McGill Law Journal
Revue de droit de McGill

Abortion in the Age of AI: A Need for Safeguarding Reproductive Rights in the United States and the European Union

Céline Castets-Renard et Caroline Lequesne

Volume 69, numéro 4, october 2024

Reimagining Justice: Artificial Intelligence (AI)'s Power for Redress and Division

URI : https://id.erudit.org/iderudit/1118433ar
DOI : https://doi.org/10.26443/law.v69i4.1683

Aller au sommaire du numéro

Éditeur(s)

McGill Law Journal / Revue de droit de McGill

ISSN

0024-9041 (imprimé)
1920-6356 (numérique)

Découvrir la revue

Citer cet article

Castets-Renard, C. & Lequesne, C. (2024). Abortion in the Age of AI: A Need for Safeguarding Reproductive Rights in the United States and the European Union. *McGill Law Journal / Revue de droit de McGill*, *69*(4), 533–555. https://doi.org/10.26443/law.v69i4.1683

Résumé de l'article

La décision *Dobbs v. Jackson Women's Health Organization*, rendue en juin 2022 par la Cour suprême des États-Unis, a renversé les arrêts *Roe v. Wade* (1973) et *Planned Parenthood v. Casey* (1992) au motif que la *Constitution* ne fait aucune référence au droit à l'avortement et qu'aucune disposition constitutionnelle ne protège implicitement un tel droit. Cette décision a, toutefois, eu des effets au-delà des frontières américaines.

De plus, son impact se fait sentir dans l'exercice des droits : l'arrêt a réinstauré un cadre répressif qui conçoit le corps des femmes comme un bien public. L'arrêt *Dobbs*, en renvoyant la question de l'avortement « au Peuple et à ses représentants élus », a accordé aux états la liberté de mettre en oeuvre individuellement des politiques pénales répressives, renforcées par des politiques numériques qui restreignent l'accès à l'information en ligne et encouragent la surveillance numérique des femmes à travers la collecte massive de leurs données intimes.

Abortion in the Age of AI: A Need for Safeguarding Reproductive Rights in the United States and the European Union

*Céline Castets-Renard and Caroline Lequesne**

The *Dobbs v. Jackson Women's Health Organization* decision, issued in June 2022 by the U.S. Supreme Court, overturned the *Roe v. Wade* (1973) and *Planned Parenthood v. Casey* (1992) rulings on the grounds that the *Constitution* makes no reference to abortion and that no such right is implicitly protected by any constitutional provision. This decision has had, however, effects beyond U.S. borders.

Furthermore, its impact is felt in the exercise of rights: the ruling has reopened a repressive framework that positions women's bodies as public property. The *Dobbs* ruling, by returning the issue of abortion "to the People and their elected representatives", has given individual states the freedom to implement repressive criminal policies, reinforced by digital policies that restrict access to online information and encourage the digital surveillance of women through the massive collection of their intimate data.

La décision *Dobbs v. Jackson Women's Health Organization*, rendue en juin 2022 par la Cour suprême des États-Unis, a renversé les arrêts *Roe v. Wade* (1973) et *Planned Parenthood v. Casey* (1992) au motif que la *Constitution* ne fait aucune référence au droit à l'avortement et qu'aucune disposition constitutionnelle ne protège implicitement un tel droit. Cette décision a, toutefois, eu des effets au-delà des frontières américaines.

De plus, son impact se fait sentir dans l'exercice des droits : l'arrêt a réinstauré un cadre répressif qui conçoit le corps des femmes comme un bien public. L'arrêt *Dobbs*, en renvoyant la question de l'avortement « au Peuple et à ses représentants élus », a accordé aux états la liberté de mettre en œuvre individuellement des politiques pénales répressives, renforcées par des politiques numériques qui restreignent l'accès à l'information en ligne et encouragent la surveillance numérique des femmes à travers la collecte massive de leurs données intimes.

* Céline Castets-Renard, Professor at University of Ottawa, Canada Research Chair on International and Comparative AI Law.

Caroline Lequesne, *Maître de conférence HDR* in public law at Université Côte d'Azur.

The authors warmly thank Janice Pole Sebagenzi, research assistant for the Chair Accountable AI in a global context and holder of a L.LL. and a J.D. from the University of Ottawa, for her invaluable assistance with the documentary research and the presentation of the footnotes.

Citation: (2024) 69:4 McGill LJ 533 — Référence : (2024) 69:4 RD McGill 533

Introduction

While one might have thought that the right to abortion was solidly recognized in Western democracies, the recent situation in the United States proves its fragility. The *Dobbs v. Jackson Women's Health Organization* decision, issued by Supreme Court of the United States in June 2022,[1] overturned both the *Roe v. Wade* (1973)[2] and the *Planned Parenthood v. Casey* (1992)[3] rulings on the grounds that the U.S. *Constitution* does not refer to abortion, notwithstanding the Fourteenth Amendment. As a result, individual states have now been at liberty to criminalize abortion in the early stages of pregnancy, provided they include an exception to safeguard the mother's health.[4] The decision has exacerbated deep divisions between states that are not new but constitute more than a simple step backwards.

As the exercise of civil rights occurs, in this day and age, under technological constraints and is, as such, subject to digital laws and policies, artificial intelligence (AI) can be used to monitor the privacy of individuals seeking abortions and exert strong control over their bodies. Several examples illustrate its broad usage. Notably, machine learning is used to aggregate and analyze reproductive health data from multiple sources to accurately profile women (data analytics) in the context of surveillance (advanced tracking methods). AI is also central to search engines like Google Search, which actively monitor women's online searches. On this basis, predictive AI can anticipate a woman's intention to have an abortion and increase surveillance. It is further employed to locate and identify women approaching abortion clinics. Simultaneously, it also plays a role in disseminating information online. Recommendation algorithms integrated with AI contribute to the propagation of misinformation, exacerbating the issue of harmful content in the realm of content moderation by online platforms. AI, then, embodies a divisive power of opinions in violation of any concept of social justice. It is, consequently, imperative to tackle the surveillance capabilities of these tools as a method of subjugating women and controlling their bodies.

This two-part contribution adopts a comparative perspective, sequentially examining the U.S. and European legal frameworks. Part I delves into the online information market related to abortion, highlighting the under-regulation that allows disinformation/misinformation to flourish

---

1 *Dobbs v Jackson Women's Health Org*, 597 US 215 (2022).

2 *Roe v Wade*, 410 US 113 (1973).

3 *Planned Parenthood v Casey*, 505 US 833 (1992).

4 Elizabeth E Joh, "Dobbs Online: Digital Rights as Abortion Rights" in Amanda Levendowski & Meg Leta Jones, eds, *Feminist Cyberlaw* (Oakland: University of California Press, 2024).

and impedes access to abortion rights. Part II considers the excessive technological surveillance of women and violation of their privacy when exercising their right to abortion.[5]

I. Online Information: Barriers to Access and Safeguards for Abortion Rights

The issue of online information is a vast and complex topic deeply rooted in culture. The availability of online information raises fundamental questions for our democracies and the exercise of our rights: how do we form opinions, listen to others, and ultimately build a society in an age dominated by information silos, disinformation, and online manipulation?[6] The issues become even more pressing as the use of artificial intelligence corroborates and intensifies these phenomena. The exercise of reproductive rights is no exception, with the use of online navigation as a primary method for access to medical, legal, and financial information. A multitude of questions may be posed: What risks do abortion procedures entail? Where can one find answers and advice from a qualified practitioner? Under what conditions are abortions performed? What forms of assistance are available? The dissemination of erroneous information on online platforms[7] may impact the responses to these pertinent inquiries. It should, however, be clarified that our intention is not to diminish the political dimension of this matter: individuals are free to formulate their own opinions on this deeply intimate subject. In this context, our focus is specifically directed towards the propagation of scientifically inaccurate or deceptive information concerning women's reproductive health.

Such disinformation or misinformation threatens reproductive rights and could become a way of oppressing women and their bodies. Whether they are intentionally false (*disinformation*) or inadvertent inaccuracies (*misinformation*), such information falls into one of four categories. The first concerns false information about medication and, specifically, "reversal" procedures, which supposedly interrupt ongoing medication-induced

---

5 Focusing our discussion on women is not intended to exclude transgender individuals, who face similar risks to their fundamental rights, along with additional specific challenges.

6 See generally Marina Vujnovic & Dean Kruckeberg, "Disinformation, Misinformation, Fake News, and Their Global Impact" in Yahya R Kamalipour & John V Pavlik, eds, *Communicating Global Crises: Media, War, Climate, and Politics* (Lanham, Md: Rowman & Littlefield, 2023) 97.

7 "Online platform" means a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public. For the purposes of this article, this definition encompasses social media platforms (e.g. Facebook, Instagram) and content creation platforms (e.g. YouTube).

abortions. Despite their active promotion by anti-abortion movements on social media, these procedures are deemed dangerous by U.S. authorities[8] due to the hemorrhagic risk they pose to women.[9] The second category includes the promotion of alternative medicines, for example, so-called "emmenagogue" herbs are consumed as tea and are claimed to induce a "natural" abortion. Not only is there no scientific evidence of these herbs' efficacy, but their consumption also endangers women's health due to their toxicity.[10] The third category pertains to the risks a woman might face following an abortion. Particularly widespread in Europe, this broad category covers physical and psychological risks. Frequently disseminated scientific inaccuracies include assertions that abortion may result in dementia, premature birth, breast cancer, and infertility.[11] Lastly, the fourth category refers to deceptive information concerning healthcare providers. This misleading information suggests that a medical centre, clinic, or professional provides abortion services when it is, in fact, a "crisis pregnancy centre" — a fake clinic opposed to abortion that aims to deter individuals from seeking out this procedure.

Digital technology thus inherently poses an early and key obstacle to the exercise of reproductive rights by compromising access to scientifically accurate information. Disinformation and misinformation simultaneously threaten access to procedures and compromise the informed consent process, as well as the ability to make fundamentally personal, health-informed choices. This section is a call for understanding and recognition of the threats to women's ability to exercise their reproductive rights. The first part of this paper examines how digital law addresses the obstacle of digital technology. The analysis reveals that the safeguards against deceptive online reproductive information, notwithstanding their diversity, are comparatively limited (A). Nevertheless, they converge on a pivotal, albeit contentious, aspect: the significant role they attribute to online

---

8 Khadijah Z Bhatti, Antoinette T Nguyen & Gretchen S Stuart, "Medical Abortion Reversal: Science and Politics Meet" (2019) 220:5 Am J Obstetrics & Gynecology 504 at 504). Reversal was also the subject of a warning by the American College of Obstetricians and Gynecologist (see ACOG, "Facts Are Important: Medication Abortion 'Reversal' Is Not Supported by Science", online: <acog.org> [perma.cc/3S4H-UJ66]).

9 An experimental scientific study had to be halted as 30% of the patients involved experienced a "severe" hemorrhage requiring their hospitalization (see Mitchell D Creinin et al, "Mifepristone Antagonization with Progesterone to Prevent Medical Abortion: A Randomized Controlled Trial" (2020) 135:1 Obstetrics & Gynecology 158 at 158).

10 Aviva Romm, *Botanical Medicine for Women's Health*, 1st ed (St. Louis, Mo: Churchill Livingstone, 2010) at 323–33.

11 Jenna Sherman, *Gendered Health Misinformation: Addressing Gendered Health Misinformation Related to Pregnancy and Infant Care, Gender-Affirming Care and Abortion* (Meedan, 2022) at 55, online (report): <meedan.com> [perma.cc/G63P-WVGP].

platforms in content moderation. The second part examines the role of online platforms in hindering access to abortion-related information (B).

A. Limited Safeguards of Digital Law

Addressing abortion-related information is a sensitive matter, inevitably entwined with individual moral, religious, political, and ethical convictions. The informational guarantees provided to women stand on the fine line between the right to personal choices in health and scientifically substantiated information. At the international level, the World Health Organization's guidelines prescribe the provision of two types of abortion-related information: general and specific information. The general information is intended for the public (accurate, unbiased, and evidence-based information on sexual and reproductive health, abortion services locations, cost of services, local regulations).[12] The specific information should be tailored to each individual seeking an abortion (information required for informed and voluntary consent, potential side effects and pregnancy symptoms, and post-procedural care details).[13] These recommendations receive different acceptance levels: they face challenges regarding freedom of expression in the United States, and they are vulnerable to changes in political national governments in Europe.

The informational battle is particularly fierce in the U.S. It has long been waged in the courts, leading to surprising reversals: if the First Amendment enshrining freedom of expression was initially the foundation of women's protection, it is now primarily mobilized by anti-abortion activists to impose significant restrictions on access to information.[14] The *NIFLA v. Becerra* case, decided by the Supreme Court in 2018, established a decisive milestone in this regard. The case focused on the California *FACT Act* that required anti-abortion pregnancy centres with a medical licence and funded by public money to inform women about the financial assistance they could receive for abortions.[15] The law sought to combat deceptive practices of anti-abortion centres, which took on the ap-

---

12 World Health Organization, *Abortion Care Guideline* (Geneva: World Health Organization, 2022).

13 *Ibid*.

14 For a comprehensive analysis of this reversal, see Yascha Mounk, "Why Freedom of Speech Is the Next Abortion Fight", *The Atlantic* (22 August 2022), online: <theatlantic.com> [perma.cc/34JR-XU7W].

15 US, AB 775, *Reproductive Freedom, Accountability, Comprehensive Care, and Transparency Act*, Reg Sess, Cal, 2015, §§ 2.7, 3.

pearance of family planning centres and clinics providing abortion.[16] These deceptive practices initially occurred in person; however, they later proliferated online through the imitation of abortion clinic websites, the optimization of online searches, and the targeting of advertisement through the massive collection of personal data. Many of these centres are listed on Google as abortion clinics. The issue before the Supreme Court centred on the classification of the information provided by the centres: commercial speech (advertisements) likely to deceive consumers (according to abortion defenders), or opinion speech under freedom of expression (according to anti-abortion activists). Following a narrow and uncommon interpretation of the *Zauderer* test,[17] the majority opinion held that the California law violated the First Amendment by compelling centres to alter their content. It is significant that the court did not consider arguments related to women's health, and the "professional speech" qualification from prior cases (information obligation for doctors) was rejected.[18] This decision paved the way for the anti-abortion lobby's strategies.[19]

Defenders of abortion are also fighting back. A primary line of defence is to call on the Federal Trade Commission (FTC) to take action based on section 5 of the *FTC Act* that enables combat against deceptive commercial practices. In this regard, President Joe Biden's Executive Order of July 8, 2022, encourages the authority to "consider options" concerning abortion misinformation.[20] A bill introduced in the U.S. Senate aims to grant express sanctioning power to the FTC against the deceptive prac-

---

16 Laura C Morel, "How Anti-Abortion Pregnancy Centers Can Claim to Be Medical Clinics and Get Away with It", *Reveal* (15 December 2022), online: <revealnews.org> [perma.cc/7N8R-EUGR]>.

17 The *Zauderer* test, developed in the jurisprudence of the same name, is the standard used to identify speech pertaining to commercial matters (see *Zauderer v Office of Disciplinary Counsel of the Supreme Court of Ohio*, 471 US 626 (1985); Bradley Queen, "The First Amendment v. Reproductive Rights: Crisis Pregnancy Centers, Commercial Speech, and Marketplaces of Misinformation" (2020) 54:1 First Amendment Studies 71 at 72–73).

18 *National Institute of Family & Life Advocates v Becerra,* 585 US 755 (2018).

19 Michele Goodwin & Mary Ziegler similarly note that the First Amendment has become the spearhead of these movements, see "The Next Anti-Abortion Tactic: Attacking the Spread of Information", *The New York Times* (3 December 2022), online: <nytimes.com> [perma.cc/VV74-W4C6].

20 "The Secretary of Health and Human Services shall, in consultation with the Attorney General and the Chair of the FTC, consider options to address deceptive or fraudulent practices related to reproductive healthcare services, including online, and to protect access to accurate information" (US, Executive Office of the President, *Executive Order on Protecting Access to Reproductive Healthcare Services* (EO 14076), 87 FR 42053 (2022), § 4(b)(iv)).

tices of crisis pregnancy centres.[21] At the state level, a joint statement by California, Oregon, and Washington[22] commits to combating misinformation on abortion and implementing various measures to try to counteract the deceptive practices of crisis pregnancy centres. Connecticut's law allows the state Attorney General to impose civil sanctions on centres engaging in deceptive reproductive health marketing.[23] An ordinance of the Los Angeles City Council allows misled individuals to bring liability lawsuits.[24]

No dedicated legislation has been enacted to combat disinformation and misinformation related to reproductive health and abortion.[25] Consequently, the content of the information is unrestricted. The main provisions available to counter abortion misinformation come from broader regulations such as the *European Digital Services Act* (*DSA*).[26] It is essential to understand that this regulation primarily points towards a method: under article 9 of the *DSA*, national judicial or administrative authorities can order online platforms to "act against illegal content." Thus, the illicit content subject to removal measures is not determined *a priori*, in itself, but falls within the scope of legality. The informational scope, therefore, depends mainly on the policy of each state. To date, no national provision explicitly recognizes abortion disinformation/misinformation as

---

21 US, Bill S 4469, *Stop Anti-Abortion Disinformation Act*, 117th Cong, 2022, § 3.

22 Gavin Newsom, Kate Brown & Jay Inslee, Joint Statement, "Multi-State Commitment to Reproductive Freedom" (24 June 2022), online (pdf): <gov.ca.gov> [perma.cc/FX37-Z4ET]. This has resulted, particularly in California, in a set of legislative proposals (see US, California Legislative Women's Caucus, *2022 LWC Reproductive Justice Policy Priority Package* (California Legislature, 2022)).

23 US, SB 835, *An Act Concerning Deceptive Advertising Practices of Limited Services Pregnancy Centers*, Gen Assem, Conn, 2021 §3(3)(c) (enacted). This law had sparked a lawsuit from an anti-abortion center, see *Pregnancy Support Center Inc v Tong,* Dist Ct (2023). The plaintiffs ended the lawsuit after negotiations with the Attorney General, who stated that such practices by the centers were non-existent. This legal dispute suggests that the law remains, for the time being, unenforced (see Matthew McDonald, "Connecticut Crisis-Pregnancy Center Withdraws Lawsuit Against 'Deceptive Advertising' Ban" *National Catholic Register* (21 January 2023), online: <ncregister.com> [perma.cc/TCK4-DRUQ]).

24 *Los Angeles Municipal Code,* art 8, Ch II (Ord No 187650 § 28.30*)* (to prohibit misleading advertising by pregnancy services centers located within the city of Los Angeles.

25 See the notable exception of French law, which, in 2017, expanded the offence of obstructing abortion to include online practices, *Loi nº 2017-347 du 20 mars 2017 relative à l'extension du délit d'entrave à l'interruption volontaire de grossesse*, JO, 21 March 2017. However, the implementation conditions limit its effects in the fight against misinformation.

26 EU, *Regulation 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 (Digital Services Act)*, [2022] OJ, L 277/1 [*Digital Services Act*].

illegal. On the contrary, attempts to limit or distort scientifically established content have flourished. Notably, Ireland previously tried to ban all communication on abortion, which was illegal in the country until 2018.[27] Other states linked information to unverified cancer risks.[28] Although the European Court of Human Rights (ECHR) recognizes the right to abortion information — which is binding on States[29] — current digital law is unlikely to have much effect on supporting this right. In the short term, platforms subjected to legal injunctions will likely remove the contentious content, but longer-term strategies are lacking.

Following the *Dobbs* decision in the United States, legal risk aversion has led platforms to perform a widespread removal of general abortion content.[30] To justify its removal, abortion content is often identified as sensitive and violent,[31] regardless of the nuanced local policies that divide the American territory.[32] The result is a phenomenon that has surpassed moderation both in content and geographically. This response denies women access to reliable and high-quality information about abortion, in violation of an informed choice.

This point leads to a broader exploration of the regulatory role and position acquired by online platforms regarding the phenomenon of misinformation.

---

27 In this regard, see the case brought before the European Court of Human Rights, *Open Door and Dublin Well Woman v Ireland* (1992), ECHR 68, 15 EHRR 244 at para 9. An injunction to prevent applicants (counselling agencies) from providing pregnant women with information concerning abortion facilities abroad was a violation of article 10 of the *European Convention on Human Rights*.

28 As an example, Russia allows information on abortion, but requires that any communication be accompanied by a warning (representing more than 10% of the communication), World Health Organization, "Global Abortion Policies Database: Russian Federation" (3 August 2022), online: <abortion-policies.srhr.org> [perma.cc/J3AJ-ZHSK].

29 In this regard, see *Open Door*, *supra* note 27 at para 80; *A, B and C v Ireland*, GC No 25579/05, [2010] VI ECHR 2032, 53 EHRR 13 at para 241; *RR v Poland,* No 27617/04, [2011] III ECHR 828, 53 EHRR 31 at para 200; *Tysiac v Poland*, No 5410/03, [2007] I ECHR 219, 45 EHRR 42 at para 52.

30 Aziz Z Huq & Rebecca Wexler, "Digital Privacy for Reproductive Choice in the Post-*Roe* Era" (2023) 98:2 NYL Rev 555 at 574.

31 Queenie Wong, "Fumbles in Its Moderation of Abortion Content", *CNET* (29 June 2022), online: <cnet.com> [perma.cc/Y6L3-QBGF].

32 Joseph Cox & Jordan Pearson, "Facebook Is Banning People Who Say They Will Mail Abortion Pills", *Vice* (27 June 2022), online: <vice.com> [perma.cc/8XNB-G4Y2].

B. Platforms as Gatekeepers of the Abortive Informational Market

Regarding content moderation, the United States and Europe have developed two distinct regulatory models: the United States advocates for the self-regulation of platforms, while Europe favours co-regulation.

Under American law, online platforms cannot be held liable or prosecuted for the publications of their users. This is the essence of section 230 of the 1996 *Communications Decency Act*, which has been designed as a fundamental guarantee of freedom of speech.[33] As a result, online platforms are free to implement their content moderation policies on reproductive health. The *Gonzalez v. Google* case, which questioned the interpretation of section 230, provided an opportunity to reinforce this regulatory model, particularly among advocates for abortion rights.[34] They argued that, in the absence of section 230's shield, most platforms would be exposed to lawsuits for allowing access to information in states, like Texas, which restrict the right to abortion. They suggested that websites and online platforms could face legal action for promoting content that aids Texas residents in obtaining an abortion, in violation of SB 8.[35] As a result, according to them, without section 230, most websites would choose to limit the legal risks by removing any abortion-related content. In a joint letter, they warned the Attorney General that "online services might be compelled to limit access to reproductive resources, for fear of violating various state anti-abortion laws."[36] Nevertheless, a lack of liability does not mean platforms should evade responsibility. As the final section describes, this is a flaw in the model: platforms do not ensure access to scientific information on reproductive health. Before delving into the platforms' policies on this matter, let's briefly explore the European model.

Conversely, European law obligates platforms to ensure a moderation policy in line with the rule of law and subject to penalties. Three legislative measures are particularly relevant to guide their policy on reproductive health. First, article 26 of the *DSA* requires online platform providers

---

33 598 US (2023).

34 *Gonzalez et al v Google LLC*, 598 USSC 617 (2023); Erica Hellerstein, "What A Law Designed to Protect The Internet Has To Do With Abortion", *Coda* (23 January 2023), online: <codastory.com> [perma.cc/M73W-TB9S].

35 Texas' anti-abortion "bounty" law, SB 8, empowers private citizens to file lawsuits against anyone who "aids or abets" another person seeking an abortion: US, SB 8, *An Act Relating to Abortion, Including Abortions After Detection of an Unborn Child's Heartbeat; Authorizing a Private Civil Right of Action*, 2021, 87th Legislature, § 171.208(2) (enacted).

36 The Honorable Merrick B Garland, "Copy of Letter to AG Garland re Gonzalez v Google" (November 21, 2022), online (pdf): <progresschamber.org> [perma.cc/8HFK-BBT2].

to ensure that "for each specific advertisement presented to each individual recipient", the recipients can "in a clear, concise and unambiguous manner and in real time" identify the natural or legal person on whose behalf the advertisement is presented (b) or who funded it (c). The text adopts a broad definition of advertising.[37] This transparency requirement[38] should help identify health providers while reducing the deceptive effect of sites mimicking governmental policies. Article 26 of the *DSA* is strengthened by the EU's *Code of Practice on Disinformation*, which binds its signatories under article 45.[39] This article provides that online platforms commit to "put in place or further bolster policies to address both misinformation and disinformation across their services, and to agree on a cross-service understanding of manipulative behaviours, actors and practices not permitted on their services".[40] Second, the *DSA* requires platforms to track professionals: by collecting their information and assessing their reliability when the intermediation service provided by the platform allows professionals to offer their products or services to EU consumers.[41] This measure aims to counter inaccurate web referencing, which leads to false clinics. Third, under article 34, very large online platforms are subject to an audit aiming to identify the "systemic risks" raised by their recommendation systems, content moderation systems or general terms and conditions, as well as their implementation.[42] Among the identified systemic risks are "any actual or foreseeable negative effects for the exercise of fundamental rights, in particular the fundamental rights to human dignity", and "any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being".[43] These risks must be mitigated to avoid sanctions. The regulation explicitly targets the fight against disinformation campaigns. This tool

---

[37] The *DSA* defines "advertisement" as a

> means information designed to promote the message of a legal or natural person, irrespective of whether to achieve commercial or non-commercial purposes, and presented by an online platform on its online interface against remuneration specifically for promoting that information (*Digital Services Act*, *supra* note 26, art 3(r)).

[38] *Ibid*, art 39. The transparency requirement is even stronger for very large online platforms.

[39] *Ibid*; EU, *Code of Practice on Disinformation* (Luxembourg: Publications Office of the European Union, 2022), online (pdf): <disinfocode.eu> [perma.cc/JG6S-U9RY] [*Code of Practice*].

[40] *Supra* note 39, art 21.

[41] *Supra* note 26, art 22.

[42] *Ibid*.

[43] *Ibid*, art 34(1)(b), 34(1)(d).

could encourage online platforms to prevent the widespread dissemination of misleading information and ultimately protect a woman's ability to make informed decisions about her health.

Given the recent entry into force of the *DSA*, it is premature to assess the effectiveness of its tools in ensuring and protecting reproductive rights. However, both the US and European regulatory frameworks result in the same fact: whether mandated or voluntary — and differently exposed to the state constraints mentioned — content moderation relies on private operators, namely the platforms. These observations call for an examination of the policies implemented through their terms of use, on the one hand, and their practices, on the other.

Despite some announcements advocating for the protection of women's reproductive health following the *Dobbs* decision,[44] online platforms remain largely silent about the guarantees provided. Only YouTube and TikTok mention it in their terms of use: the first prohibits content contradicting advice from local health authorities or the World Health Organization concerning the safety of medical and surgical abortion methods;[45] the second prohibits advertising abortion services and the diffusion of misinformation in the American market.[46] X, formerly Twitter, restricts the promotion of health and pharmaceutical products and services. Terms and conditions of use require prior authorization for advertising (notably) abortion clinics and advocacy.[47]

Regarding practices, empirical studies show that the spread of false information about abortion has significantly increased in the last two years. In the United States, 83% of Google searches regarding abortion refer to reversibility procedures,[48] which the search engine considers to be "safe and effective" techniques.[49] Meanwhile, YouTube has failed to re-

---

44 In July 2022, Google announced that it would remove online content promoting lies related to abortion and would redirect users to health authority websites (Davey Alba & Jack Gillum, "Google Maps Regularly Misleads People Searching for Abortion Clinics", *Bloomberg* (15 August 2022), online: <bloomberg.com> [perma.cc/E89X-BKS7]).

45 YouTube Help, "Medical misinformation policy", online: <support.google.com> [perma.cc/ACX3-QKLE].

46 TikTok, "Combating harmful misinformation", online: <tiktok.com> [perma.cc/CAH8-NG4G].

47 X Help Center, "Illegal or certain regulated goods or services" (March 2023), online: <help.twitter.com> [perma.cc/4B8W-QW4J].

48 Center for Countering Digital Hate, "Endangering Women for Profit: How Facebook and Google sell ad space for dangerous medical misinformation about so-called abortion 'reversals'" (14 September 2021) at 13, online (pdf): <counterhate.com> [perma.cc/SK8V-WUAE].

49 *Ibid* at 8.

move videos promoting false information. Despite its terms of use and its promise to label and identify content approved by scientific studies, the platforms initiatives are marginal: they focus exclusively on English-language videos.[50]

It also appears that the online platforms' monetary interests influence moderation. Dissemination of misleading and/or false content on abortion appears to be particularly lucrative. Targeted advertising about reversibility procedures generated significant profits in the United States.[51] The substantial funding of anti-abortion movements also ensures the consistent online presence of these narratives. These figures derive mainly from North America, as no equivalent empirical European studies were found. However, experience in content regulation indicates that policies are only partially regionalized.[52] Observational data also suggests that the regulation by platforms is susceptible to private interests, influencing moderation policies and, consequently, guarantees in terms of reproductive health. The dominance of corporate economic interests over the human rights of women must be challenged and actively resisted.

We have described how the regulation of the online informational market is threatened by both public capture (censorship for public policy reasons) and private capture (exposure to conflicts of interest). The digital realm — and its law, to some extent — thus contributes to hindering access to the abortion right. The second part of this article focuses on the exercise of this very right. Digital means then become repressive tools of pro-natalist policies, in disregard of reproductive health rights. Once again, such practices must be tackled to preserve women's rights.

II. Digital Enforcement of Policies Penalizing Abortion in the *Post-Dobbs* Era

Following the *Dobbs* decision, means of digital surveillance were mobilized by states that had adopted abortion criminalization laws (Alabama,[53] Arkansas,[54] South Dakota,[55] Oklahoma,[56] Louisiana[57]) to ensure

---

50 Clara Martiny, "How Platforms Profited from Abortion Misinformation in the Lead up to the Overturning of Roe v. Wade" *ISD* (11 October 2022), online (blog): <isdglobal.org> [perma.cc/K4DY-H4ST].

51 Center for Countering Digital Hate, *supra* note 48 at 7, 12.

52 Farhana Shahid & Aditya Vashistha, "Decolonizing Content Moderation: Does Uniform Global Community Standard Resemble Utopian Equality or Western Power Hegemony?" (delivered at the CHI Conference on Human Factors in Computing Systems, 23–28 April 2023), online (pdf): <adityavashistha.com> [perma.cc/MQ53-NQSR].

53 US, HB 314, *Alabama Human Life Protection Act*, Reg Sess, Ala, 2019.

54 US, SB 6, *Arkansas Unborn Child Protection Act*, 93rd Gen Assem, Ark, 2021.

their enforcement.[58] In contrast, progressive states (Washington,[59] California,[60] Massachusetts[61]) enacted protective laws to limit this society of surveillance (A). Even if, in the European Union, the use of technology is not as oppressive as in the United States, it is equally urgent to assess the ability of digital laws to protect reproductive rights in the age of AI, threatening respect for human rights (B).

A. Digital Surveillance of Reproductive Rights in the United States

The use of digital surveillance in criminal matters is not new. In this context, however, it supports pro-natalist policies and particularly affects the privacy and exercise of women's reproductive rights. A report published in May 2022 by the Surveillance Technology Oversight Project (STOP)[62] highlights that conservative state legislators are pressuring police and prosecutors to use all tracking tools available to target pregnant individuals and healthcare providers.[63] The diversity of digital means involved is alarming: collecting search engine data;[64] recording electronic payments on retail sales of abortion pills, over-the-counter medication and prescription medication;[65] collecting mobile phone data[66] and men-

---

55 S Dak Codified Laws § 22-17-5.1 (2022) (repealed).

56 Okla Stat § 63-1-734 (2023).

57 La Revised Stat § 40-1061.

58 Meagan Barrera & Danny Rayman Labrin, "Protecting Reproductive Rights Post-Roe, Can Companies Keep Your Data Safe?" (2023) 8:2 Bus & Human Rights J 259.

59 US, HB 1155, *An Act Addressing the Collection, Sharing, And Selling of Consumer Health Data*, Reg Sess, Wash, 2023.

60 US, AB 1242, *Reproductive Rights Act*, Reg Sess, Cal, 2022.

61 Brianna Keefe-Oates et al, "Use of Abortion Services in Massachusetts After the *Dobbs* Decision Among In-State vs Out-of-State Residents" (2023) 6:9 JAMA Network Open 1.

62 Albert Fox Cahn & Eleni Manis, *Pregnancy Panopticon: Abortion Surveillance After Roe* (New York: Surveillance Technology Oversight Project, 2022).

63 *Ibid* at 1.

64 David Ingram, "Can the Government Look at Your Web Habits without a Warrant? Senators Hope to Clarify That", *NBC News* (15 May 2020), online: <nbcnews.com> [perma.cc/M8A8-KSTF].

65 Lauren Rankin, "How an online search for abortion pills landed this woman in jail", *Fast Company* (26 February 2020), online: <fastcompany.com> [perma.cc/6G67-VBEL].

66 See *Riley v California*, 573 US 373 (2014); Cat Zakrzewski, Pranshu Verma & Claire Parker, "Texts, Web Searches about Abortion Have Been Used to Prosecute Women", *The Washington Post* (3 July 2022), online: <washingtonpost.com> [perma.cc/ERB4-UYQX].

struation tracking app data;[67] and monitoring electronic communications[68] (e.g. emails, social media messages, communications from video games). For example, Meta's "Messenger" service shared conversation data between a teenager and her mother with the Nebraska police to prove an illegal abortion.[69] It is worth clarifying that in this case, Messenger did not share the conservations. It was in fact Meta that disclosed the details of the conversation that occurred via Messenger after receiving a copy of the police warrant concerning the exchange. This example is important as it highlights the complicated relationship between Meta's obligation to comply with disclosures subject to a warrant (often explicitly mentioned in an organization's privacy policy) and an individual's right to privacy. This case is not isolated.[70] Access to advice and reproductive services is increasingly online,[71] exposing individuals to liability in anti-abortion states.

Digital surveillance also occurs through the collection of geolocation data from mobile phones around abortion clinics and identification data from body cameras used by anti-abortion activists, as well as automatic licence plate reading.[72] Data can also be shared by "crisis pregnancy centres," located near family planning centres, to deter individuals from seeking abortions.[73] On another note, AI can enhance an organization's location tracking capacities, for example, by applying computer vision technology to photos and videos.[74] Geolocation, notably, poses a risk in

---

67 Laura Shipp & Jorge Blasco, "How private is your period? A systematic analysis of menstrual app privacy policies" (2020) 2020:4 Proceedings on Privacy Enhancing Technologies 491 at 491; Michele E Gilman, "Periods for Profit and the Rise of Menstrual Surveillance" (2021) 41:1 Colum J Gender & L 100.

68 Jason Koebler & Anna Merlan, "This Is the Data Facebook Gave Police to Prosecute a Teenager for Abortion", *Vice* (9 August 2022), online: <vice.com> [perma.cc/6K6P-LKD4].

69 Johana Bhuiyan, "Facebook Gave Police Their Private Data. Now, This Duo Face Abortion Charges", *The Guardian* (10 August 2022), online: <theguardian.com> [perma.cc/LT4G-XHK5].

70 Runa Sandvik, "How US Police Use Digital Data to Prosecute Abortions", *Tech Crunch* (27 January 2023), online: <techcrunch.com> [perma.cc/P342-YTYX].

71 Huq & Wexler, *supra* note 30 at 560.

72 AW Ohlheiser, "Anti-abortion Activists Are Collecting the Data They'll Need for Prosecutions Post-roe: Body Cams and License Plates Are Already Being Used to Track People Arriving at Abortion Clinics", *MIT Technology Review* (31 May 2022), online: <technologyreview.com> [perma.cc/A6V9-2CGD].

73 The American Congress of Obstetricians and Gynecologists, "Crisis Pregnancy Centers: Issue Brief" (October 2022), online: <acog.org> [perma.cc/4VHJ-XAWY].

74 Geoff Brumfiel, "Artificial Intelligence Can Find Your Location in Photos, Worrying Privacy Experts", *NPR* (19 December 2023), online: <npr.org> [perma.cc/44XQ-43H8].

states such as Idaho, where cross-state movement to abort is prohibited.[75] Location data, then, constitutes potential evidence of a state crime.[76] This tracking method is also relevant to online activity. For example, Google claimed to exclude abortion clinics from users' location history,[77] but investigations by *Accountable Tech*[78] and *The Washington Post*[79] revealed that this promise was not kept.

The collection of personal data is further facilitated by the fact that entities subject to federal laws regarding health (through the *Health Insurance Portability and Accountability Act of 1996*),[80] financial data (through the *Gramm-Leach-Bliley* or *Financial Services Modernization Act of 1999*),[81] and electronic communications (through the *Stored Communications Act of 1986*)[82] must respond to criminal investigations and, in many cases, to warrants and subpoenas as well. Moreover, digital actors are not within the scope of these laws, meaning that brokers[83] can sell data to police services, outside of any judicial and legislative control. Furthermore, criminal investigations are now characterized by general warrant requests, based on a broad spatial perimeter by geofence around abortion

---

75 Idaho Stat §18-623, art 3.

76 Abby Vesoulis, "How a Digital Abortion Footprint Could Lead to Criminal Charges—And What Congress Can Do About It", *Time* (10 May 2022), online: <time.com> [perma.cc/BR5C-TEBG]; Alfred Ng, "'A Uniquely Dangerous Tool': How Google's Data Can Help States Track Abortions", *Politico* (18 July 2022), online: <politico. com> [perma.cc/R7DV-QH6Q].

77 Jennifer Elias, "Google says it will delete location history for visits to abortion clinics after overturning of Roe v. Wade", *CNBC* (1 July 2022), online: <cnbc.com> [perma.cc/7C7Q-NVAM].

78 Nicole Gill & Aditi Ramesh, "Big Tech's Toxic Business Model Could Land Abortion Seekers in Jail. Here's How to Stop Them", *Tech Policy Press* (13 June 2023), online: <techpolicy.press> [perma.cc/5RD8-BF6M].

79 Geoffrey A Fowler "Google Promised to Delete Sensitive Data. It Logged My Abortion Clinic Visit", *The Washington Post* (9 May 2023), online: <washingtonpost.com> [perma.cc/9EXP-QXKK]; Johana Bhuiyan, "Googling Abortion? Your Details Aren't as Private as You Think", *The Guardian* (29 November 2022), online: <theguardian.com> [perma.cc/5NWC-7AE7].

80 US, Bill HR 313, 104th Cong, 1996 (enacted).

81 US, Bill HR 10, 106th Cong, 1999 (enacted).

82 18 USC § 2703(a), (enacted under US, Bill S 2575, *Electronic Communications Privacy Act*, 99th Cong, 1986).

83 Several federal bills aimed to regulate them. See e.g. US, Bill S 2342, *A Bill To provide for requirements for data brokers with respect to the acquisition, use, and protection of brokered personal information and to require that data brokers annually register with the Federal Trade Commission*, 116th Cong, 2019. California adopted a data broker law on October 10, 2023 (see US, SB 362, *Data broker registration: accessible deletion mechanism*, Reg Sess, Cal, 2023 (enacted)).

clinics[84] as well as by online search keywords.[85] These "digital dragnets" allow the identification of a large number of abortion seekers,[86] even if the Supreme Court of the United States has declared that the Fourth Amendment of the *Constitution* prohibits the use of such warrants in the absence of evidence of a "probable cause."[87]

In response to the overcollection of personal data and in order to reinforce the respect of the women's reproductive rights, progressive states are defending reproductive rights by enacting data protection legislation. The state of Washington was the first to enact such legislation with the *My Health My Data Act* in April 2023,[88] which requires tech companies (e.g. social networks apps) to obtain explicit consent before collecting and selling health data. This includes information on sexual and reproductive health collected by menstruation tracking apps, as well as location data that may indicate a consumer is receiving health services. Geofencing within a perimeter of 2,000 feet around abortion clinics is prohibited.

California also passed a series of thirteen laws in September 2022 to expand access to abortion.[89] The *Reproductive Rights Act*[90] prohibits law enforcement agencies, as well as California companies providing electronic communication services, from complying with requests (arrest or search warrants) from law enforcement agencies of another state[91] or federal agency[92] if abortion is legal in California. Another law, the *Confidentiality*

---

84 See "Geofence Warrants and the Fourth Amendment" (2021) 134:7 Harv L Rev 2508 at 2509. Geofences are virtual perimeters or "fences" built around a given location that can be used to monitor the physical position of an object.

85 Chelsa C Edano, "Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants" (2022) 97:4 Wash L Rev 977 at 978.

86 Albert Fox Cahn & Eleni Manis, *Pregnancy Panopticon: Abortion Surveillance After Roe* (Surveillance Technology Oversight Project, 2022) at 3, online (pdf): <stopspying.org> [perma.cc/LP8D-46N9].

87 See *United States v Chatrie*, 590 F Supp (3d) 901, 927 (ED Va 2022) at 62 (regarding the invalidation of warrants based on the Fourth Amendment).

88 US, HB 1155, *An Act Addressing the Collection, Sharing, and Selling of Consumer Health Data; adding a new section to chapter 44.28 RCW; adding a new chapter to Title 19 RCW; and providing an expiration date*, Reg Sess, Wash, 2023, § 2(3) (enacted).

89 Office of Governor Gavin Newsom, "New Protections for People Who Need Abortion Care and Birth Control" (27 September 2022), online: <gov.ca.gov> [perma.cc/G5ND-46MB].

90 US, AB 1242, *Reproductive Rights*, Reg Sess, Cal, 2022. Regarding the creation of a new § 56.108 of the *Civil Code*, see US, AB 2091, *Disclosure of information: reproductive health and foreign penal civil actions,* Reg Sess, Cal, 2022, § 2.

91 Cal Pen Code §1546.5(a) (modifying Ch 3.6 of the *Electronic Communications Privacy Act*, 629.51).

92 *Ibid*, § 13778.2(b).

of Medical Information Act: reproductive or sexual health application information (*CMIA*), was enacted in September 2023[93] to protect data collected by mobile apps or websites that collect reproductive or sexual health information. These services will have to comply with the same medical information confidentiality standards as traditional healthcare providers. California legislation additionally prohibits government entities from submitting, and courts from executing, a "reverse keyword" or "reverse location" request by judicial warrants.[94] In Massachusetts, the *Location Shield Act*[95] prohibits brokers from selling mobile phone location data to third parties, requiring law enforcement to obtain a warrant.

While the measures taken by progressive states are a step in the right direction for the defense of women, they are often limited in scope. As a result, every new protective rule granted to women is immediately denied by conservative states. Such a legislative approach is therefore not sufficient to protect women's reproductive rights in a sustainable and effective way. Moreover, the efforts made in the U.S. to regulate AI at the federal level are very limited. The lack of legislative agreement before Congress led the Biden administration to publish an executive order.[96]

In this context, it is important to see if the European Union succeeds in implementing a legislative model that is truly favorable to women. At first glance, the exercise of the right to abortion seems less controversial in Europe than in the United States, but the potential for a setback in reproductive rights is worrisome in the era of AI.

B. Digital Surveillance of Reproductive Rights in the European Union

The European Union is built on common values and fundamental rights. However, the *Charter of Fundamental Rights of the European Union*[97] does not enshrine a right to reproductive freedom. Additionally, while all member states allow abortion, significant legal and practical disparities exist. The rise of conservatism in countries like Poland or

---

93 US, AB 254, *Confidentiality of Medical Information Act: reproductive or sexual health application information*, Reg Sess, Cal, 2023.

94 US, AB 793, *An Act to add §1546.8 to the Chapiter 3.8 of Title 12, Part 2 of the Penal Code, relating to privacy*, Reg Sess, Cal, 2023.

95 US, H 357, *An Act Protecting Reproductive Health Access, LGBTQ Lives, Religious Liberty, and Freedom of Movement by Banning the Sale of Cell Phone Location Information*, 193rd Gen Ct, Mass, 2023, § 2(e)(3).

96 The White House, Factsheet, "President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence" (30 October 2023), online: <federalregister.gov> [perma.cc/G27F-95QF].

97 EU, *Charter of Fundamental Rights of the European Union*, [2000] OJ, C 364/1 [*Charter*].

Hungary comes with threats, both in law and in practice, to the exercise of abortion. In Poland, a 1993 law[98] banned abortion except in three cases and one of the exceptions was declared unconstitutional in October 2020 by the country's Constitutional Tribunal[99]. This decision was later confirmed through an amendment of the law in January 2021.[100] Now, doctors in Poland face imprisonment for performing abortions deemed illegal. Consequently, Polish women often turn to online sources for abortion pills or travel abroad for the procedure,[101] making them vulnerable to digital tracking. This risk is heightened by the Polish government's creation of a pregnancy declaration and tracking database,[102] purportedly to improve patient care. Yet, there are concerns that this information could be used to crack down on abortions outside the country or to prosecute healthcare professionals.[103] Thus, while digital surveillance is not as widespread as in the United States, the collection of reproductive health data exerts pressure on those seeking abortions and on medical staff.

Given the growing threats to reproductive rights and risks of technological surveillance, can European digital legislation serve as protective barriers? Besides the aforementioned *DSA*, the *General Data Protection Regulation* (*GDPR*)[104] protects personal data and is complemented by the

---

98 *Law of January 7, 1993, on family planning, protection of the human fetus, and the conditions for termination of pregnancy* (Pol), 1993, Poland, 44:2 Intl Digest Health Legislation.

99 Judgment of the Constitutional Tribunal of 22 October 2020, K 1/20, Dz.U.2021.175. The exception related to situations where "prenatal tests or other medical premises indicate a high probability of a serious and irreversible impairment of the fetus or an incurable life-threatening illness of the fetus" was deemed unconstitutional. Abortion is still permitted in two notable cases: when the pregnancy poses a threat to a woman's life or health, and in the case where it is the result of rape or incest.

100 Poland, "Ustawa z dnia 7 stycznia 1993 r. o planowaniu rodziny, ochronie płodu ludzkiego i warunkach dopuszczalności przerywania ciąży" ("Law of January 7, 1993, on family planning, protection of the human fetus, and the conditions for termination of pregnancy"), online: <isap.sejm.gov.pl> [perma.cc/95LV-9YUM].

101 Harriet Barber, "Abortion Surveillance: How Women's Bodies Are Being Monitored", *The Telegraph* (10 October 2022), online: <telegraph.co.uk> [perma.cc/LT6B-5T3F].

102 Carly Penrose, "Poland's New Digital Health Data System Will Allow the Government to Track Pregnancies", *The National Post* (9 June 2022), online: <nationalpost.com> [perma.cc/6YQ4-UHKT].

103 Vanessa Gera, "Poland, with Near-Total Abortion Ban, to Record Pregnancies", *AP News* (6 June 2022), online: <apnews.com> [perma.cc/9QYA-43MR].

104 EU, *Regulation 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 [*GDPR*].

AI Act.[105] Article 9(1) of the *GDPR* prohibits the processing of sensitive data, including health data and data on sexual life or orientation. However, article 9(2) provides exceptions that permit such processing if the individual has given explicit consent. This may apply when using menstrual tracking apps or health information websites, but also when sharing delivery information to order abortion pills online. Individuals might, furthermore, agree to location tracking through mobile apps like Google Maps when visiting healthcare facilities. Still, the legitimacy of this data processing becomes questionable in light of opaque automated data processing practices and potential information sharing with law enforcement. There are also doubts regarding compliance with principles of legality, loyalty, necessity, purpose, and minimization which stipulate that data cannot be used outside its collection purpose.[106]

Additionally, individuals have rights, such as the right to "not to be subject to decisions based exclusively on automated processing, including profiling", that produce legal or similarly significant effects on them.[107] Yet exceptions, especially those related to the laws of Members States, diminish this right.[108] With Poland's national registry authorized by local law, automated processing might apply to the collected data, potentially profiling women. Procedural safeguards, like the need for a judicial warrant,[109] might be insufficient.

Moreover, article 23 of the *GDPR* allows for limitations to individual rights when member state law provides for measures related to crime prevention and detection, investigations, prosecutions, or penal sanctions execution. Thus, digital entities could share user personal data upon state requests. These limitations must, however, respect fundamental freedoms and rights and be necessary and proportional in a democratic society. But

---

[105] The regulation is in the final step of adoption, pending a final vote by the European Parliament in plenary session in April 2024. Our analysis is based on the final version of the text (see EU, *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*, COM [2021] 206 [*AI Act*]). See also *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)*, [2024].

[106] *GDPR, supra* note 104, art 5(1).

[107] *Ibid*, art 22(2).

[108] *Ibid*.

[109] *Ibid*. It should be noted, however, that the recent change of government in Poland has raised hopes of greater respect for fundamental rights, and, in particular, women's reproductive rights.

without a reproductive freedom protection right in the EU *Charter*, how would the Court of Justice interpret these provisions? Would it rely on privacy protection and personal data in a context where abortion is criminalized nationally?[110] Its jurisprudence leans on the subsidiarity legal principle, deciding that "[i]t is not for the Court to substitute its assessment for that of the legislature in those Member States where the activities in question are practised legally."[111] It merely recognizes abortion as a service, per article 57 of the *Treaty on European Union*,[112] allowing individuals to benefit from it in more permissive states without interfering in national laws to defend women's reproductive rights. Consequently, such an interpretation does not recognize these rights throughout the European Union.

Furthermore, the *AI Act* aims to apply rules based on the risk levels of AI systems. High-risk systems prevention relies on meeting requirements for use cases listed in Annex III of the regulation.[113] However, according to the final version of the *AI Act*, the AI use cases outlined in this contribution are not included in the category of high-risk AI systems. Furthermore, it prohibits

> the placing on the market, putting into service for this specific purpose, or use of an AI system for making risk assessments of natural persons in order to assess or predict the risk of a natural person to commit a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics.[114]

This prohibition does not apply to AI systems used "to support the human assessment of a person's involvement in criminal activity, which is already based on objective and verifiable facts directly related to the criminal activity."[115] It is highly likely that the various search processes used to track down women could collect "objective and verifiable facts" of such a nature as to fall within the exception. The interpretation of the text raises concerns: should the issue of digital surveillance of women seeking abortions not command greater attention within the values upheld by the EU?

---

[110] *Charter*, *supra* note 97, arts 7–8.

[111] *Society for the Protection of Unborn Children Ireland Ltd v Stephen Grogan and others,* C-159/90, [1991] ECR I-04685 at 20.

[112] EU, 7 February 1992 (consolidated 26 October 2012), C 326/13, art 57, online: <european-union.europa.eu> [perma.cc/4LYM-V39H].

[113] *AI Act*, supra note 105, arts 8–15.

[114] *Ibid*, art 5(d).

[115] *Ibid*.

Women whose reproductive rights are criminally threatened in their countries are left insufficiently protected by the European Union.

Finally, law enforcement agencies are allowed to use high-risk AI systems

> intended to be used by or on behalf of law enforcement authorities or by Union agencies institutions, agencies, offices or bodies in support of law enforcement authorities for profiling of natural persons as referred to in article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences.[116]

While high-risk systems are bound by specific obligations, such as implementing data governance measures to mitigate bias and errors, the use of an AI system for profiling individuals during the detection, investigation, or prosecution of criminal offenses is allowed. The regulation sets rules to minimize these systems' risks without banning them outright. Considering the risks analyzed in this paper for women seeking abortions, the European Union has not adequately recognized the potential threats to reproductive rights in a post-*Dobbs* era dominated by American tech firms. At this stage, we can only hope that the Court of Justice will interpret the *AI Act* in a way that protects women.

In this contribution, we have explored the diverse implications for women's reproductive rights within the realm of technology, specifically AI, spanning both the United States and the European Union. The first part demonstrated the pervasiveness and perils associated with online misinformation and disinformation surrounding abortion, emphasizing the heightened risks posed to women. The reluctance in the United States to adopt content moderation measures, coupled with the robust protection of freedom of expression, exposes women to risks and obstructs their access to quality information on reproductive healthcare, especially abortion. Meanwhile, in the European Union, the recently implemented measures under the *DSA* appear hopeful, but their real effectiveness remains uncertain. The second part showed how surveillance technologies can directly enforced criminal abortion policies, adversely affecting women's rights. Not only the access to abortion can be compromised, but their right to privacy and dignity can also be violated. The European Union provides more protection for the right to privacy and the personal data through the *GDPR*, but this text is unable to prevent a State from implementing a criminal policy and authorizing the processing of personal data for this purpose. Lastly, the *AI Act* addresses unacceptable and high-risk AI systems, but certain applications by repressive authorities receive ex-

---

[116] *Ibid*, Annex III, art 6(f).

emptions (unacceptable AI) or fall under the high-risk AI category, making them permissible. As a result, women are inadequately protected from the risks we have identified.

Therefore, there is an urgent need to recognize the surveillance capabilities of AI tools as instruments of women's oppression, safeguarding their reproductive rights for enhanced social justice. In this, like other fields, the restorative power of AI still needs to find its place. In the U.S., Danielle Citron encourages to consider certain forms of intimate privacy as a civil right.[117] In the EU, privacy and data protection are already fundamental rights,[118] however there is a need to go further. While the *AI Act* seeks to mitigate discrimination risks, it falls short in adequately and systematically addressing gender effects in the use of AI. The exercise of reproductive rights is just one example among many, and this is crucial to advocate for a better understanding of the negative impact of AI on women and for a more robust legal framework to ensure a better gender balance. One of the solutions could be to encourage the European Court of justice to interpret the *AI Act* and reinforce the non-discrimination provisions, through articles 21 and 23 of the EU *Charter of Fundamental Rights*.[119] Article 21(1) prohibits any discrimination based on sex and article 23(1) states that "equality between men and women must be ensured in all areas."[120] It is time to guarantee such equality within AI and digital technologies. Moreover, the principle of equality shall not prevent the maintenance or adoption of measures providing for specific advantages in favor of the under-represented sex. Feminist Science and Technology Studies have, notably, yielded substantial evidence of discrimination against women.[121] This body of knowledge must be translated to the legal and judicial framework to address the inequalities they face.

---

[117] Danielle Keats Citron, "Intimate Privacy in a Post-*Roe* World" (2023) 75:6 Fla L Rev 1033 at 1038. See also Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity and Love in the Digital Age*, (New York: Norton & Company, 2022) at 291.

[118] *Charter*, *supra* note 97, arts 7–8.

[119] *Ibid*.

[120] *Ibid*.

[121] See e.g. Fabian Lütz, "The AI Act, gender equality and non-discrimination: what role for the AI office?" (2024) 25 ERA Forum 79. See also the work of Donna Haraway, Sandra Harding, Evelyn Fox Keller, Carroll Pursell, and Judy Wajcman.