migrated from one side of the Atlantic to the other. Indeed, albeit several years later, Europe also adopted a regulatory framework inspired by concerns not to inconvenience the business models of " information society service providers " : in other words, to favour e-commerce as much as possible [27]. The (few) provisions dedicated to the liability regime were set out within Directive 2000/31/EC, known as the " E-Commerce Directive " [28], which laid down two fundamental rules : first of all, the lack of any general requirement of preventive supervision for service providers (in keeping with the absence of any editorial liability and with the aim of maintaining as much as possible the free flow of online content without any " conditioning ") ; second, the provision of a " notice and takedown " mechanism, which was imported from the special rules (providing for an exception to Section 230) contained in the US Digital Millennium Copyright Act (DMCA) [29]. This framework is based on the absence of any direct liability on the part of the service provider for any unlawful content ; it provides, by contrast, that the service provider incurs liability where it fails to ensure the removal of any manifestly unlawful content, despite effectively being aware of it.

It is clearly apparent that the legal framework in Europe and the USA was adopted within a specific context, where there were reasonable prospects of cyberspace becoming a location for realising the metaphor of the free marketplace of ideas. Within this scenario of major competition between virtual communities, it was inevitable that the concern of lawmakers would be to keep regulatory pressure to a minimum, trusting in the inherent capacity of cyberspace to " self-regulate ", offering alternative spaces that were capable of establishing and legitimising themselves.

Within this context, competition law has reigned supreme in the USA, although also in Europe, as the only instrument allowing for *ex post* intervention in relation to the concentrations of economic power that gradually and inevitably emerge. The relevant context is specifically the market, and the relevant freedom is freedom of enterprise. A profound paradigm shift occurred within the space of a few years. The new players that had emerged in the digital era transformed from economic operators into private powers, following which antitrust law proved inadequate, resulting in the need for intervention using the instruments typical of constitutional law [30].

2. European Media Freedom Act : killing two birds with one stone ?

3 - The legal, social, political and economic context changed together with (and, maybe, also because of) the role of private powers. The EU, as anticipated, tried to wave this renovated realm, reacting to the deficiencies of the past and adopting several sectorial and horizontal regulations, such as the EMFA. Scholars underlined that it can be defined as a " meta regulation " [31] that aims to reconcile the self-regulatory nature with the need for EU-defined standards for media freedom.

To be concise [32], the proposed regulation : 1. It aims at safeguarding the independent functioning of public service media providers (Art. 5 of the proposal) ; 2. It establishes media service providers' duties to provide news and current affairs content (Art. 6) ; 3. It

20. Giovanni De Gregorio and Roxana Radu, " Trump's Executive Order : Another Tile in the Mosaic of Governing Online Speech " (*MediaLaws*, 6 June 2020) <https ://www.medialaws.eu/trumps-executive-order-another-tile-in-the-mosaic-of-governing-online-speech/>.
21. *Gonzalez v. Google LLC*, 598 U.S. __ (2023). The Hearing of the parties arguments in front of the Supreme Courts, held last February, have been quite instructive. More precisely it is worth mentioning the opinion of justice Elena Kagan. On the one hand, she admitted : " We're a court, we really don't know about these things, " adding, " These are not like the nine greatest experts on the internet. " Kagan's suggestion seems to be that reviewing section 230 is a job for Congress and not for the Court. On the other hand, Kagan also pointed out probably the most evident weakness of the legislation at stake : " this was a pre-algorithm statute in a post algorithm world ".
22. See " Twitter, Inc. v. Taamneh " (SCOTUSblog, October 2022) <https ://www.scotusblog.com/case-files/cases/twitter-inc-v-taamneh/> accessed 2 May 2023.
23. *Stratton Oakmont v Prodigy*, 23 Media L. Rep. 1794 (N.Y. Sup. Ct. 1995).
24. Just a few years earlier, the US District Court for the Southern District of New York, in *Cubby, Inc. v CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991) had seemingly seconded the assimilation of online platforms to distributors, suggesting a similarity with news-stands, libraries, and book-shops as far as control over content is concerned.
25. Giovanni De Gregorio, *Digital Constitutionalism in Europe*, Cambridge University Press (2022).
26. Jack Balkin, *Free Speech and Hostile Environments*,99 Columbia Law Review, 2295 (1999).
27. Giovanni De Gregorio, *op. cit.*
28. See Lillian Edwards (ed), *The New Legal Framework for e-Commerce in Europe*, Bloomsbury (2005).
29. Digital Millennium Copyright Act 1998 (DMCA).
30. This is also because, in the meantime, the Internet was undergoing a major transformation, which had significant repercussions on the physiognomy and role of platforms. The rules introduced in the USA in 1996 and in Europe in 2000 appeared to be increasingly obsolete. They were ill-suited to the characteristics specific to the new platforms that were establishing themselves and, during the initial stages of those platforms (as we shall see when considering the reactions of digital sovereignty to the consolidation of private power), required a major dose of creativity, if not even manipulation, within the case law of the ECJ.
31. Marta Cantera Gamito, *The European Media Freedom Act (EMFA) as meta-regulation*, Computer Law & Security Review 48 (2023).
32. For an in-depth analysis, refer to Vincenzo Iaia, *The regulatory road to the European Media Freedom Act : opportunities and challenges ahead*, Rivista di Diritto dei Media, 2 (2023), pp. 221-240.

creates a framework for regulatory cooperation and a well-functioning internal market for media services (Chapter III), comprising stricter rules for very large online platforms [33] (hereafter, VLOPs, Art. 17-18) ; 4. It establishes the European Board for Media Services (Art. 8-12). From this brief overview, it is possible to observe how the act fosters both regulations with respect to the Member State's (MS) duties towards free speech and integrates the DSA obligations for VLOPs. In a way, it aims to kill two birds with one stone. For what interests this article, the authors will focus only on the second aspect [34].

The relations between private actors and journalists come at stake precisely with respect to the removal (*i.e.*, suspension) of content from the platform itself. Thus, Art. 17 outlines a provision safeguarding editorial content published by media service providers on very large online platforms (VLOPs). In the event that such providers assert compliance with specific conditions to a VLOP, they are entitled to preferential treatment for their content within the moderation practices of that platform. A comparable provision had been previously deliberated within the DSA, proposed as a mandatory " media exemption " encompassing general terms and conditions and notice-and-action mechanisms. However, no political consensus was achieved on this matter at that time [35]. This provision now undergoes renewed consideration outside the DSA, without formal amendment to the DSA itself, by introducing the new EMFA provision. In more granular terms, Article 17(1) mandates VLOP to offer a self-declaration functionality for the specific category of their " recipients " (i.e., users). These users must be identified as belonging to the group of media service providers who are independent and subject to some form of regulatory oversight in their function [36].

This provision is worrisome for two reasons : substantive and procedural.

Within the first issue, Art. 17 states that VLOPs shall take " all possible measures " to communicate to the media service provider the reasons for the decision to suspend the provision of its service concerning content provided by that media service provider that is incompatible with its terms and conditions (Article 17(2) EMFA). The substantive problem is compliance : it is not well clarified if, where and when platforms should act, and, in terms of contrasting disinformation, this might create pitfalls in the circulation of fake news. On a procedural level, Art. 17 does not provide any procedural mechanism or mention any sort of procedural safeguard for the media service providers to contrast the VLOPs' decision. This aspect seems to contrast with the logic of the DSA, which, instead, establishes specific obligations on VLOPs for dispute settlements (Art. 20 – 21). Instead, Art. 17(4) only specifies that : " where a media service provider that submitted a declaration pursuant to paragraph 1 considers that a provider of very large online platform frequently restricts or suspends the provision of its services in relation to content provided by the media service provider without sufficient grounds, the provider of very large online platform shall engage in a meaningful and effective dialogue with the media service provider, upon its request, in good faith with a view to finding an amicable solution for terminating unjustified restrictions or suspensions and avoiding them in the future. The media service provider may notify the outcome of such exchanges to the Board ".

It says nothing about what happens if the entire service is suspended, as also observed by scholars [37]. The issue is not insignificant : the lack of *ad hoc* procedural mechanisms and the presence of interpretative doubts as to the extent of the ability of VLOPs to suspend contents opens up several issues relating to the application of the rule and, consequently, to the practical and expeditious protection of the persons concerned. Journalists and media service providers have given their delicate role in protecting freedom of expression and information. The risk is of fragmenting VLOP's obligations and, as a result, of the protection of rights, creating a loophole mechanism that harms the very scope of the EMFA : securing the market against undemocratic positions coming from the political world and stagnating in and by the digital realm.

Conclusion

4 - There is an inherent tension between the role of journalists as " watchdogs ", their freedom of expression, and the stemming interests of controlling their voices descending both from public and private powers. This article analysed the second's influence on the exercise of the journalists' professions, in particular, considering the soon-to-be-enacted European Media Freedom Act. This ambitious regulation still leaves space for ambiguity due to the design of procedural solutions with respect to the suspension of contents by VLOPs. It stressed the issues related to Art. 17 EMFA due to its connection with the DSA, resulting in a *lex specialis* of the latter. As a matter of fact, the entire lack of safeguards of any type leaves the private operator to decide what arrangements should be applied, which obviously undermines the rights of the individual on both a procedural and a substantive level. Seemingly, the creation of substantive rights without a well-defined procedural framework can give rise to uncertainties, pushing back the obtained safeguards to a precedent period of the digital regulation history that the EMFA purpose is to leave beyond. Hence, the creation of new substantive rights without the appropriate procedural safeguards can risk producing rights that only exist on paper.■

33. As defined under Art. 3 of the DSA.

34. The EMFA imposes rules on MS under Art. 4, which must respect media service providers' editorial freedom. In that regard, certain actions by Member States, including by their national regulatory authorities and bodies, are prohibited, such as a) not interfering in editorial policies, b) detaining, sanctioning, intercepting, subject to surveillance or search and seizure, or inspect media service providers ; c) deploy surveillance measures. This is a matter that created many tensions during the trilogue phase since some MS tried to negotiate a position that expands the list of crimes that may justify the use of surveillance measures, as recalled by digital rights advocates EDRi, *Challenges ahead : European Media Freedom Act falls short in safeguarding journalists and EU fundamental values* (2024).

35. Diana Willis, *European Media Freedom Act : No to any media exemption*, Euractiv, 15 May 2023.

36. See also Institute of European Media Law, *ibid*.

37. Doris Buijs, *Article 17 Media Freedom Act & the Digital Services Act : aligned or alienated ?*, DSA Observatory (2022).

15

A Rapidly Shifting Landscape : Why Digitized Violence is the Newest Category of Gender-Based Violence

Rangita DE SILVA DE ALWIS [1],

Faculty at the University of Pennsylvania Penn Carey Law School and the Wharton School of Business, Senior Fellow at the Harvard Law School Center on the Legal Profession

This paper proposes that new research on technology-facilitated violence must shape gender-based violence against women laws. Given the AI revolution, including large language models (" LLMs "), and generative artificial intelligence, new technologies continue to create power disparities that help facilitate gender-based violence both online and offline. The paper argues that the veil of anonymity provided by the digital realm facilitates violence ; and the automation capabilities offered by technology amplify the scope and impact of abusive behavior. Although the direct physical act of sexual violence is different from offline violence, there are similarities. Firstly, both acts share the structural gender and intersectional inequities that lie at the root of such conducts in the first place. Secondly, the defense that women and girls are free to exercise the option to leave an abusive online environment denies women's and girls' free exercise of rights to assembly and expression in the online public square. In the final analysis, although not all isolated acts of online violence meet a legal threshold, we need to see these acts as a part of a continuum of offline violence that call for new forms of discourse and a dynamic application of international women's human rights norms into evolving categories of violence.

Introduction

1 - Naming has the power to shift legal and social norms. Technology facilitated gender-based violence is still largely an unnamed crime. Technology facilitated misogyny has many faces, both figuratively and in real terms. FaceMash, the precursor to Facebook, was developed by Facebook creator Mark Zuckerberg in 2003, and was designed to compare women's physical looks in elite American colleges. The paper calls for the application of human rights theory, critical gender theory and critical information theory to address this type of technology facilitated gender-based violence. Critical Information Theory examines an asymmetry in power relations and unmasks the power inequalities behind structures. Critical information theory not only calls attention to biased data but also asks whether the structures for using information have a chilling effect on certain groups of users. Technology-facilitated violence has the effect of : 1) blurring the lines between the real and the virtual worlds where online harassment and abuse targeted at women and minorities spill into the real world, thereby causing both physical and psychological violence ; 2) digital and internet technologies are embedded in ubiquitous ways that compromise women's ability to seek freedom from violence and render abusers " omnipresent " ; 3) technology-facilitated gender-based violence, by its very nature, is both personal and structural.

The dichotomy between " online " and " offline " violence collapses when it is subject to scrutiny through the lenses of critical gender theory and critical information theory. This article proposes the revision of anti-violence against women frameworks to address the evolving category of coded violence. A new generation of laws on gender-based violence should focus not only on the punishment of the perpetrator but on more structural remedies addressing the root causes of violence through preventative mechanisms. Efforts to address technology facilitated violence against women would include education on digital violence, including critical information theory (" CIT "). Because CIT engages culture and cultural change, this model would also consider how culture and information intersect and draw attention to the engagement of men as leaders and role models.

Technology-driven violence has a shape-shifting quality. It has the effect of blurring the lines between the real and the virtual worlds of violence against women. Online harassment and abuse targeted at women and minorities spill into the real world, thereby causing both physical and psychological violence. Digital and Internet technologies are embedded in ubiquitous ways that compromise women's ability to seek freedom from violence and render abusers " omnipresent. " In this paper, I will critically explore the human rights framework, especially the Convention on the Elimination of Discrimination against Women (" CEDAW "), and the landscape of domestic laws and regulations which provide new normative frameworks for combating violence in the digital space. In the final analysis, I call for a new gender-based violence framework that is informed both by critical information theory and

1. Rangita de Silva de Alwis is faculty at the University of Pennsylvania Carey Law School and the Wharton School of Business. She is Hillary Rodham Clinton Distinguished Fellow on Global Gender Equity at the Georgetown Institute for Women, Peace and Security and Senior Fellow at the Harvard Law School Center on the Legal Profession where she was Visiting Faculty at the Harvard Kennedy School of Government. She will be a Visiting Fellow at Bonavero Institute for Human Rights, Oxford University in 2024. She was elected as an expert to the treaty body on the Convention on the Elimination of Discrimination against Women (CEDAW) for the 2023-2026 term. She thanks her colleague on the CEDAW Committee, Nicole Ameline, for her inspiration and for encouraging her to address new frontiers for the CEDAW. She also thanks her Research Assistant Yungjee Kim (Penn Carey Law " 25) and her student Octavie Jacquet, Editor in Chief of the Sciences Po Law Review for their leadership.

human rights to address technology enabled violence as a growing category of both interpersonal and structural violence.

Technology facilitated gender-based violence like other forms of gender-based violence is about power, control and power imbalance. You can see this in data bias, or algorithmic bias that occurs when predefined data types or data sources are intentionally or unintentionally treated differently than others. Data is not inherently neutral ; data control itself is a form of power. It has the potential for great good and for great harm. We need a new way of thinking about technology and data science –one that is informed by intersectional feminist thought.

1. THIS MOMENT IN TIME

2 - The emergence of brand-new technology, including large language models (" LLMs "), and generative artificial intelligence (" AI ") continues to create power disparities and help facilitate gender-based violence as an evolving category of violence. Writing recently, Noam Chomsky, one of the world's leading linguists, warns us : " machine learning...will degrade our science and debase our ethics by incorporating into our technology a fundamentally flawed conception of language and knowledge. " [2] To this, I would like to add that machine learning (" ML ") and other evolving technology can create a fundamentally flawed conception of not only language and knowledge, but of power, especially over those who have historically been rendered powerless.

While the #MeToo movement was a key inflection point that galvanized a new era of digital feminist activism, this moment of generative AI is sparking fresh concerns about synthetic media and deepfakes. Digital sexual violence is rapidly changing with the dizzying changes in AI. Newer-and more interactive-digital and online spaces such as deepfakes and generative AI offer hitherto unanticipated forms of gender-based violence. While these digital spaces replicate in some ways the gender inequality in human interactions which occur outside of online environments, these online spaces offer a dystopian forum that can amplify inequality and magnify violence against women. Technology has outpaced legal reform, and even our ability to envision new forms of online harms and digital violence in social media sites and online games.

A. - New Forms of Online Violence Against Women

3 - In the contemporary digital era, the Internet has emerged as a new battleground where violence against women manifests itself. Online gender-based violence (" OGBV ") harnesses digital technology to instigate threats, intimidation, and harassment, constituting a dynamic and ever-evolving phenomenon within the rapidly progressing realm of technology. OGBV encompasses various forms such as cyberstalking, online harassment, non-consensual dissemination of intimate images, doxing, slut-shaming, trolling, cyber-flashing, gendered hate speech, disinformation, misinformation, cyber smear campaigns, threats of sexual violence and murder, morphing, as well as the proliferation of AI-generated sexually explicit media.

The intersection of technology and violence highlights the dual nature of technological advancements. While technology offers unprecedented connectivity and accessibility, it also serves as a double-edged sword, providing a platform for perpetrating, targeting, harassing, and threatening women. In this increasingly interconnected world, technology has opened new avenues through which acts of violence against women can be perpetrated.

Firstly, a notable characteristic of OGBV is the ability for offenders to remain anonymous to their victims. This veil of anonymity provided by the digital realm not only enables their actions but also emboldens them in their abusive behavior. Secondly, the geographical distance facilitated by online platforms allows offenders to engage in abusive conduct from afar, without the need for physical proximity or even being in the same country as their victims. This geographical detachment provides a sense of detachment and impunity for the offenders. Thirdly, the automation capabilities offered by technology amplify the scope and impact of abusive behavior. Offenders can exploit technological tools to perpetrate their abuse more efficiently and with minimal effort. Moreover, the pile-on effect is a significant concern in the online space, where multiple offenders can join forces in harassing and bullying a sole individual. The digital platforms themselves, designed for easy and rapid dissemination of content, facilitate this collective harassment.

Most of all, the unequal power dynamics between men and women, along with the devaluation of women in society, permeate into the online sphere as an extension of offline belief systems. 85% of women reported encountering some form of OGBV. [3] Furthermore, 23% of women reported encountering online harassment at least once in their lives, and one in ten women experienced OGBV since the age of fifteen. [4] The impact of OGBV is substantial-for example, 20% of surveyed women journalists report withdrawing from all online interaction because of OGBV. [5]

The U.N. General Assembly recognized the growing concern of ICT-facilitated abuses against women human rights defenders, and the need for effective responses in line with human rights principles. [6]

The structure of the Internet and social media platforms creates echo chambers, where individuals reinforce their existing views through repetition and interaction within a self-contained bubble. This echo chamber phenomenon, devoid of opposing perspectives, leads to confirmation bias and has far-reaching social, political, and cultural effects. In the context of OGBV, an example of this phenomenon is the incel movement, an internet subculture that frequently expresses deeply misogynistic content. However, it is important to acknowledge that while technology can contribute to discriminatory behaviors, it also has the potential to promote gender equality and challenge societal norms and ideologies that perpetuate such abuses.

Several technological solutions have emerged to counter OGBV, such as smartphone applications and software that protect against stalkerware, malware, spyware, and trackers, as well as alert emergency contacts and services with geolocation features and crisis alarms. Additionally, there is a concerning trend of AI-powered chatbots, created as on-demand romantic or sexual partners, being subjected to abuse by users. This form of chatbot mistreatment often exhibits a gendered component, with men creating digital partners representing women and subjecting them to abusive language and aggression. Online forums on platforms like Reddit and Discord even provide spaces for abusers to share tactics and strategies for further harming their virtual partners.

2. Noam Chomsky et al., *The False Promise of ChatGPT*, NY Times (Mar. 8, 2023), https ://www.nytimes.com/2023/03/08/opinion/noam-chomsky-chatgpt-ai.html.

3. *Measuring the Prevalence of Online Violence Against Women*, The Economist : Intelligence Unit, https ://onlineviolencewomen.eiu.com/.

4. *Amnesty Reveals Alarming Impact of Online Abuse Against Women*, Amnesty Int'l (Nov. 20, 2017), https ://www.amnesty.org/en/latest/press-release/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/.

5. Julie Posetti et al., *Online Violence Against Women Journalists : A Global Snapshot of Incidence and Impacts*, U.N. Educ., Sci. & Cultural Org. [UNESCO] (2020), https://www.icfj.org/sites/default/files/2020-12/UNESCO%20Online%20Violence%20Against%20Women%20Journalists%20-%20A%20Global%20Snapshot%20Dec9pm.pdf.

6. G.A. Res. 68/181, U.N. Doc. A/RES/68/181 (Jan. 30, 2014) (stating that " [ICT]-related violations, abuses, discrimination and violence against women, including women human rights defenders, such as online harassment, cyberstalking, violation of privacy, censorship and the hacking of e-mail accounts, mobile phones and other electronic devices, with a view to discrediting them and/or inciting other violations and abuses against them, are a growing concern and can be a manifestation of systemic gender-based discrimination, requiring effective responses compliant with human rights. ").

B. - Why Technology Facilitated Violence is Gender-Based Violence

4 - Although the direct physical act of sexual violence, and the degree of violation of sexual autonomy that arises from it, differ between online and offline worlds, both acts share the structural causes that lie at the root of such conduct in the first place : patriarchy, and historical power differences between the genders.

First, this power difference is inherent to the argument that women and girls are free to exercise the option to leave an abusive online environment which helps to take away women's and girls' right to equality, including their equal rights to the Internet and the online community. Secondly, online violence may result in direct physical, emotional and psychological violence-whether it be mental harm suffered as a result of online violence or bodily harm suffered offline.

Digital gender-based violence has many faces, both figuratively and in real terms. FaceMash, the precursor to Facebook, was developed by Facebook creator Mark Zuckerberg in 2003, and was designed to compare women's physical looks in elite American colleges. [7] More recently, feminist gaming critic Anita Sarkeesian was forced to leave her San Francisco home due to ongoing threats by online trolls had threatened to kill her parents, drink her blood, and rape her-all while publishing her personal details online. [8] Most horrifyingly, an interactive game was created in her likeness, in which players were encouraged to " beat up Anita Sarkeesian " by virtually punching an image of her face. [9]

These online threats against women in public life are common and have sometimes resulted in women leaving office. For instance, Diane Abbott, the first black member of Parliament in the U.K., was targeted with more than 8,000 tweets in the first six months of 2017 alone. [10] Maria Ressa, the Nobelist, has been subject to abuse for her stand against civil rights violations by the Duterte regime. Researchers analyzed nearly 400,000 tweets and more than 57,000 Facebook posts and comments directed at Ressa between 2016 and 2021 : while 60% of the online violence questioned Ressa's credibility as a journalist, 40% of the attacks were threats to physical safety including threats of rape and murder. [11] In the U.K., following years of online abuse over her political coverage, journalist Laura Kuenssberg announced that she would move to a new role at BBC. [12] Due to the harassment she has been a target of, she was assigned a bodyguard. [13]

C. - A Continuum of Violence : Deepfakes

5 - The proliferation of deepfakes, AI-generated images, videos, and other media content against women is another emerging category of violence that must be named in new and revised gender-based violence laws and by the CEDAW. Deepfake technology uses AI and facial mapping technology to merge, combine, and superimpose images and video clips onto one another to generate authentic-looking media called " deepfakes. " Pornographic deepfakes reinforce a culture that commodifies and objectifies women's bodies.

Companies such as DeepSwap.Ai allow an individual to upload an image or video and swap it with any number of faces a user chooses to upload. [14] Some websites explicitly promise to turn any person into a " porn star " by uploading their photo onto the website, which uses deepfake technology to swap the person's face into an adult. [15]

Deepfakes have become the new sites for violence against women and technology-facilitated abuse. Estimates suggest that more than ninety-five percent of deepfake videos on the Internet in 2019 were pornographic. [16] Companies like Google allow users to request the removal of involuntary fake pornography. [17] Facebook has expressed that they will address deepfakes and other manipulated media, including investigating AI-generated content and deceptive behaviors, in partnership with academic, government, and industry professionals to remove misleading images and punish perpetrators of media misuse. [18] DeepSwap.Ai's terms of service explicitly disallow the creation of pornographic deepfakes :

> [Y]ou shall not upload, share or otherwise transmit to or via the Services any content that : is...obscene, abusive, racially or ethnically offensive, pornographic, indecent, lewd, harassing, threatening, invasive of personal privacy.... [19]

D. - The Nexus Between Online Gender-Based Harassment and the Erosion of the Democratic Space

6 - In August 2020, Speaker Nancy Pelosi and other American women lawmakers, along with legislators around the world, wrote a letter to Facebook calling upon the platform to take action to protect female political actors from online attacks. The letter went on to say : " Make no mistake... [t]hese tactics, which are used on your platform for malicious intent, are meant to silence women, and ultimately undermine our democracies. " [20] Further, it read : " We are imploring Facebook to do more to protect the ability of women to engage in democratic discourse and to foster a safe and empowering space for women. " The letter was written in the aftermath of Facebook's refusal to take down a deep-fake video of her that was manipulated so she appeared intoxicated. [21]

The disproportionate and often strategic targeting of women politicians has both direct and indirect impact on the democratic process by driving women out of political office and muffling those who remain online. [22] While censoring free speech erodes the democratic space, a vibrant democracy calls for the full and equal

7. Katherine A. Kaplan, *Facemash Creator Survives Ad Board*, Harvard Crimson (Nov. 19, 2003), https ://www.thecrimson.com/article/2003/11/19/facemash-creator-survives-ad-board-the/.
8. Soraya Nadia McDonald, *Gaming Vlogger Anita Sarkeesian is Forced from Home After Receiving Harrowing Death Threats*, Wash. Post (Aug. 29, 2014, at 5 :23 a.m. EDT), https ://www.washingtonpost.com/news/morning-mix/wp/2014/08/29/gaming-vlogger-anita-sarkeesian-is-forced-from-home-after-receiving-harrowing-death-threats/.
9. *Id.*
10. Anastasia Powell et al., *The Palgrave Handbook of Gendered Violence and Technology* (Palgrave Macmillan eds. Nov. 2022).
11. David Mass, *New Research Details Ferocity of Online Violence Against Maria Ressa*, Int'l Journalists " Network (Mar. 8, 2021), https ://ijnet.org/en/story/new-research-details-ferocity-online-violence-against-maria-ressa.
12. *Laura Kuenssberg to Step Down as BBC's Political Editor*, BBC (Dec. 20, 2021), https ://www.bbc.com/news/entertainment-arts-58996925.
13. Patrick Kingsley, *Why the BBC's Star Political Reporter Now Needs a Bodyguard*, NY Times (Sept. 27, 2017), https ://www.nytimes.com/2017/09/27/world/europe/uk-bbc-laura-kuenssberg-labour.html.
14. DeepSwap, https ://www.deepswap.ai/landing/playable-faces.
15. Kweilin T. Lucas, *Deepfakes and Domestic Violence : Perpetrating Intimate Partner Abuse Using Video Technology*, 17 Victims & Offenders 647 (2022).
16. Meredith Somers, *Deepfakes, Explained*, MIT Sloan (July 21, 2020), https ://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained.
17. *Remove Involuntary Fake Pornography from Google*, https ://support.google-.com/websearch/answer/9116649 ?hl=en.
18. Monika Bickert, *Enforcing Against Manipulated Media*, Meta Newsroom (Jan. 6, 2020), https ://about.fb.com/news/2020/01/enforcing-against-manipulated-media/.
19. However, in the U.S., online platforms are protected by Section 230 of the Communications Decency Act from civil liability for user-generated content.
20. Emma Goldberg, *Fake Nudes and Real Threats : How Online Abuse Holds Back Women in Politics*, NY Times (June 7, 2021), https ://www.nytimes.com/2021/06/03/us/disinformation-online-attacks-female-politicians.html.
21. Abram Brown, *Facebook Can Be Toxic for Female Politicians, Company Documents Show*, Forbes (Oct. 27, 2021, 04 :27pm), https ://www.forbes.com/sites/abrambrown/2021/10/27/facebook-can-be-toxic-for-female-politicians-company-documents-show/ ?sh=258e3f175020.
22. *See further*, Lucina di Meco & Saskia Brechenmacher, *Tackling Online Abuse and Disinformation Targeting Women in Politics*, Carnegie Endowment for Int'l Peace (Nov. 30, 2020), https://carnegieendowment.org/2020/11/30/tackling-online-abuse-and-disinformation-targeting-women-in-politics-pub-83331 (detailing online gender-based abuse of female politicians around the world) ; Nina Jankowicz et al., *Malign Creativity : How Gender, Sex, and Lies are Weaponized Against Women Online*, Wilson Ctr. Sci. & Tech. Innovation Program (Jan. 2021), https://www.wilsoncenter.org/sites/default/files/media/uploads/documents/Report%20Malign%20Creativity%20How%20Gender

participation of both men and women online and offline. Female politicians are not only targeted disproportionately but also subjected to different forms of harassment and abuse based on physical appearance and sexuality. [23] All this has the very real potential to pose a chilling effect on the participation and engagement of women in civic and political life-not just as politicians but as participants in the online debates that now drive so much of political culture.

In October 2023, a former student from the National Polytechnic Institute, Mexico was charged in connection with a first-of-its-kind cases involving AI-driven digital violence. [24] The student had used AI to generate non-consensual deepfake pornography, digitally undressing fellow students, and subsequently profited from selling these manipulated images on the Internet. [25] The accused is currently facing charges related to privacy offenses, as outlined by the Olympia Law. [26] This legislation, specific to Mexico City, safeguards individuals from the creation and dissemination of intimate images without their consent. [27] Remarkably, this law appears to have anticipated the potential misuse of AI in such instances, reflecting the proactive nature of its provisions. [28]

In September 2023, the UK adopted the Online Safety Act-one of the most wide-ranging efforts by a Western democracy to oversee digital discourse. [29] These far-reaching guidelines have sparked discussions on the fine balance between free expression and prevention of harmful online content, with a specific focus on safeguarding children. [30] The bill defines " primary priority content that is harmful to children " as " content which encourages, promotes or provides instructions " [31] for " suicide, " [32] " an act of deliberate self-injury, " [33] and " an eating disorder. " [34] On the other hand, in 2020, the French Constitutional Council struck down similar regulations due to concerns about overreach and censorship. [35]

2. HUMAN RIGHTS FRAMEWORK

A. - International Human Rights Law's Response to Digital Violence

7 - The proliferation of digital violence is raising key normative and institutional challenges to the existing international human rights law and international women's human rights frameworks. A changing normative landscape creates new opportunities for promoting human rights in the digital age. We need a radical reinterpretation of existing human rights in order to allow them to meet the new conditions of the digital age.

International human rights law has always responded to the ways in which individuals and societies confront changing economic, social, and cultural conditions. It could be argued that the current " digital revolution " represents yet another moment for transformation in the international human rights law framework. This revolution also invites a process of normative transformation involving the articulation of new legally binding or soft law instruments. The UN Human Rights Council (" HRC ") has adopted a plethora of non-binding resolutions that advocate the extension of offline human rights to activities and interactions online. [36]

The EU Commission, too, is dealing in this moment with new regulations and those yet in the pipeline. [37] The Commission has promulgated a Declaration on Digital Rights and Principles for the Digital Age which addresses rights of individuals both offline and online. [38]

These evolving norms will be discussed under three pillars :

1° Due Diligence Principle

8 - The first involves efforts to strengthen corporate responsibility through the Business and Human Rights platform following the adoption of the Ruggie Principles, or the Guiding Principles on Business and Human Rights, a legally binding instrument on business and human rights. The Guiding Principles require businesses to exercise " human rights due diligence, " to impose legal liability for human rights abuses, to see to it that remedies are provided to victims, and to engage in international cooperation in the implementation of the instrument. This framework also applies to technology companies whose activities affect the enjoyment of digital human rights, and, in particular, to those operating online platforms, providing Internet services and developing AI products.

2° Extraterritoriality

9 - The second involves the extraterritorial reach of the human rights obligations of technology exporting countries in relation to the conduct of private companies. Although States are largely defined by territorial sovereignty and territorial jurisdiction, the evolving digital rights call for addressing the extra-territorial activity of non-state actors. [39] One transformation is the extra-territorial application of human rights obligations on governments to actively regulate private businesses.

The extra-territorial application of international human rights is manifest in the work of treaty bodies. For example, in 2018, the HRC Committee developed a jurisdictional standard covering conduct with extraterritorial effects that has " direct and reasonably foreseeable impact " on the enjoyment of the right to life. [40] In 2021, the Committee on the Rights of the Child (" CRC ") embraced " reasonable foreseeability " of impact as the test for exercising extra-territorial jurisdiction in a climate change case. [41]

In its 2014 review of the fourth periodic report of the US, the HRC Committee raised concerns about media reports describing surveillance activities undertaken by US security agencies both inside and outside US territory. These episodes included the collection of bulk data and metadata, and the alleged wiretapping of European leaders. The Committee recommended that the U.S. take the necessary measures to ensure that " any interference with the

%2C%20Sex%2C%20and%20Lies%20are%20Weaponized%20Against%20Women%20Online_0.pdf (same).

23. *Id.*
24. María Alejandra Trujillo, *Mexico : Arrest in Landmark AI-Related Digital Violence Case*, BNN (Nov. 26, 12 :29 PM), https ://bnn.network/breaking-news/crime/mexico-arrest-in-landmark-ai-related-digital-violence-case/.
25. *Id.*
26. *Id.*
27. *Id.*
28. *Id.*
29. Adam Satariano, *Britain Passes Sweeping New Online Safety Law*, NY Times (Sept. 19, 2023), https ://www.nytimes.com/2023/09/19/technology/britain-online-safety-law.html.
30. *Id.*
31. Online Safety Act 2023, 2023 ch. 50 § 61 (U.K.).
32. *Id.* at § 61(3).
33. *Id.* at § 61(4).
34. *Id.* at § 61(5).
35. *Freedom on the Net 2020*, Freedom House (last visited Nov. 26, 2020), https ://freedomhouse.org/country/france/freedom-net/2020.
36. *See e.g.*, G.A. Res. 68/167, [para] 3 (Dec. 18, 2013) ; G.A. Res. 69/166, [para] 3 (Dec. 18, 2014) ; G.A. Res. 73/179, [para] 3 (Dec. 17, 2018) ; G.A. Res. 75/176, [para] 3 (Dec. 16, 2020) ; Human Rights Council [HRC] Res. 26/13, U.N. Doc. A/HRC/RES/26/13, at 2 [para] 1 (June 26, 2014) ; HRC Res. 32/13, U.N. Doc. A/HRC/RES/32/13, at 3 [para] 1 (July 1, 2016) ; HRC Res. 38/7, U.N. Doc/HRC/RES/38/7, at 3 [para] 1 (July 5, 2018).
37. The EU AI Act was passed in December 2023 during the writing of this article. The European Commission president Ursula Von der Leyen heralded the AI Act as a " unique legal ; framework for the safety and fundamental rights of people and businesses. ". *See* Morgan Meaker, *The EU Just Passed Sweeping New Rules to Regulate AI*, Wired (Dec. 8, 2023 at 06 :20 PM), https ://www.wired-.com/story/eu-ai-act/.
38. European Declaration on Digital Rights and Principles for the Digital Decade, Commission Decl. at Ch. 1, COM (2022) 28 final (Jan. 26, 2022).
39. *See e.g.*, Mariarosaria Taddeo & Luciano Floridi, *New Civic Responsibilities for Online Service Providers*, *in* the responsibilities of online providers 1 (Mariarosaria Taddeo & Luciano Floridi eds., 2017).
40. Human Rights Committee [HRC Committee], General Comment No. 36 : The Right to Life, [para][para] 22, 63 U.N. Doc. CCPR/C/GC/36 (2018).
41. *Sacchi v. Argentina*, Views of the C.R.C., [para] 10.7, U.N. Doc. CRC/C/88/D/104/2019 (2021).

right to privacy complies with the principles of legality, proportionality, and necessity, regardless of the nationality or *location* of the individual whose communications are under *direct* surveillance. " [42]

3° Interrelatedness of Human Rights Norms

10 - The third pillar is the emerging effort in relation to a holistic understanding of the core treaties. This involves giving effect to the 1993 Vienna Declaration core values concerning the indivisibility, interdependence, and interrelatedness of all human rights, as well as the drawing of treaty bodies from each other's jurisprudence. [43]

The international human rights agenda itself provides a powerful framework to prevent coded violence against women, including the CEDAW, and the Declaration on the Elimination of Violence against Women. The CEDAW General Recommendation 35 Paragraph 6 acknowledges that :

> Gender-based violence against women, whether committed by States, intergovernmental organizations, or non-State actors, including private persons... It manifests itself on a continuum of multiple, interrelated and recurring forms, in a range of settings, from private to public, including technology-mediated settings...

Furthermore, the Declaration on the Elimination of Violence Against Women's recognition that " violence against women is a manifestation of historically unequal power relations between men and women, which have led to domination over and discrimination against women by men and to the prevention of the full advancement of women " provides us with a strong conceptual framework for the understanding of coded bias.

In 2018, the U.N. Special Rapporteur on Violence Against Women, its Causes and Consequences (" UNSRVAW ") recognized the diverse nature of online violence against women, including its sexualized forms :

> Online and ICT-facilitated acts of gender-based violence against women and girls include threats of such acts that result, or are likely to result, in psychological, physical, sexual or economic harm or suffering to women. (...) ICT may be used directly as a tool for making digital threats and inciting gender-based violence, including threats of physical and/or sexual violence, rape, killing, unwanted and harassing online communications, or even the encouragement of others to harm women physically.

Addressing online violence against women for the first time in an official UN report, Dubravka Šimonovic, the then-UN Special Rapporteur, presented her report to the HRC and argued that " online and ICT-facilitated forms of violence against women have become increasingly common, particularly with the use, every day and everywhere, of social media platforms and other technical applications. " [44] The Special Rapporteur called for " due diligence " on the part of businesses to eliminate online violence against women and address the phenomenon of violence against women facilitated by new technologies and digital spaces from a human rights perspective. She posited the interrelated rights to live a life free from violence to freedom of expression, to privacy, to have access to information shared through information and communications technology (" ICT "), and other rights.

Addressing the widespread and systemic structural discrimination and gender-based violence against women and girls, facilitated by new types of gender-based violence and gender inequality in access to technologies, which hinder women's and girls " full enjoyment of their human rights and their ability to achieve gender equality, she acknowledged that the vernacular in this area is still developing and not univocal. The Special Rapporteur referred to " online violence against women " as a more user-friendly expression but also used the terms " cyberviolence " and " technology-facilitated violence. " While the report argued the principle that human rights protected offline should also be protected online, it is now obvious that offline bleeds into online and vice versa.

Given the significant role played by technology companies in facilitating the enjoyment of digital human rights, including online free speech, online privacy, and the right to be forgotten, it is hardly surprising that human rights officials, such as the UN Special Rapporteurs for Freedom of Expression and Privacy, have turned their attention increasingly towards the regulatory role of governments vis-à-vis technology companies. [45]

The HRC Committee has had the opportunity to review the matter of export of digital products manufactured by private companies in its review of Italy in 2017. The Committee expressed concern about :

" Allegations that companies based in the State party have been providing online surveillance equipment to Governments with a record of serious human rights violations and about the absence of legal safeguards or oversight mechanisms regarding the export of such equipment. " [46]

It recommended that " measures are taken to ensure that all corporations under its jurisdiction, in particular technology corporations, respect human rights standards when engaging in operations abroad. " The matter of export controls relating to surveillance technology has also been taken up by the UN Special Rapporteur on Freedom of Expression, who has reported on the harmful effects on political expression of resort by governments to spyware programs and called for a moratorium on the export of such technology. [47]

The HRC has examined digital forms of violence and reaffirmed that the violence against women in digital contexts is a growing concern and emphasized the need to address systemic gender-based discrimination through effective responses in accordance with human rights. [48] Resolution 38/5 underscored the multi-jurisdictional and transnational nature of violence against women and girls in digital contexts, calling for active cooperation among different actors (States and their law enforcement and judicial authorities, and private actors) to detect, report, and investigate such crimes. [49] It also highlighted the critical role that digital technology companies, especially Internet service providers and digital platforms, have in ameliorating the damage caused by digital violence. [50]

In 2012, the HRC declared that " the same rights that people have offline must also be protected online, " [51] and in 2015, recognized that domestic violence could include acts such as cyberbullying and cyberstalking. [52] The UN General Assembly acknowledged,

42. HRC Committee, Concluding Observations in the Fourth Periodic Report of the U.S.A., [para] 22, U.N. Doc, CCPR/C/USA/CO/4 (2014) (emphasis added). The extra-territorial use of drones was another topic discussed in the same US periodic review session.
43. Vienna Declaration and Programme of Action, U.N. Doc. A/CONF.157/23 (July 12, 1993).
44. Dubravka Šimonovic (Special Rapporteur on Violence Against Women, Its Causes and Consequences), Rep. on Online Violence Against Women and Girls From a Human Rights Perspective, U.N. Doc. A/HRC/38/47 (June 18, 2018).
45. *See e.g.*, Irene Khan (Special Rapporteur on the Freedom of Opinion and Expression), *Rep.*, at 18 [para] [para] 90-91, U.N. Doc. A/HRC/47/25 (Apr. 13, 2021) ; David Kaye (Special Rapporteur on the Freedom of Opinion and Expression), *Rep.*, at 22 [para] 57, U.N. Doc. A/74/486 (Oct. 9, 2019).
46. Human Rights Committee, Concluding Observations on the Sixth Periodic Report of Italy, 36, U.N. Doc. CCPR/C/ITA/CO/6 (2017).
47. *See e.g.*, Special Rapporteur on the Freedom of Opinion and Expression, *Rep.*, at 14-15, 48-49, U.N. Doc. A/HRC/41/35 (May 28, 2019).
48. HRC Res. 38/5, U.N. Doc. A/HRC/RES/38/5 (July 4, 2018).
49. *Id.* at [para] 11.
50. Id. at [para] 10(d). (calling for States to " strengthen or adopt positive measures, including internal policies, to promote gender equality in the design, implementation and use of digital technologies with a view to eliminating violence against women and girls, and to refrain from presenting women and girls as inferior beings and exploiting them as sexual objects.... ").
51. HRC Res. 20/8, U.N. Doc. A/HRC/RES/20/8, at [para] 1 (July 5, 2012).
52. HRC Res. 29/14, U.N. Doc. A/HRC/RES/29/14, at [para] 4 (July 22, 2015).

just a year later, that women were particularly affected by violations of the right to privacy in the digital age and called upon all States to further develop preventive measures and remedies. [53] The HRC reaffirmed this call again in 2017, noting that abuses of the right to privacy in the digital age may affect all individuals, with particular effects on women, children and marginalized groups. [54]

B. - Mining the CEDAW and Regional Treaties

11 - As the only universal and widely ratified bill of rights for women, the Convention on the Elimination of Discrimination against Women (" CEDAW ") is the most authoritative treaty to combat technologically facilitated violence against women. General Recommendation No. 35, which builds on CEDAW General Recommendations No. 19, can be a tool to combat pornographic deepfakes internationally. General Recommendation No. 35 refers specifically to digital forms of gender-based violence and provides a comprehensive list of measures for State parties to support prevention, protection, prosecution, punishment, and reparations of digital gender-based violence, points that could easily translate to a national strategy to combat deepfakes. [55] For prevention, the Committee recommended that State parties " adopt and implement effective legislation and other appropriate measures to address the underlying cause of gender-based violence. " [56] General Recommendation No. 35 represents preliminary steps by the CEDAW Committee to address digital gender-based violence and frequently neglected negative consequences arising from technological advancements. [57] This sentiment raises a broader inquiry if there should be a new CEDAW Committee general recommendation that addresses AI-driven gender-based violence, which has been largely under-analyzed through the lens of women's rights.

Furthermore, the Declaration on the Elimination of Violence Against Women's recognition " that violence against women is a manifestation of historically unequal power relations between men and women, which have led to domination over and discrimination against women by men and to the prevention of the full advancement of women " provides us with a strong conceptual framework for the understanding of algorithmic bias.

Regional treaties on women's rights such as the Maputo Protocol [58] and the Belem Do Para treaty [59] are silent on technology facilitated violence against women. However, the Secretariat of the Violence Against Women Division of the Council of Europe, published a paper titled " Protecting women and girls from violence in the digital age – The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women. " The Budapest Convention addresses directly and indirectly some types of cyberviolence against women. [60]

C. - Domestic Frameworks

1° Korean Legal System Reform

12 - In response to the Nth Room case which ripped apart the veiled world of online violence [61], the Korean National Assembly has enacted a series of amendments to various legislative acts, including the Criminal Act, Act on Special Cases Concerning the Punishment of Sexual Crimes, Act on Regulation and Punishment of Criminal Proceeds Concealment, Act on the Protection of Children and Youth Against Sex Offenses, Act on Promotion of Information and Communications Network Utilization and Information Protection, and the Telecommunications Business Act. [62]

One key amendment to the Criminal Act involves Article 305, which now stipulates that individuals aged nineteen or older who engage in sexual intercourse or indecent acts with individuals aged thirteen or older but under sixteen shall be subject to punishment. [63] This amendment raises the age at which consent can be given for statutory rape from thirteen to sixteen years, thereby enhancing the protection of minors. [64]

Another significant amendment to the Criminal Act introduces a new provision making individuals who prepare or conspire with the intent to commit rape, [65] imitative rape, [66] or quasi-rape [67] are liable to imprisonment with labor for a maximum period of three years.

However, concerns have been raised regarding the adequacy of punishments in cases like the Nth Room, where the primary evidence consisted of self-taken images and footage shared in chatrooms. These concerns stem from the difficulty in establishing conclusive proof that the violence and threats inflicted on over seventy victims through chat messages resulted in the actual crimes

53. G.A. Res. 71/199, U.N. Doc. A/RES/71/199, at [para] 5(g) (Dec. 19, 2016).
54. HRC Res. 34/7, U.N. Doc. A/HRC/RES/34/7 (Apr. 7, 2017).
55. CEDAW, General Recommendation No. 35 (2017) on gender-based violence against women, updating general recommendation No. 19 (1992), U.N. Doc. CEDAW/C/GC/35 (July 26, 2017). (" Gender-based violence against women occurs in all spaces and spheres of human interaction, whether public or private... and the redefinition of public and private through technology-mediated environments, such as contemporary forms of violence occurring online and in other digital environments. ")
56. *Id.*
57. *Id.* (" Gender-based violence against women, whether committed by States, intergovernmental organizations, or non-State actors, including private persons... It manifests itself on a continuum of multiple, interrelated and recurring forms, in a range of settings, from private to public, including technology-mediated settings... ").
58. Protocol to the African Charter on Human and Peoples " Rights on the Rights of Women in Africa, better known as the Maputo Protocol, is an international human rights instrument established by the African Union.
59. Inter-American Convention on the Prevention, Punishment, and Eradication of Violence against Women, better known as the Belém do Pará Convention.
60. In fact, in March 2019, the Committee of Ministers of the Council of Europe adopted a new recommendation on preventing and combating sexism that contains a seminal definition of sexism, including online and via new technologies, Sexism is defined as : " Any act, gesture, visual representation, spoken or written words, practice or behaviour based upon the idea that a person or a group of persons is inferior because of their sex, which occurs in the public or private sphere, whether online or offline, with the purpose or effect of : I. violating the inherent dignity or rights of a person or a group of persons ; or II. resulting in physical, sexual, psychological or socio-economic harm or suffering to a person or a group of persons ; or III. creating an intimidating, hostile, degrading, humiliating or offensive environment ; or IV. constituting a barrier to the autonomy and full realisation of human rights by a person or a group of persons ; or V. maintaining and reinforcing gender stereotypes. "
61. The Nth Room case (2020) involved an infamous network of chatrooms in the Telegram messaging app, women and girls in South Korea were blackmailed and coerced into sharing non-consensual images of sexual acts. The police identified approximately 1,100 women and girls who were victims of this network. The two most infamous of these chatrooms were the Nth Room (which refers to any one of eight different chat rooms) and the Doctor's Room. In both rooms, women and girls-some of them middle-school age-were deceived and coerced into uploading sexually explicit photos and videos of themselves to Telegram, which were then sold and shared in chatrooms with up to tens of thousands of users. The victims were often ordered to film themselves performing lewd acts under the threat that noncompliance would result in the release of the content to their families and-in the case of minors-their educational institutions.
62. Wonchul Kim, *'Nth Room Prevention Law " Passed : Imprisonment For Up to 3 Years For Possessing or Viewing Sexual Exploitation Media*, Hankyoreh (Apr. 29, 2020), https ://www.hani.co.kr/arti/politics/assembly/942627.html.
63. Hyeongsabeob [Criminal Act] art. 305(2), partially amended by Act. No. 17572, Dec. 8, 2020 (S.Kor.).
64. *Id.*
65. *Id.* at art. 297. (" [A] person who, by means of violence or intimidation, has sexual intercourse with another shall be punished by imprisonment with labor for a limited term of at least three years. ").
66. *Id.* at art. 297-2. (" A person who, by means of violence or intimidation, inserts his or her sexual organ into another's bodily part (excluding a genital organ), such as mouth or anus, or inserts his or her finger or other bodily part (excluding a genital organ) or any instrument into another's genital organ or anus shall be punished by imprisonment with labor for a limited term of at least two years. ").
67. *Id.* at art. 299. (" A person who has sexual intercourse with another or commits an indecent act on another by taking advantage of the other's condition of unconsciousness or inability to resist shall be punished in accordance with [rape, imitative rape, and indecent act by compulsion]. ").

listed in the provision. [68] Therefore, it is necessary to carefully examine the evidence and ascertain whether the existing legal framework adequately addresses the offenses committed in cases like the Nth Room, particularly with regards to the connection between the violence inflicted and the specific crimes specified in the aforementioned provision.

In response to the imperative of preventing crimes resembling the Nth Room case, the Act on Special Cases Concerning the Punishment of Sexual Crimes also underwent notable reform. These amendments introduced significant changes to the penalties associated with various offenses, including special rape, [69] aggravated rape, indecent act by compulsion against minors under the age of thirteen, and indecent acts in crowded places. [70]

One salient modification pertains to special rape, for which the penalty has been enhanced to imprisonment with labor for an indefinite term or for a minimum of seven years, in contrast to the previous minimum of five years. [71] Similarly, the penalty for aggravated rape has been raised from five to seven years. [72], [73] In the case of indecent act by compulsion against minors below the age of thirteen, the relevant provision has been revised to eliminate the previous fine range of thirty to fifty million won (30,000 to 50,000 USD), replacing it with a penalty of imprisonment with labor for a minimum term of five years. [74], [75] Regarding indecent acts in public settings, the amendment remains unchanged (not exceeding three million won) but the amendment now allows for imprisonment of up to three years as an alternative, compared to the former maximum sentence of one year. [76], [77]

Furthermore, an amendment of particular significance concerns Article 13, which addresses obscene acts through communication media. [78] The revised provision encompasses the transmission of any words, sounds, writings, pictures, images, or other materials that may induce a sense of sexual shame or aversion, with the intent to arouse or satisfy the sender's or recipient's sexual urges. Violators are now subject to imprisonment with labor for a maximum of two years or a fine not exceeding twenty million won (20,000 USD). [79] This represents a departure from the previous arrangement, where the same act warranted a comparable period of confinement but entailed a maximum fine of five million won (5,000 USD). [80]

While substantial and noteworthy amendments have been made to provisions concerning the production and dissemination of sexually exploitative media, it is important to note that the language of the Act still lacks the nuanced recognition that the victims are, indeed, victims of exploitation. Although the penalties have been augmented for the filming and distribution of sexually exploitative photographs and videos taken without the subject's consent, the description of such materials as capable of causing " sexual stimulus or shame " fails to acknowledge the exploitative nature of these images. [81] In contrast, the Children and Youth Sex Offense Protection Act explicitly designates victimizing videos as sexually exploitative material, thereby recognizing the victims as victims of exploitative crimes. [82] The Act on Special Cases Concerning the Punishment of Sexual Crimes, primarily applied to cases involving adult victims, falls short in fully acknowledging adult victims as victims. [83] Consequently, the lack of complete recognition of adult victims as victims serves as evidence that existing attitudes within courts and investigative authorities have not undergone significant improvement.

Moreover, the Act clarifies that individuals who distribute sexually exploitative photographs or videos obtained without the subjects " consent, even if the subjects themselves took the images, will be subject to punishment. [84] Additionally, those who seek to profit from the illicit filming or dissemination of such photographs will face imprisonment for a specified term, which now surpasses the previous maximum sentence of seven years. [85], [86]. Furthermore, the revised law expands the scope of legal action to include individuals in possession of, purchasing, storing, or viewing illegally obtained sexual photographs or videos, whereas previously only those involved in distribution, sale, leasing, or provision of illicit footage were liable to punishment. [87]

In addition to these modifications, several newly introduced provisions deserve attention. They maintain that a person intimidates another person by using photograph or its duplicates (including a duplicate of the duplicate) which may cause sexual desire or shame shall be punished by imprisonment for at least one year and that any person who interferes with the exercise of a person's right by intimidation or has the person to the work not obligatory for him/her shall be punished by imprisonment with labor for at least three years. [88] Another provision states that individuals who plan or conspire with the intention of committing rape or sexual assault can now be subjected to a maximum of three years of imprisonment, even if they did not directly perpetrate the crime. These newly inserted provisions specifically aim to address the methods employed in the Nth Room case, wherein victims were coerced through the use of their own photos, and to hold lower-level administrators accountable for their role in facilitating the operations of higher-level administrators such as Cho or Moon in establishing the illicit chat rooms. Nonetheless, a critical question remains regarding the prosecution of bystanders whose actions may not amount to the level of planning or preparation for rape or sexual assault against the victims, despite their presence in the chat rooms and their failure to intervene, thereby contributing to the perpetuation of the sex slave network.

The Act on Regulation and Punishment of Criminal Proceeds Concealment underwent significant amendments, introducing several new provisions including Article 10-4, which establishes guidelines for calculating the criminal proceeds associated with cybersex crimes. [89] Article 10-4 stipulates that the criminal proceeds acquired by the offender during the commission of the

68. Kim, *supra* note 62.
69. Seongpongnyeokcheobeolbeop [Act on Special Cases Concerning the Punishment of Sexual Crimes 2020] art. 3, partially amended by Act. No. 17507, Oct. 20, 2020 (S.Kor.). (" A person commits special rape if they commit rape, imitative rape, indecent act by compulsion, quasi-rape, or quasi-indecent act by compulsion in the course of committing intrusion upon habitation, compound larceny, special larceny, or attempt of larceny or robbery. ").
70. *Id.* at art. 3(1), 4(1)-(2), 7(3) & 11.
71. *Id.* at art. 3(1).
72. *Id.* at art. 4(1).
73. Seongpongnyeokcheobeolbeop [Act on Special Cases Concerning the Punishment of Sexual Crimes 2019] art. 3(1), partially amended by Act. No. 16445, Aug. 20, 2019 (S.Kor.).
74. *Id.* at art. 7(3).
75. Act on Special Cases Concerning the Punishment of Sexual Crimes 2020, at art. 7(3).
76. *Id.* at art. 11.
77. Act on Special Cases Concerning the Punishment of Sexual Crimes 2019, at art. 11.
78. Act on Special Cases Concerning the Punishment of Sexual Crimes 2020, at art. 13.
79. *Id.*
80. Act on Special Cases Concerning the Punishment of Sexual Crimes 2019, at art. 13.
81. Act on Special Cases Concerning the Punishment of Sexual Crimes 2020, at art. 14.
82. Go-eun Park, *" You Remove It But It Keeps Coming Back " : New Laws Leave Adult Digital Sex Crime Victims Little Recourse*, Hankyoreh (Dec. 12, 2021), https ://english.hani.co.kr/arti/english_edition/e_national/1022931.html.
83. *Id.*
84. Act on Special Cases Concerning the Punishment of Sexual Crimes 2020, at art. 13.
85. Act on Special Cases Concerning the Punishment of Sexual Crimes 2019, at art. 14(3).
86. Act on Special Cases Concerning the Punishment of Sexual Crimes 2020, at art. 14(3).
87. *Id.* at art. 14(4).
88. *Id.* at art. 14(3).
89. Beomjoesuigeunnikgyujebeop [Act on Regulation and Punishment of Criminal Proceeds Concealment] art. 10-4, partially amended by Act. No. 17263, May 19, 2020 (S.Kor.).

crime shall be presumed as the illicit gains, taking into account factors such as the amount of the proceeds, the timing of property acquisition, and other relevant circumstances ; if there is a reasonable possibility that the criminal proceeds were obtained through the perpetration of the same crime, they shall be presumed as the proceeds related to that particular offense. [90] This amendment carries significant implications as it addresses the historical challenge of establishing a direct correlation between cybersex crimes and the profits generated, thereby facilitating the seizure of criminal proceeds. [91] By easing the burden of proof, these new provisions enable a more effective demonstration of the relationship between these crimes and the associated criminal profits. [92]

The Act on the Protection of Children and Youth Against Sex Offenses have also been revised, marking a crucial milestone in safeguarding minors from cyber violence against women and girls (" VAWG "). Particularly significant is the alteration of the term " child and adolescent pornography " to " child and adolescent exploitation material. " [93] This revision represents an important shift in recognizing the vulnerability and protection needs of minors affected by cyber VAWG. [94]

The Act on the Protection of Children and Youth Against Sex Offenses encompasses notable enhancements in penalties concerning the production and distribution of child and adolescent exploitation material. These amendments are accompanied by provisions for imposing aggravated punishment on repeat offenders, thereby emphasizing the gravity of such offenses. [95] An admirable initiative has been introduced, wherein individuals who report crimes related to this matter are eligible to receive cash prizes. [96] This commendable provision not only serves as an incentive to promote the welfare of minors but also offers investigative authorities an additional avenue for combating the sexual exploitation of children. However, it is important to acknowledge that the effectiveness of this new cash prize provision in detecting and preventing cyber VAWG may be hindered by the low rate of prosecutions for digital sex crimes and the lenient nature of punishments, as highlighted by the CEDAW Committee in 2018. [97] Consequently, careful monitoring of the provision's impact is crucial for evaluating its efficacy in addressing this issue.

Furthermore, a significant addition to the Act is found in Article 7-6, which specifies that individuals involved in the preparation or conspiracy to commit crimes such as rape or indecent act by force against children and adolescents can be subjected to a maximum imprisonment term of three years. [98] This particular provision aims to proactively prevent such offenses by deterring potential perpetrators.

In relation to the Act on Promotion of Information and Communications Network Utilization and Information Protection, a noteworthy legislative measure known as the Deepfake Prevention Law was passed during the National Assembly plenary session, introducing several amendments to the act. [99] Primarily, the amendment mandates the Ministry of Science and ICT to actively promote the development and dissemination of technologies capable of accurately identifying false audio and visual content. [100]

Moreover, an additional provision has been incorporated into the act, requiring information and communication service providers to designate a responsible individual accountable for preventing the distribution of illegal filming material. [101]

Regarding the Telecommunications Business Act, its revision now compels internet service providers to promptly remove sexually exploitative images as defined in Article 14 of the Special Act on Punishment of Sexual Crimes. [102] Nonetheless, despite this amendment, the law still exhibits two significant loopholes : it 1) vaguely defines the " technical and managerial " measures providers are meant to take [103] and 2) is enforceable only for open online forums, allowing offenders to circumvent the law by using private forums instead. [104] These loopholes necessitate urgent attention and rectification to ensure its effectiveness in combating the proliferation of sexually exploitative content.

2° Other Legal Frameworks

13 - The new regulatory developments in the field of AI (such as the Draft EU AI Regulations and the White House's blueprint for an AI Bill of Rights of 2022) show that as digital technology becomes ubiquitous, it will be impossible to regulate it in isolation to other bodies of domestic, regional, and international law. [105] Although not exhaustive, this section maps laws which attempts to address coded gender-based violence in different ways so as to understand how States are attempting to tackle this continually emerging forms of coded gender-based violence. I examine recent reformist agendas in different jurisdictions. In the UK, the Crown Prosecution Service on online violence against women has recommended :

> The landscape in which VAWGCrimes are perpetrated is changing. The use of the Internet, social media platforms, emails, text messages, smartphone apps (for example, WhatsApp and Snapchat), spyware and GPS (Global Positioning System) tracking software to commit VAWG offences is rising. Online activity is used to humiliate, control and threaten victims, as well as to plan and orchestrate acts of violence. [106]

The South African government explicitly acknowledged online gender-based violence in the National Strategic Plan on Gender-Based Violence and Femicide. [107] In the plan, the South African government announced plans to conduct studies on the impact of online violence against women and roll out cyber violence awareness programs and strategies to respond to online gender-based violence.

On December 21, 2020, Lebanon became the first Arab country to pass a law criminalizing online sexual harassment. The law also

90. *Id.*
91. Kim, *supra* note 62.
92. *Id.*
93. Cheongsonyeonseongbohobeop [Act on the Protection of Children and Youth Against Sex Offenses] art. 2(5), 12 & 17, partially amended by Act. No. 17352, June 9, 2020 (S.Kor.).
94. Park, *supra* note 82.
95. Act on the Protection of Children and Youth Against Sex Offenses, at art. 11.
96. Act on the Protection of Children and Youth Against Sex Offenses, at art. 59(1).
97. CEDAW, *Concluding Observations on the Eighth Periodic Report of the Republic of Korea*, [para] 22(c), CEDAW/C/KOR/CO/8 (Mar. 14, 2018).
98. Act on the Protection of Children and Youth Against Sex Offenses, at art. 7-6.
99. Jeongbotongsinmangbeop [Act on Promotion of Information and Communications Network Utilization and Information Protection] art. 4-2, partially amended by Act. No. 17358, June 9, 2020 (S.Kor.).
100. *Id.*
101. Act on Promotion of Information and Communications Network Utilization and Information Protection, at art. 44-9 & 76-2.
102. Jeongitongsinsaeopbeop [Telecommunications Business Act] art. 22-5(1), amended by Act. No. 17460, June 9, 2020 (S.Kor.).
103. *Id.* at art. 22-5(2).
104. Eun-Jee Park, *[MAGNIFYING GLASS] Rushed " Nth Room Law " Unlikely to Actually Stop Criminals*, Korea JoongAng Daily (June 2, 2020), https ://koreajoongangdaily.joins.com/2020/06/02/business/indepth/Nth-room-digital-crime-Naver/20200602195600193.html.
105. In 2013, only three U.S. states had revenge porn laws, and a decade later, 48 states do, plus Washington, D.C., Puerto Rico, and Guam. In 2023, three US states (Virginia, Texas, and California) adopted laws on deepfakes. There are significant examples of successful prosecutions in different jurisdictions of such crimes, which could extend to images that have " been altered to appear to show a person's private parts, or a person engaged in a private act, in circumstances in which a reasonable person would reasonably expect to be afforded privacy, " as legislation in Australia recently established.
106. *Social Media and Other Electronic Communications*, Crown Prosecution Service (Jan. 9, 2023), https ://www.cps.gov.uk/legal-guidance/social-media-and-other-electronic-communications.
107. Republic of S. Afr., National Strategic Plan on Gender-Based Violence & Femicide (Mar. 11, 2020). (" Online violence refers to any act of gender-based violence against a woman that is committed, assisted or aggravated in part or fully by the use of [ICT], such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately. ")

encompasses harassment that takes place online through social media and other technological mediums. Perpetrators may spend up to four years in prison and pay fines up to fifty times the minimum wage. Despite the importance of the law, there is ambiguity in the laws as to who is deemed a perpetrator and whether platforms could be held responsible for the offense.

In 2014, the Australian Protection from Harassment Act (" POHA ") 2014 extended the substantive definition of harassing behavior to include electronic means and provided more comprehensive protection orders for victims outside intimate relationships. As such, victims are potentially able to obtain a protection order from the courts, after their images have been shared without consent.

In Singapore, the 2014 Protection from Harassment Act focuses on online harassment and prohibits the intentional or reckless issue of a communication that is threatening, abusive or insulting, which is heard, seen or otherwise perceived and likely to harass or cause alarm or distress or instill in a person fear or provoke violence. A 2019 amendment " prohibits the publication of information identifying the victim or a person related to the victim to harass, threaten or facilitate violence against the victim (also known as " doxing. ") "

The Philippines's 2018 Safe Spaces Act defines gender-based online sexual harassment as :

> Any conduct targeted at a particular person that causes or is likely to cause another mental, emotional or psychological distress ; and fear of personal safety ; sexual harassment acts, including unwanted sexual remarks and comments ; threats ; uploading or sharing of one's photos without consent ; video and audio recordings ; cyberstalking and online identity theft.

However, this definition does not include social media platforms, gaming and similarly to South Africa, does not include new forms of AI and synthetic media.

In 2019, the Philippines amended the Anti-Violence Against Women and Their Children Act of 2004 (" Anti-VAPC Law ") to include ICT-related violence. [108] Under the amendment, ICT violence such as " hacking of personal accounts on social media, the use of location data from electronic devices, fabrication of fake information or news through text messages or other cyber, electronic, or multimedia technology " falls under violence against partners and children. The House of Representatives of the Philippines passed House Bill No. 8009 in May 2023 ; the bill will further expand the Anti-VAPC Law to define ICT-related violence as " any act of omission involving the use or exploitation of data or any form of ICT which causes or is likely to cause mental, emotional, or psychological distress or suffering to the woman and/or her children. " [109] The bill expands protection measures to include " the immediate blocking, blacklisting, removal, or shutdown of any upload, program, or application that causes or tends to cause violence against a woman and/or her children. "

The Cyberspace Administration of China (" CAC "), the national Internet regulator and censor for the PRC, has acknowledged cyberviolence in regulatory actions such as the November 2022 Notice on Effectively Strengthening the Governance of Cyber Violence. [110] In the notice, the CAC describes cyberviolence as " publishing illegal information such as insults, slander, privacy violations, and other unfriendly information against individuals, infringing on the legitimate rights and interests of others, and disrupting the normal order of the Internet. "

In April 2023, the CAC proposed Measures for the Administration of Generative Artificial Intelligence Services to address rising issues in generative AI. [111] The proposal places responsibility on generative AI providers (" organizations and individuals that use generative AI to provide services such as chat and text, image, and sound generation ") as producers of the content generated by their products, heightening the responsibility of providers as they can be held responsible for content created by users of their tools. In addition, generative AI providers assume statutory responsibility of personal information processors when personal information is involved, which confers a duty to protect personal information. Generative AI providers would also be required to take measures to prevent false information and discrimination based on characteristics including gender. However, the proposal does not define ways in which generative AI may discriminate based on gender. The proposal also protects personal information of individuals from being used without consent and requires providers to guide users to not use the generated content to damage the image and reputation of others. Providers found in violation of the proposal are subject to punishment according to relevant law, such as the Personal Information and Protection Law of the People's Republic of China.

In 2020, South Korea introduced the Framework Act on Intelligent Informatization, a social impact assessment on intelligent informatization services, including AI. [112] State and local governments assess the intelligent informatization services on safety and reliability as well as impacts on information culture, society, and the economy. However, this assessment was introduced only in the public sector ; there is no similar regime for the private sector. The assessment is also limited to general impact on society and individuals' personal information and does not assess discrimination or bias against women.

In response to the death of a female actor following online insults, Japan revised its Penal Code in June 2022 to mandate jail time for up to a year or a fine up to 300,000 yen (approximately $2,150) for online insults (when an individual has insulted another in the public sphere to damage their social reputation). [113] The revision also extended the statute of limitations to three years. However, the Penal Code makes no special provisions for online VAWG.

In 2020, the Law on Women's Access to a Violence-Free Life in Mexico City was amended to extend the notion of violence against women to include any acts carried out through information and communication technologies that threatens the integrity, dignity, intimacy, freedom, and private life, of women or causes psychological, physical, economic or sexual harm or suffering, both in the private and public spheres, as well as any act that causes nonmaterial loss to them and/or their families. Following an increase in online attacks on journalists, Spain developed protocols to provide procedures for journalists' complaints, assessment of online harassment complaints by the newspaper's social media team including the withdrawal of comments from social media platforms, and referral to legal counsel and human resources for the purpose of filing legal actions. Despite these good intentions there is little information on what follow up action has been taken in the aftermath of the passage of this protocol.

108. An Act Amending R.A. No. 9262, Rep. Act. No. 4888 (Sept. 30, 2019) (Phil.), https ://hrep-website.s3.ap-southeast-1.amazonaws.com/legisdocs/basic_18/HB04888.pdf.

109. Jean Mangaluz, *House Bill Defining Online Abuse vs Women, Children Hurdles Final Reading*, Inquirer (May 22, 2023, at 11 :43 PM), https ://newsinfo.inquirer.net/1772911/bill-defining-online-abuse-against-women-and-children-hurdles-final-reading-in-house.

110. *Notice on Effectively Strengthening the Governance of Cyber Violence*, Office of the Central Cyberspace Affairs Commission (Nov. 4, 2022, at 19 :10), http://www.cac.gov.cn/2022-11/04/c_1669204414682178.htm.

111. Notice of the Cyberspace Administration of China on Public Comments on the " Administrative Measures for Generative Artificial Intelligence Services (Draft for Comment) ", Office of the Central Cyberspace Affairs Commission (Apr. 11, 2023, at 12 :51), http://www.cac.gov.cn/2023-04/11/c_1682854275475410.htm.

112. Jeong Jonggu, *Introduction of the First AI Impact Assessment and Future Tasks : South Korea Discussion*, 11 Laws 73 (2022).

113. *Japan Introduces Jail Time, Tougher Penalties for Online Insults*, Kyodo News (July 7, 2022, at 00 :004), https ://english.kyodonews.net/news/2022/07/1590b983e681-japan-to-introduce-jail-time-tougher-penalties-for-online-insults.html.

The 2022 reauthorization of the United States Violence Against Women Act (" VAWA "), 1994 (As Amended) Subtitle M-Strengthening America's Families by Preventing Violence Against Women and Children included :

> [E]stablishing a federal civil cause of action for individuals whose intimate visual images are disclosed without their consent, allowing a victim to recover damages and legal fees ; creating a new National Resource Center on Cybercrimes Against Individuals ; and supporting State, Tribal, and local government efforts to prevent and prosecute cybercrimes, including cyberstalking and the nonconsensual distribution of intimate images.

This new provision in the reauthorization of the VAWA is welcome and helps build the law as a living document which needs to dynamically address new forms of violence that have been given name to, since its first adoption in 1994.

Apart from national efforts, there are supranational and multinational effort to address online harassment and abuse. The U.S., together with Denmark, Australia, the U.K., and Sweden, launched the Global Partnership for Action on Gender-Based Online Harassment and Abuse during the 2022 meeting of the UN Commission on the Status of Women. [114] This multinational initiative will align countries, international organizations, and civil society to prioritize, understand, and address technology-facilitated gender-based violence.

Although not all forms of isolated acts of technology driven gender-based violence can meet a legal threshold, we need to see them as parts of a continuum of violence against women and underrepresented groups. The 2020 case of Buturuga v. Romania [115] was the first case in which the European Court of Human Rights recognized technology facilitated privacy invasion by an ex-spouse as a form of violence. Violence against women as coercive control needs to be framed through the strengthening of human rights standards and critical information theory. Much like how in the 1970's legal advocates named the field of domestic violence, technology facilitated violence against women must be named so legal remedies can be created for those affected by this offense.

CONCLUSION : NEW DIRECTIONS

14 - Given the rapid growth of technologies, we have entered a new cultural moment, where LLMs and generative AI have the potential to reshape the way we learn, engage, and interact. This moment gives us pause to question whether law has the capacity and agility to keep pace with the ever-changing parade of new technology and their potential to be misused as tools of coded violence against women. I turn in this section to two broad based recommendations.

First, how can Environment, Social and Governance (" ESG ") activities help in addressing digital violence ? The focus on ESG activities has been dubbed the " new paradigm for business. " The corporate social responsibility movement, a forerunner to ESG, spurred the U.S. to enact the Comprehensive Anti-Apartheid Act of 1986, which imposed sanctions and prohibited U.S. nationals from making any new investments in South Africa during the apartheid regime. [116] Similarly, the ESG movement must spark transformative action on ending gender inequality. One way to do this is to mainstream women's human rights norms into ESG. The CEDAW is an inalienable standard of conduct whereby businesses are held accountable to rights violations with corresponding remedies for restitution. However, even when mainstreamed into ESG, these rights must be upheld regardless of their value for business success.

Recent momentum on the " S " in ESG was spurred by the 2018 #MeToo anti-sexual harassment movement and provides a narrative arc for the integration of international women's human rights and intersectional rights into ESG. The 2020 Black Lives Matter movement further shined a spotlight on diversity, equity, and inclusion, as did the Stop Asian Hate movement. The confluence of the global public reckoning on social justice with the COVID-19 pandemic has increased renewed awareness and attention of the role of business in inclusion and human rights.

One way in which investors have tried to address institutional sexism is by putting pressure on corporations to select diverse directors on their Boards. In 2021, the Nasdaq Stock Exchange received approval from the U.S. SEC to adopt a Board Diversity Rule, a disclosure standard designed to encourage a minimum board diversity objective for companies and provide stakeholders with consistent, comparable disclosures concerning a company's current board composition. Having more women on boards in technology companies may drive emerging technologies to address the impact of new technologies on women.

Moreover, recently, the UN OHCHR B-Tech Project released guidance in rights respecting investment in digital technology companies in 2021. [117] This would help incentivize tech innovators to develop codes of ethics for AI and other new technologies that uphold the primacy of women's human rights. The same year saw UNESCO adopting Recommendations on the ethics of AI. The Recommendations call for guardrails and impact assessments and recognize that the rapid rise of AI creates great promise in many areas, including in healthcare, education and climate change, but also raises profound ethical concerns of human rights violations. [118] A human rights-based approach that also includes the Guiding Principles on Business and Human Rights is an important tool to evaluate the effectiveness of these new guidelines.

Although the business case for gender equality is now well recognized, I argue that the CEDAW and women's rights are inalienable and must be guaranteed regardless of their value to the business case. I argue for a more prescriptive and less indeterminate idea of international women's human rights in business. The CEDAW calls upon states to hold business entities accountable to women's human rights. In fact, CEDAW's Article 2(e) calls upon states parties to " take all appropriate measures to eliminate discrimination against women by any person, organization or enterprise[.] " [119]

Second, for a newer understanding of solutions, I turn yet again to the role of Critical Information Theory. Although not mentioned by name, this theory is alluded to in the submission by the " Internet Democracy Project " on online violence against women in India to then-UN Special Rapporteur on Violence against Women, Dubravka Šimonovic. The Project recommended that what was needed was not more laws but more discourse to address online violence :

> What is primarily needed in India, therefore, is more discourse, more awareness and a variety of non-legal measures, so as to challenge and ultimately displace these socio-cultural norms. We believe that measures to tackle online abuse must go

114. Press Release, U.S. Dept. of State, 2023 Roadmap for the Global Partnership for Action on Gender-Based Online Harassment and Abuse (Mar. 28, 2023), https ://www.state.gov/2023-roadmap-for-the-global-partnership-for-action-on-gender-based-online-harassment-and-abuse/.
115. European Court of Human Rights, Buturuga c. Roumanie, n° 56867/15, 11 February 2020, BUTURUGA c. ROUMANIE (coe.int).
116. Comprehensive Anti-Apartheid Act of 1986, Pub. L. No. 99-440, 100 Stat. 1083 (1986).
117. U.N. Hum. Rts. Off. of the High Comm'r, Rights-Respecting Investment in Technology Companies (Jan. 2021), https ://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/B-Tech-Briefing-Investment.pdf.
118. *UNESCO's Recommendation on the Ethics of Artificial Intelligence : key facts* (June 1, 2023), https ://unesdoc.unesco.org/ark :/48223/pf0000385082.
119. G.A. Res. 34/180, Convention on the Elimination of All Forms of Discrimination Against Women, art. 2 (Dec. 18, 1979).

> hand-in-hand with measures to protect women's expression. [120]

This comment raises several important points : first, that discourse on the threats of coded gender-based violence is as important as new laws to address the challenge ; second, that measures to combat online violence must co-exist with the protection of women's freedom of expression rather than with the forced removal of women from the online space.

In balancing this nuanced argument, I would argue that new gender-based violence laws address the orthodoxy of gender-related power relations as a structural or root cause of violence. For example, Nicaragua's Comprehensive Act on Violence against Women and the Reform on Criminal Code (Act No. 641) call for " an education that eliminates the stereotypes of male supremacy and the macho patterns that generated their violence. " [121]

In the final analysis, the idea of digital gender-based violence gives rise to the assumption that algorithms are mathematical models and outside of the control of human behavior. That is far from the truth.

Gender bias in algorithms developed by mostly male technologists drive the programs and platforms that reproduce and reinforce violence against women and recreate a vicious feedback loop. To break this misogynistic cycle of coded violence, we need both law reform and cultural reform. The US Violence against Women Act encodes a humanistic form of male behavior :

> Engaging Men as Leaders and Role Models : To develop, maintain or enhance programs that work with men to prevent domestic violence, dating violence, sexual assault, and stalking by helping men to serve as role models and social influencers of other men and youth at the individual, school, community or state-wide levels. [122]

This provision calls upon male technologists, programmers, developers, and users of technology to rise to the role of leaders, role models, and humanists who can be stakeholders in the prevention on technology driven violence. Toward this end, new and revised gender-based violence laws must adopt a two-pronged approach based in both human rights and Critical Information Theory to address this growing form of violence.■

120. Letter from Anja Kovacs, Dir., Internet Democracy Project, to Dubravka Šimonovic, Special Rapporteur on Violence against Women (Nov. 2, 2017), https ://cdn.internetdemocracy.in/idp/assets/downloads/reports/un-srvaw-report/Internet-Democracy-Project-Submission-Online-VAW-2-November-2017-4.pdf.

121. Comprehensive Act against Violence towards Women (Act No. 779) and the reform of the Criminal Code (Act No. 641), art. 19., A/HRC/WG.6/19/NIC/1, para. 67 (2012).

122. Violence Against Women Reauthorization Act of 2013, §§ 402(a)(b)(3).