Facial Recognition Technology vs Privacy: The Case of Clearview AI

Camilla Dul*

Abstract. *In January 2020, the New York Times revealed the existence of Clearview AI, a company that had developed a facial recognition tool of unprecedented performance. Various actors were fast in declaring the loss of privacy accompanying the deployment of the application. This paper analyses how the economic motives behind facial recognition technologies challenge the established understanding and purpose of the fundamental right to privacy by the example of the EU. It argues that Clearview AI's business model, based on the surveillance of the company's data subjects, forcibly entails a violation of the latter's fundamental right to privacy. The traditional vertical application of fundamental rights in cyberspace disregards the power asymmetry existing between private individuals and private companies with state-like power in the Digital Age, thus resulting in legal ineffectiveness in face of this violation. The author concludes that the most fruitful approach to safeguard privacy would be the horizontal application of the fundamental right to privacy.*

1. Introduction

"The Secretive Company That Might End Privacy as We Know It": On 18 January 2020 Kashmir Hill introduced one of the world's most advanced tech companies in the field of facial recognition technologies.[1] Up to that point, Clearview AI (hereinafter "Clearview") had more or less secretively scraped the internet for face images of individuals and aggregated a database containing 3 billion pictures.[2] In October 2021, the number had climbed to 10 billion pictures.[3] When users of the company's application upload a portrait of an individual onto the application, all pictures of the individual that are stored in the database, together with the links to the websites from which the photographs were scraped, are shown within seconds. Clearview explicitly stated that it only sold its facial recognition application to law enforcement services in the USA and Canada.[4] Shortly afterwards, this claim would be debunked: private companies and individuals have been using the tool as well.[5] This was implicitly confirmed by the

* MLaw, PhD Candidate and Academic Assistant at the Faculty of Law of the University of Zurich (Switzerland). The author would like to thank Prof Christoph B Graber, PhD, MLaw, Giulia Walter, MLaw Alexander B Rom as well as two anonymous reviewers for their constructive suggestions.

[1] Kashmir Hill, 'The Secretive Company That Might End Privacy as We Know It' The New York Times (18 January 2020) https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html accessed 03 February 2022.

[2] ibid.

[3] Dev Kundaliya, 'Clearview AI has scraped 10 billion photos from the web' (2021) https://www.computing.co.uk/news/4038410/clearview-ai-scraped-billion-photos-web accessed 15 October 2021.

[4] Hill (n 1).

[5] Kate O'Flaherty, 'Clearview AI, The Company Whose Database Has Amassed 3 Billion Photos, Hacked' Forbes (26 February 2020) https://www.forbes.com/sites/kateoflahertyuk/2020/02/26/clearview-ai-the-company-whose-database-has-amassed-3-billion-photos-hacked/ accessed 04 February 2022.

company in February 2022.[6] The way in which Clearview has built a lucrative enterprise defies the fundamental right to privacy of its data subjects in an unprecedented manner. By linking the portraits in Clearview's database to other online information about the data subjects,[7] their identities are accessible to and can be compiled for anybody using Clearview's application, without the data subjects being aware of it. Privacy, as we know it,[8] has been lost.

When it comes to the protection of personal data in the digital realm, the EU has been the most advanced and consistent legislator, providing a *lex specialis* to the fundamental right to privacy, and the right to protection of personal data. Nonetheless, cases like the one Clearview presents have shown that even the supranational organisation's expression of the specific fundamental right in secondary law statutes have proven to be ineffective; otherwise, a tech firm like Clearview would not have been able to expand its business, *inter alia* in the EU. Traditionally, the protection of the individual by fundamental rights becomes necessary if a power asymmetry between the individuals and the State that influences and regulates the former with political means is ascertained. In the Digital Age, private companies like Clearview have a comparable regulatory effect. The only difference is their instrument of power: tech companies regulate by code, not by law.[9] Despite the parallel between the physical world and cyberspace, the novel power asymmetry has not been considered by law. Companies can therefore use the power asymmetry favouring them and capitalise on it. The application of the fundamental right to privacy in the vertical dimension between the individual and the State is inefficient in the case of online surveillance of individuals by private companies like Clearview. This surveillance then serves as a basis for the company's business model and enables the violation of other fundamental rights building upon the right to privacy.

In response to the ineffectiveness of the protection of the fundamental right that led to Hill's dystopian title, this paper answers the following research question: to what extent would

[6] In February 2022, Clearview publicly communicated that it wanted to massively expand beyond law enforcement. See Drew Harwell, 'Facial recognition firm Clearview AI tells investors it's seeking massive expansion beyond law enforcement' The Washington Post (16 February 2022) https://www.washingtonpost.com/technology/2022/02/16/clearview-expansion-facial-recognition/ accessed 25 February 2022.

[7] Hill (n 1); Kashmir Hill, 'Facial Recognition Start-Up Mounts a First Amendment Defense' The New York Times (11 August 2020) https://www.nytimes.com/2020/08/11/technology/clearview-floyd-abrams.html accessed 24 October 2021.

[8] Oxford English Dictionary, 'privacy, n.' https://www.oed.com/view/Entry/151596?redirectedFrom=privacy accessed 26 October 2021. The Oxford English Dictionary provides, *inter alia*, the following definition of privacy: "The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; seclusion; freedom from interference or intrusion". Also see Udo Fink, 'Protection of privacy in the EU, individual rights and legal instruments' in Normann Witzleb and others (eds), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge intellectual property and information law, Cambridge University Press, Cambridge UK 2014) 76-77.

[9] Lawrence Lessig, *Code: Version 2.0* (2nd edn Basic Books, New York 2006) 5. Lessig's famous wording "code is law" and the theory behind it accurately describe the regulatory powers of tech companies.

the horizontal application of the fundamental right to privacy ensure a more effective protection against business models being based on the violation of the basic right?

First, the functioning of Clearview's facial recognition technology is explained. This is followed by a chapter on the company's surveillance and business practices. The fourth chapter touches upon the current legal regulation of facial recognition technologies in the EU, and regulatory examples from the US are also discussed for the purpose of comparison. This then leads to the discussion on how the fundamental right to privacy could be best protected with horizontal application in cyberspace.

2. The secretive company: how Clearview's facial recognition technology works

Clearview has remained very secretive about the functioning of its facial recognition technology and has never disclosed what allows its application to outperform similar technologies. The company's facial recognition technology is a so-called black box:[10] it is impossible to see through its coding processes. Thus, only assumptions about the tool's functioning can be made.

Facial recognition technologies are based on artificial intelligence (AI).[11] An AI-based system acts intelligently in the sense that it analyses its environment, processes the results, and ultimately achieves a pre-specified goal. To a certain extent, it acts autonomously. To improve their performance, AI technologies need to be trained on data. Facial recognition algorithms are exposed to a developmental set of images. They then learn how to detect faces and how to extract relevant features from them.[12] Once the algorithms have reached a satisfying level of performance, they assist in improving and automating the system's decision-making process.[13]

Facial recognition technologies identify data points within images, which at first represent unstructured data, with the help of cognitive approaches.[14] An automated biometric facial recognition technology acquires biometric data (a person's face image), extracts discriminating feature vectors of the person's face (biometric templates)[15] and then compares the set of features against features in biometric templates that are stored in a database. Most

[10] For an explanation of the expression "black box," see Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, Cambridge MA 2015) 3, 40.
[11] European Commission, *On Artificial Intelligence - A European approach to excellence and trust (White Paper)* (Brussels 2020) 2.
[12] Lucas D Introna and Helen Nissenbaum, 'Facial Recognition Technology: A Survey of Policy and Implementation Issues' [2009] Center for Catastrophe Preparedness and Response, New York University https://nissenbaum.tech.cornell.edu/papers/facial_recognition_report.pdf accessed 25 October 2021, 18.
[13] European Commission, *Artificial Intelligence for Europe (Communication)* (Brussels 2018) 2.
[14] See Introna and Nissenbaum (n 12) 15-16. Machine learning is an example for such a cognitive approach.
[15] Hisham Al-Assam and others, 'Privacy in Biometric Systems' in S Zeadally and M Badra (eds), *Privacy in a Digital, Networked World: Technologies, Implications and Solutions* (Springer International Publishing Switzerland, Cham 2015) 237.

identification systems include the following three elements: biometric identifiers (e.g., face images), biographical identifiers (e.g., an address) and attributed identifiers (e.g., a name). Strengthening the links between biographical and attributed identifiers is expected to create a reliable identity triad.[16] Detailed personal profiles of the data subjects can be composed[17] without obtaining the data subjects' consent,[18] without them even knowing.

One of the few disclosures Clearview made about the functioning of its algorithms is that the company's technology considers a person's unique facial features that remain the same during the aging process.[19] Scraped pictures as well as pictures uploaded onto Clearview's application presumably represent the inputs which train the algorithms, and which are subsequently added to the company's database. We can assume that the scraping of, allegedly, ten billion face images from the Internet must have trained Clearview's algorithms. All the pictures, including the ones being uploaded onto the application, are additionally sent to and stored on the company's server.[20]

Likewise, the collection of face image material happens in secrecy. Clearview acts like a search engine for faces and scrapes the internet for publicly available images of people. Search engines deploy digital robots that crawl the internet "as if they were peripatetic web surfers."[21] That is, with an algorithm: the robots click on link after link, record the results and arrange them so that they can be used for search. The gathering of huge amounts of data of an undefined number of people generates big data. There is no previously defined purpose or aim for the data collection.[22] Clearview started to build up its database before deciding on a specific application,[23] thus its database consists of big data. Extracting big data from face images is one of the factors making the company's conduct revolutionary. Clearview keeps scraped pictures in its database indefinitely unless it grants a request to have an individual's picture(s) deleted.[24]

---

[16] Introna and Nissenbaum (n 12) 9.
[17] Stephan Finsterbusch and Thiemo Heeg, 'Wie die KI die Gesichtserkennung revolutioniert' Frankfurter Allgemeine Zeitung (26 February 2020) https://www.faz.net/aktuell/wissen/computer-mathematik/wie-die-ki-die-gesichtserkennung-revolutioniert-16647830.html accessed 25 October 2021.
[18] For an explanation of the term "data broker", see Kirsten Martin and Helen Nissenbaum, 'Privacy Interests in Public Records: An Empirical Investigation' (2017) 31 Harv J L and Tech 111, 125.
[19] CNN Business, *Clearview AI's founder Hoan Ton-That speaks out [Extended interview],* minutes 09:09-09:39.
[20] Hill (n 1).
[21] Nancy Blachman and Jerry Peek, 'How Google Works' (02 February 2007) https://www.googleguide.com/google_works.html accessed 04 November 2021, found in Jonathan Zittrain, *The Future of the Internet and How to Stop It* (Yale University Press, New Haven CT, London UK 2008) 223.
[22] Bart van der Sloot, 'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities' in Serge Gutwirth, Ronald Leenes and Paul de Hert (eds), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Law, Governance and Technology Series: Issues in Privacy and Data Protection, Springer Science+Business Media, Dordrecht 2016) 413.
[23] See CNN Business (n 19), minutes 00:44-00:52.
[24] ibid. So far, no request has been granted. See section 4.3.

Upon realizing how Clearview has established its facial recognition technology, by not setting itself any limits when it comes to the collection of image data, privacy concerns emerged rapidly. In order to comprehensively explain how Clearview's activities endanger privacy, it is crucial to understand the sociological phenomena enabling them. The following chapter is dedicated to the sociological explanation of the Clearview case.

3. How Clearview challenges privacy

As mentioned in the introduction, until the beginning of 2022, Clearview repeatedly emphasised that its tool was exclusively meant to support law enforcement,[25] a claim that was easily debunked. There is strong suspicion that the lucrative primary use of the company's technology is to enable the surveillance of its data subjects. The support of law enforcement serves as a cover and is, in fact, the technology's secondary use. Regarding fundamental rights considerations, it is crucial to first assess the technology's actual purpose. Only if the latter allows for the respect or legitimate restriction of fundamental rights of data subjects, it makes sense to evaluate if the secondary use also does. This paper focuses on the evaluation of the primary purpose of Clearview's facial recognition technology.

3.1. Generativity in cyberspace

In contrast to the physical world which seems rigid and largely regulated by legal or social norms, the internet appears open, largely unregulated, and participative. Zittrain introduced the term "generativity" in the realm of cyberspace to describe the open character of technological systems like the internet in one word.[26] Generativity allows citizens in the Digital Age not just to use cyberspace, but also to co-create it through interactions with others and with the use of technology.[27] Physical as well as virtual spaces where expressive interactions happen may constitute public *fora*.[28] As nowadays social media platforms represent a major source of information exchange, social media platforms can be defined as public *fora*. People have a right to communicate and gain relevant information on the internet, without the unfair trade-off they are often forced to undergo.[29] People have a right to share what they wish about their

[25] It has not been publicised how the company verifies if individuals acquiring the application are governmental agents. On Clearview's homepage (https://www.clearview.ai, accessed 11 March 2022), for example, there is no information about such a verification process.
[26] Zittrain (n 21) 34.
[27] David S Allen, 'Spatial Ethics and the Public Forum: Protecting the Process of Creating Public Space and Meaning' in Bastiaan Vanacker and Don Heider (eds), *Ethics for a Digital Age* (Peter Lang, New York 2016) 206.
[28] ibid 195-96. By legal definition, social media platforms are not public *fora*. They are private *fora* having been opened to citizens. Allen convincingly counters this outdated legal view by bringing into focus the creation of public *fora* by interactions.
[29] Carol C Gould, 'How Democracy Can Inform Consent: Cases of the Internet and Bioethics' (2019) 36 Journal of Applied Philosophy 173, 176. The "unfair trade-off" refers to the inevitability of sharing one's data and therefore become transparent to tech companies in order to be able to use the conveniences of the internet.

lives, and social media platforms can facilitate this. Such an exchange can occur in the form of sharing photographs. According to Zittrain, the entirety of people sharing pictures online, the "army of the world's photographers", represents a powerful generative source;[30] a source Clearview is making economic use of.

The internet's generative character is double-edged for tech firms from an economic perspective: on the one hand, they can use data as raw material for free. On the other hand, providing free services can mean undergoing financial losses. The reaction of tech firms has often been a shift to tethered, controlled systems. Nowadays, most applications can only be changed by their vendors,[31] and no external coders have access to the application's data or algorithms.[32] Clearview's conduct is characteristic of the shift: the company takes advantage the "army of the world's photographers" in a novel manner when crawling the web for face images. It uses the generative source to establish its tethered, completely untransparent facial recognition application. In the absence of (legal) rules that would provide a clear answer to whether Clearview has a right to make use of the generative source, the question of legitimacy arises. On one side, it can be argued that once people have chosen to deposit information about themselves in a public forum, they cannot expect that the information can later be completely suppressed. If it could, the freedom of other people would be restrained because they observe information about others without intruding upon the latter's private realm. They cannot be asked to actively look away when being exposed to deliberately shared information.[33] On the other side, it might be asked whether companies, *inter alia* Clearview, have a legitimate commercial interest in the collection of voluntarily shared data,[34] in other words, in making use of generativity.

When following traditional theories of fundamental rights, the interests of all parties interacting in public *fora* are to be balanced against each other.[35] Whereas generativity helps moderating the power gap between governments and citizens in cyberspace, new hierarchies and power gaps are being constructed among private actors. Scrutinizing others and

[30] Zittrain (n 21) 215.
[31] ibid 101.
[32] ibid 124.
[33] Helen Nissenbaum, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public' (1998) 17 Law and Philosophy 559, 572.
[34] See ibid 573. Nissenbaum answers this question in the affirmative, at least in principle.
[35] See Ignacio Garcia Vitoria, 'Environment Versus Free Enterprise' in Eva Brems (ed), *Conflicts between fundamental rights* (Intersentia, Antwerp 2008) 477. Since Clearview scrapes pictures from social media platforms that have received data subjects' consent (at least to a certain degree), the commercial interests of those platforms would also have to be balanced against those of Clearview. This paper focuses on privacy concerns of individuals in light of facial recognition technologies, interest trade-offs between tech firms and questions of copyright infringements regarding scraped photographs are therefore not considered.

simultaneously escaping scrutiny oneself represents one of the strongest forms of power, for knowledge is power. Knowledge about data subjects can be sold. At the same time, there is little known about how exactly this knowledge is acquired, and regulators are given limited information if at all about how the scrutiny of data subjects occurs.[36] By aggregating data of billions of people in secrecy, Clearview has created itself a power position hardly ever seen before. To illustrate the perils of the glaring imbalance between the tech company and its data subjects, this paper first discusses what constitutes Clearview's power. Afterwards, a connection to the privacy infringement of its data subjects is made

3.2. Clearview's economic surveillance power

It is not the technology of search engines, social media, etc. that generates money. It is the sale of information being collected as raw material in the form of big data in virtual public *fora* that does.[37] Lyon broadly defines surveillance as "any systematic, routine, and focused attention to personal details for a given purpose".[38] There are two sides to surveillance. One is the protection and care for individuals; the other one, often occurring simultaneously, is watching individuals for regulatory purposes, that is, controlling and disciplining them into a certain behaviour or set of norms.[39]

Haggerty and Ericson developed the concept of "surveillant assemblage" to describe systems combining surveillance and social control functions. According to their theory, human bodies are abstracted from their territorial settings and are separated into a series of discrete flows that are then reassembled into "data doubles".[40] These doubles can be scrutinised and used for intervention. This means that human beings are separated from their physical selves, which is de-humanizing, or "dividualizing".[41] A data double constitutes a supplementary self, a "functional hybrid".[42] A unique, human face is turned into a data set being used as raw material, which runs counter to the fundamental right of human dignity. Participation with one's own data (product) is rendered impossible. This violates a data subject's autonomy and therefore also their privacy. The process shows what Haggerty and Ericson call a "rhizomatic

[36] Pasquale (n 10) 3-4.
[37] Andrea Sangiovanni, 'Democratic Control of Information in the Age of Surveillance Capitalism' (2019) 36 Journal of Applied Philosophy 212.
[38] David Lyon, 'Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique' (2014) 1 Big Data & Society 1, 2; according to Zittrain (n 21) 109, surveillance systems are tethered appliances.
[39] Maša Galič, Tjerk Timan and Bert-Jaap Koops, 'Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation' (2017) 30 Philosophy & Technology 9, 10.
[40] Kevin D Haggerty and Richard V Ericson, 'The Surveillant Assemblage' (2000) 51 The British Journal of Sociology 605, 611.
[41] Gilles Deleuze, 'Postscript on the Societies of Control' (1992) 59 October 3, 5.
[42] Sean P Hier, 'Probing the Surveillant Assemblage: on the dialectics of surveillance practices as processes of social control.' (2002) 1 Surveillance & Society 399, 400.

levelling of the hierarchy of surveillance": groups which were formerly not subjected to routine surveillance are now being monitored as well, by private institutions that are integrated into the "surveillant assemblage".[43]

Lyon explains the shift from purely state surveillance to agency surveillance as a shift from discipline to control, with control serving as a driving force of regulation.[44] Surveillance is no longer carried out through visible and physical forces on individuals; rather, it is carried out through secretive networks that render surveillance abstract and numerical.[45] The "datafication" of society has led surveillance to combine the monitoring of both physical (where, for example, face pictures are taken) and digital spaces (where data doubles circulate). In the resulting hybrid surveillance spaces, corporate surveillance is complemented with self-surveillance as well as "forms of watching-and-being-watched" through social media platforms (public *fora*) and the voluntary data sharing they are sustained by.[46]

Modern surveillance shows exponential expansion and leads to an asymmetry of transparency: individuals' everyday lives become transparent to tech organisations. At the same time, the organisations' surveillance becomes invisible to the data subjects.[47] Hence, not only have the hierarchies and purposes of surveillance been transformed, but also the institution of privacy has been under severe attack.[48] Surveillance has become an apparatus consisting of a combination between practices and technologies. The assemblage operates across governmental institutions and, substantially, across private ones.[49] The Clearview case provides a prime example thereof. The company has systematically scraped the internet for individuals' images to build up the database that it uses to increase its societal power and to earn money.

Although not presenting a "classical" surveillance method, in its effect, Clearview's secretive facial recognition technology is an omnipresent invasive surveillance system: there is a constant chance of having one's pictures uploaded onto a social media platform (for example, when involuntarily appearing in the background of somebody else's picture that they have posted on their profile, as opposed to the voluntary sharing of information mentioned in the previous section), and then having one's face image scraped by Clearview's search engine

[43] Haggerty and Ericson (n 40) 606-07.
[44] Lyon (n 38) 7.
[45] Galič, Timan and Koops (n 39) 19.
[46] ibid.
[47] See Lyon (n 38) 4.
[48] See Haggerty and Ericson (n 40) 616.
[49] ibid 610.

algorithm. There is a clear knowledge, and thus power asymmetry between the company and its data subjects whose data, and therefore privacy, are not protected at all.

3.3. The umbrella concept of "privacy"

Once a society has become accustomed to a certain type of surveillance (be it conducted by private companies or state entities), reasonable[50] privacy expectations disappear.[51] This is not to be equalled with a complete loss of expectations towards privacy. It means that the internalisation of specific surveillance methods lower expectations of individuals below a level they once considered reasonable. Privacy is a general "umbrella" concept that encompasses many aspects.[52] In Western societies, privacy is considered to be a value in itself and it is linked to other values of moral, political and legal content.[53] Westin argues that privacy furthers human ends in democratic and free societies because it enhances personal autonomy.[54] Privacy is every person's right and it is an important aspect of one's personal autonomy to decide how much privacy they are willing to give up when posting pictures on the internet. The right to privacy should include both a right to control whether one's information is shared and if so, with whom.[55] A protected realm for emotional release is created and a context for individuals to exert their individuality is provided. This all allows for confidential communication to be ensured.[56] With its intrusive surveillance practices, Clearview takes away autonomous choices from its data subjects. "Dataveillance" does not only infringe upon citizens' privacy rights. By depriving them of making decisions about what happens with their personal data, the practices of "dataveillance" menace principles of self-determination that used to define the existential and political canon of the modern liberal order and were established during centuries.[57] Undermining this fundamental principle endangers the strong association there is between the respect for human autonomy and the right to human dignity and freedom.[58]

Although the right to privacy is an individual right, it also bears societal significance. It can be described as a term of interaction, that is, it only is of value in the context of the

[50] To get an idea about what "reasonable" could mean in this context, see subsection 3.1.
[51] Mitchell Gray, 'Urban Surveillance and Panopticism: will we recognize the facial recognition society?' (2003) 1 Surveillance & Society 314, 325.
[52] Anita L Allen, Marc Rotenberg and Rok Lampe, *Privacy Law and Society* (3rd edn West Academic Publishing, St. Paul MN 2016) 7.
[53] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press, Stanford CA 2010); Jonathan Cinnamon, 'Social Injustice in Surveillance Capitalism' (2017) 15 Surveillance & Society 609, 620. Most legal systems recognize privacy as a fundamental right.
[54] Alan F Westin, *Privacy and Freedom* (Atheneum, New York 1967) 33.
[55] James Rachels, 'Why Privacy Is Important' (1975) 4 Philosophy & Public Affairs 323, 328.
[56] Westin (n 54) 36.
[57] Shoshana Zuboff, 'Wie wir Googles Sklaven wurden' Frankfurter Allgemeine Zeitung (05 March 2016) https://www.faz.net/aktuell/feuilleton/debatten/die-digital-debatte/shoshana-zuboff-googles-ueberwachungskapitalismus-14101816.html accessed 11 October 2021.
[58] European Commission, *Ehtics Guidelines for Trusworthy Artificial Intelligence* (Brussels 2019) 11.

regulation of behaviour between individuals.[59] Before the Digital Age, privacy evolved around intimate and sensitive information. Nowadays, information made public represents an additional problem. The actual revolution of the Digital Age is not the gathering of data per se, but the analysis of data that is willingly shared, even if the intentions behind this sharing are of entirely private nature. People sharing information are sometimes accused of being complicit in their own privacy violation.[60] The accusation is wrong: it is legitimate for citizens to use public *fora* on the internet to express themselves. Nevertheless, this behaviour can cause a so-called privacy paradox. People voluntarily disclose private information but are then concerned about how private and public entities collect and use their data.[61] An isolated piece of information, for example a picture of a person, does not reveal much about them. But as soon as information is systematically aggregated and shared, comprehensive dossiers about individuals can be assembled[62] and thus violate their legitimate right and expectation to privacy. The price society pays for freedom on the internet is represented by the help they provide in training the algorithms that can later harm privacy,[63] another paradox that emerges alongside Clearview's rhizomatic spread. The new culture of personal transparency leads to infringements of privacy and makes the need for disclosure on the opposite side paramount.[64]

The idea of privacy in the public domain being a moral aspect of the right to privacy in cyberspace has always existed, but only new technologies have rendered it problematic. Today, there is an unlimited amount of information that can be recorded, an unlimited scope of possible analysis that can be conducted, and the information can be stored virtually forever.[65] The power asymmetry between states and individuals has been remarkable. But the ignorance of privacy gives tech firms far more power than states have ever had.[66] What happens to public privacy hinges on how the ones with the most power and with the strongest lobbies handle it.[67] This renders the threat to privacy in public general and systematic. The problem the Clearview case

[59] Jessica Heesen and Marc Sehr, 'Technikethik: Verantwortung für technische Produkte – „Ex Machina"' in Thomas Bohrmann, Matthias Reichelt and Werner Veith (eds), *Angewandte Ethik und Film* (Springer Fachmedien Wiesbaden GmbH, Wiesbaden 2018) 252.
[60] Larry Hunter, 'Public Image' in Deborah Johnson and Helen Nissenbaum (eds), *Computers, Ethics, and Social Values* (Prentice Hall, Englewood Cliffs 1995) 294. This claim fits Zittrain's expression "army of the world's photographers" that represent a generative source of the Internet Zittrain (n 21) 215.
[61] Michael Friedewald and others, 'The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security' in Serge Gutwirth, Ronald Leenes and Paul de Hert (eds), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Law, Governance and Technology Series: Issues in Privacy and Data Protection, Springer Science + Business Media, Dordrecht 2016) 52-53.
[62] Gray (n 51) 318.
[63] Lyon (n 38) 7.
[64] Richard A Posner, 'Privacy, Surveillance, and Law' (2008) 75 U Chi L Rev 245, 249.
[65] Nissenbaum (n 33) 576.
[66] See Introna and Nissenbaum (n 12) 8.
[67] Nissenbaum (n 33) 566.

exemplifies is how such technologies prevent individuals from enjoying complete privacy even in their homes.[68] It is impossible to know when people secretively take pictures of others to run them through a database like Clearview's. The knowledge that one's picture and the connected data *might* be gathered and stored creates the danger of a chilling effect on people's freedom of expression and expectation of privacy. The Clearview case shows how tech firms, which have the regulatory power of nation states through code instead of law,[69] violate the fundamental right to privacy without them being able to be held accountable for the infringement.

For it is both of individual (as a "basic fundamental right") and societal (as an enabler of public *fora*) importance, privacy is to be considered a constitutive element of modern society. Economy also bears substantial societal significance. But if privacy is neglected, "digital society" is deprived of one of its constitutive elements. If one of the latter is missing, social systems, such as economy, cannot operate like their societal function would require them to. This does not mean that the right to privacy is absolute or inviolable.[70] Though it does mean that commercial interests, which are not of constitutive societal importance in contrast to privacy, must take a backseat. In the next chapter it is described how Clearview's indifference to individual's privacy is made possible under current legislation in the EU and some parts of the USA; in other words, how the legal systems regulate facial recognition technologies.

4. The current legal responses to facial recognition technologies

Several legal systems worldwide, among them the EU and different legislators in the USA on a state or municipal level, have started to regulate facial recognition technologies because of deep concerns over the effects these might have on society, whereby the threat of data subjects' privacy rights is the main argument for regulation in each case.[71] In the Digital Age, privacy law has gained particular importance in the more specific form of data privacy law, *inter alia*

[68] In *Silverman v. United States* [1961] (U.S. Supreme Court), the US Supreme Court held that the Fourth Amendment's "very core" was "the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion". Although the case treated intrusion into the home by federal officers without a warrant, the formula well describes the importance and intimacy of a person's home. The intrusiveness and ubiquity of Clearview's facial recognition technology deprives the formula of its meaning. It is imaginable that Clearview's database also contains pictures that were taken with phone or computer cameras within a person's home, without them being aware of it.

[69] Lessig (n 9) 5.

[70] See Normann Witzleb and others, 'An overview of emerging challenges in privacy law' in Normann Witzleb and others (eds), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge intellectual property and information law, Cambridge University Press, Cambridge UK 2014) 1. The right to privacy can be restricted under strict legal conditions. To anticipate examples of the EU, data can only be legally processed if data subjects have consented to it (article 6(1)(a) General Data Protection Regulation) or if it is necessary to protect superior interests (see article 6(1)(b-f) General Data Protection Regulation).

[71] Marit Hansen, 'Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen [DSGVO]' in Spiros Simitis, Gerrit Hornung and Indra Spiecker genannt Döhmann (eds), *Datenschutzrecht: DSGVO mit BDSG* (NomosKommentar, Nomos, Baden-Baden 2019) 749.

as a powerful counterweight to "technocratic imperatives",[72] as is the case for the legal handling of facial recognition technologies. Whereas the EU comprehensively restricts the gathering of personal data by both public and private parties,[73] the US Constitution only limits government actions that would infringe upon the right to privacy of individuals.[74] This chapter discusses the two diverging regulatory approaches using the example of the Clearview case in order to show their respective ineffectiveness.

4.1. The legal regulation of facial recognition technologies in the EU

With its General Data Protection Regulation (GDPR)[75] the EU has taken up a global leading role when it comes to the data protection of individuals, including facial recognition technologies. In the following it is first assessed if Clearview's conduct and application can be subsumed under the GDPR. The GDPR, which is based on article 16(2) of the Treaty of the Functioning of the EU (TFEU), succeeded the Data Protection Directive[76] and came into force in 2018 (article 99(2) GDPR).[77]

As laid down in article 2(1) GDPR, the "Regulation applies to the processing of personal data wholly or partly by automated means […]". This requirement holds true for Clearview, that processes image data with the help of AI. Article 3(2)(a) GDPR describes the *lex loci solutionis*.[78] The GDPR is to be applied even if the responsible business is located outside the EU but influences the EU's market. Considering the eleven-digit number of face images that are (allegedly) found in the company's database, it is highly probable that millions of EU citizens are represented in the database. Each monitoring of the behaviour of individuals within the EU falls under article 3(2)(b) GDPR. This means that practically all website operators deploying tracking or profiling measures have to comply with the GDPR.[79]

---

[72] LA Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press, Oxford UK 2014) 5.
[73] Sharon Nakar and Dov Greenbaum, 'Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy' (2017) 23 BU J Sci & Tech L 88, 108.
[74] ibid 116.
[75] *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): GDPR.
[76] *Directive 95/46/EC of the European Parliament and of the Council* of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data: Data Protection Directive.
[77] Thomas Riesz, 'Schutz personenbezogener Daten [Art 8]' in Michael Holoubek and Georg Lienbacher (eds), *Charta der Grundrechte der Europäischen Union: GRC-Kommentar* (2nd edn MANZ'sche Verlags- und Universitätsbuchhandlung, Wien 2019) 171; also see Peter Hustinx, 'The reform of EU data protection: towards more effective and more consistent data protection across the EU' in Normann Witzleb and others (eds), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge intellectual property and information law, Cambridge University Press, Cambridge UK 2014) 65.
[78] Christian Bergauer, 'Artikel 3 Räumlicher Anwendungsbereich' in Dietmar Jahnel (ed), *Kommentar zur Datenschutzgrundverordnung (DSGVO)* (Jan Sramek Verlag, Wien 2021) 26. If a search engine operator, which has its seat or branches outside the EU, analyses the internet conduct of a citizen of a non-EU state during the citizens holiday in a EU country, the GDPR is applicable.
[79] ibid 28. The CJEU being in favour of a broad extra-territorial scope of data protection provisions was visible in its famous Case C-131/12 *Google Spain v AEPD and Mario Costeja González* [2014]. In 2014, when the case was decided, the Data

Furthermore, article 4(14) GDPR defines "biometric data" and explicitly mentions "facial images" as an example thereof. Hence, in principle, Clearview's conduct falls under the scope of the GDPR.

According to article 5(1)(a) GDPR, personal data are only to be "processed lawfully, fairly and in a transparent manner" by both state and private parties. Article 5(1)(b) GDPR states that data are only allowed to be "collected for specified, explicit and legitimate purposes". Article 6 GDPR, entitled "Lawfulness of processing" and listing six alternative prerequisites thereof in its first subparagraph ((a) to (f)), directly links to its preceding provision. Whereas article 6(1)(a) contains the prerequisite of the data subject's consent to the processing of their personal data for at least one specific purpose, the other *literae* mention necessities of different kinds in the sense of a balancing of interests. Clearview's conduct is in breach of article 6 GDPR. Above, it was explained in depth that Clearview has established its business by secretively collecting face images of individuals without a legitimate, pre-defined purpose in order to then process the big data in an equally wrongful manner. Clearview does not have any legal duties or superior interests it must fulfil which would justify the processing. This claim is in line with the argument brought forward by the French National Commission on Informatics and Liberty (CNIL), that led to Clearview being ordered to stop the reuse of photographs available online in December 2021.[80]

Notwithstanding the GDPR's rather clear applicability to the Clearview case, the company has never been sentenced to a penalty as laid down in Chapter VIII of the GDPR. The reasons are to be found in the interpretive flexibility of the Regulation[81] as well as in the complexity of practical implementation of sanction mechanisms. To provide an example, the supervisory authorities (such as which Member States are required to establish based on article 51 GDPR) that could take measures and impose sanctions against parties violating the GDPR, only have the authority to do so within their territory. Enforcement and execution require the cooperation of the respective authorities of the state in which companies have their registered office. Court decisions or findings are not directly enforceable based on the GDPR in other

Protection Directive was in force, not the GDPR. The Court's attitude is transferrable to the extra-territorial scope of the GDPR.

[80] CNIL, 'Facial recognition: the CNIL orders CLEARVIEW AI to stop reusing photographs available on the Internet' (2021) https://www.cnil.fr/en/facial-recognition-cnil-orders-clearview-ai-stop-reusing-photographs-available-internet accessed 28 February 2022. The CNIL accused Clearview of having violated articles 6, 12, 15 and 17 GDPR, without indicating specifically which subparagraphs of each provision had been infringed upon.

[81] For an example, see Simon Hurtz, 'Warum automatisierte Gesichtserkennung so gefährlich ist' Süddeutsche Zeitung (21 January 2020) https://www.sueddeutsche.de/digital/clearview-datenschutz-gesichtserkennung-dsgvo-1.4766724 accessed 29 October 2021.

states in or outside the EU. Enforcement treaties would be required.[82] So far, no joint actions between the EU and the USA against Clearview have been taken. Making a connection to the point of cooperation between different judicial systems, the following section describes different attempts to take legal action against Clearview in the US.

4.2. The legal regulation of facial recognition technologies in the US

The legal answer to facial recognition technologies in the USA is an illustrative example of a legal hotchpotch hindering determined response to companies like Clearview. Some cities have entirely banned the police use of facial recognition technologies, for example, Minneapolis, Boston,[83] and San Francisco.[84] Texas and Illinois have issued laws prohibiting the use of facial recognition technologies to identify people without informed consent. The *ratio legis* behind both laws is the protection of (biometric) privacy.[85] The Texas Business and Commerce Code[86] prohibits in § 503.001(b)(1) and (2) the capturing of biometric identifiers for commercial purposes without informing the individual beforehand and receiving the individual's consent. The fact that Clearview collects face images for commercial interest and the fact that it has not obtained its data subjects' consent renders its conduct illegal under Texan law. The same holds true for Illinois: according to § 15(d)(1) of the State's Biometric Information Privacy Act (BIPA), [87] the corporate use of residents' faceprints is forbidden without explicit consent. Illinois could consequently make Clearview create a specific opt-out form for its citizens.[88]

Following US examples, the European Parliament adopted a (non-binding) resolution banning the use of facial recognition technologies by the police in the beginning of October 2021.[89] The resolution[90] repeatedly stresses the significance of respecting individuals' right to privacy. Additionally, it asks for the ban of private facial recognition databases, Clearview

[82] Bergauer (n 78) 28. Articles 16(2) TFEU and 8(3) Charter of the Fundamental Rights of the European Union also state that an independent authority has to control compliance with data protection rules.
[83] Kashmir Hill, 'Your Face Is Not Your Own' The New York Times Magazine (18 March 2021) https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html accessed 28 October 2021.
[84] Dave Lee, 'San Francisco is first US city to ban facial recognition' (2019) https://www.bbc.com/news/technology-48276660 accessed 28 October 2021.
[85] See Ben Sobel, 'Facial recognition technology is everywhere. It may not be legal.' The Washington Post (11 June 2015) https://www.washingtonpost.com/news/the-switch/wp/2015/06/11/facial-recognition-technology-is-everywhere-it-may-not-be-legal/ accessed 08 October 2021.
[86] *Texas Business and Commerce Code* (2003).
[87] *740 ILCS 14/ Biometric Information Privacy Act Illinois Biometric Identification Privacy Act: BIPA* (2008).
[88] Clearview AI, 'Privacy & Requests' https://www.clearview.ai/privacy-and-requests accessed 10 March 2022. Although the success of this consequence remains doubtable, Illinois' example shows that legal statutes can have an influence on powerful companies like Clearview.
[89] Melissa Heikkilä, 'European Parliament calls for a ban on facial recognition' Politico (06 October 2021) https://www.politico.eu/article/european-parliament-ban-facial-recognition-brussels/ accessed 27 October 2021.
[90] European Parliament, *Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters* (Brussels 2021).

being explicitly mentioned as an example of a company acting illicitly in the field.[91] The examples provided from the USA prove that legal provisions can hinder malicious tech companies to operate, at least for a certain period. The sustainability of these successes is however questionable. First, until an affected citizen files a complaint against Clearview, it will be unknown if the company is continuing to collect data in secrecy in Texas or in Illinois. Second, in the common law system of the USA, only the Supreme Court can issue binding precedents that would render Clearview's machinations illegal (or unconstitutional) in the entire country. Until this happens, if it ever does, Clearview can easily circumvent US States in which its conduct is deemed illegal, and extensively expand in US States where its technology has not been banned yet. This inconsistent, uncoordinated legal attitude towards Clearview makes it easy for the latter to constantly expand. Subsequently, this last statement will be demonstrated with examples of futile attempts to proceed against Clearview.

4.3. Futile actions against Clearview

Since the Clearview case was made public in 2020, there have been several attempts at proceeding against the tech firm by individuals, NGOs, and governments. Public authorities from several states have ordered Clearview to cease its machinations. One of the most recent examples is the one of the Office of the Privacy Commissioner of Canada (OPC): the authority has ordered Clearview to stop operating on its territory and to delete all photographs of Canadian citizens. Clearview has lodged a complaint against the ban to operate before the Supreme Court of British Columbia (Canada).[92] It remains to be seen how the Court will decide. In the EU, individuals must address Clearview directly in order to demand the deletion of their data in the company's database.[93]. In Hamburg, Germany, the local data protection authority (Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit, HmbBfDI) started to act against Clearview[94] only after a citizen had gone against Clearview directly and without success and had therefore requested the authority's help.[95] Disappointingly, Clearview was just ordered to delete hash values, the mathematical representations of biometric profiles.

---

[91] ibid, para 28.

[92] Tomas Rudl, 'Clearview AI zieht gegen kanadische Datenschutzbehörde vor Gericht' (2022) https://netzpolitik.org/2022/biometrie-clearview-ai-zieht-gegen-kanadische-datenschutzbehoerde-vor-gericht/ accessed 15 February 2022; Also see James Vincent, 'Clearview AI ordered to delete all facial recognition data belonging to Australians' (2021) https://www.theverge.com/2021/11/3/22761001/clearview-ai-facial-recognition-australia-breach-data-delete accessed 28 October 2021. In 2021, the Office of the Australian Information Commissioner ordered Clearview to destroy the entirety of images and facial templates of residents in its database. In response, one of Clearview's lawyers affirmed the company's legality, as has been done various times before.

[93] Rudl (n 92).

[94] *Bescheid gegen Clearview AI erlassen* (2020).

[95] Patrick Beuth, 'Hamburgs Datenschützer will Clearview zur Datenlöschung zwingen' (2021) https://www.spiegel.de/netzwelt/web/gesichtserkennung-hamburger-datenschuetzer-will-clearview-zur-datenloeschung-zwingen-a-9227eca6-0730-400a-946b-c126d3866353 accessed 15 February 2022.

NGOs have also filed complaints against the tech firm in at least five European countries,[96] as well as the American Civil Liberties Union (ACLU) in the USA.[97]

Despite legal backlashes and societal pressure, Clearview appears to be rather unimpressed by the actions that have been taken against it; on the contrary, it has expanded incessantly. So far, there has been no clear court ruling stating that Clearview has been engaging in illicit and illegal conduct. Even if such rulings will be issued in the future, it will be impossible to control how the company reacts to the orders because of the secrecy of its operations. Most probably, only hash values will be deleted, not photographs, as was the case in Hamburg.[98] Even if facial recognition technologies were to be banned, as the EU parliament has recently demanded, it would be impossible to ensure that no sensitive data appeared in untransparent databases and that they were not deployed in an illegitimate manner.[99] Even though the HmbBfDI doubts that Clearview's business model is legal in the EU, it equally doubts that the order to delete data would be viable. Clearview would need information about its data subjects' domiciles, which is an unrealistic requirement.[100]

Besides the concerns competent authorities have voiced with regard to the legal handling of Clearview, the common problem of all provisions applied in mentioned actions is that they apply *ex post*: only after illicit conduct by tech companies has taken place, the law reacts. The reactive character is the corollary of the extreme discrepancy between the pace of development of technology and law. An additional problem is the focus on territoriality:[101] competent authorities can only take action for "their" citizens and on their territory. Questions of competence are often unclear and play into the hands of tech companies. The harmful consequences for Clearview's data subjects become visible in the previously discussed futile actions against the enterprise and emphasize the need for a more fundamental legal answer to the dangers of online surveillance and facial recognition technologies.

[96] Bill Goodwin, 'NGOs file complaints against Clearview AI in five countries' (27 May 2021) https://www.computerweekly.com/news/252501435/NGOs-file-complaints-against-Clearview-AI-in-five-countries accessed 04 February 2022.
[97] ACLU, 'Illinois Court Rejects Clearview's Attempt to Halt Lawsuit against Privacy-Destroying Surveillance' (2021) https://www.aclu.org/press-releases/illinois-court-rejects-clearviews-attempt-halt-lawsuit-against-privacy-destroying accessed 04 February 2022.
[98] This means that the original data would be retained, and numerous negative effects are speculated about. First, we do not know what Clearview will do with the pictures it is legally allowed to keep. It is well possible that the company will again generate hash values of these pictures after some time. Second, Clearview can still sell face images. Third, chances are high that companies which had bought face images and hash values from Clearview before the deletion order saved both in their computer systems. Additionally, Clearview's data subjects have not consented to the company owning their face images,
[99] Rudl (n 92).
[100] ibid.
[101] In contrast to cyberspace, laws still respect territorial borders.

In the subsequent chapter, the case is made for such in the form of the horizontal application of the fundamental right to privacy under EU law. The Court of Justice of the European Union (CJEU) has dealt with the horizontal application of some fundamental rights in various cases, thus the Court's reasonings are taken as a point of reference.

5. Addressing facial recognition technologies with the horizontal application of the fundamental right to privacy

From a historical point of view, fundamental rights have protected citizens from illegitimate and excessive encroachment from public power.[102] Their formalisation into constitutional principles occurred as a reaction to power imbalances.[103] Tech firms, instead, can be said of having been shielded from issues of political accountability so far,[104] in spite of their *de facto* regulatory power. This has allowed Clearview to profit from regulatory deficiencies on the level of laws described in the previous chapter. The horizontal application of the fundamental right to privacy would take this power to regulate into account. After a brief examination of the importance of the fundamental right to privacy in the EU, the current court practice of the CJEU in relation to horizontal application of fundamental rights is discussed in order to make the argument for the application of the practice to the fundamental right to privacy.

5.1. The EU's approach towards the fundamental right to privacy in the Digital Age

The right to privacy enjoys universal value. Besides national constitutions, it is manifested in international and supranational legal frameworks, such as of the UN, the OECD, the CoE, the ECOWAS or the EU.[105] The latter has taken an innovative stance on the value of privacy in the Digital Age, a stance that meets the challenges of the fundamental right in cyberspace best. With its article 8 of the Charter of Fundamental Rights of the European Union (CFR), entitled "Protection of personal data", the EU has created a structurally autonomous right that widens the right to privacy protected by article 8(1) of the European Convention on Human Rights (ECHR),[106] on which it is based. The protection of personal data requires an independent scope of protection, although it forms part of the more general respect of private and family life enshrined in article 7 CFR.[107] Ascribing the protection of personal data the status of a *lex specialis* is the appropriate step towards an adequate protection of privacy within

[102] Sonya Walkila, *Horizontal Effect of Fundamental Rights in EU Law* (Europa Law Publishing, Groningen 2016) 199.
[103] Volker Epping, *Grundrechte* (9th edn Springer, Berlin 2021) 1-3.
[104] See Gavin W Anderson, *Constitutional Rights after Globalization* (Hart Publishing, Oxford UK, Portland OR 2005) 150.
[105] Bygrave (n 72) 31.
[106] Riesz (n 77) 163; Peter Hustinx (n77) 63.
[107] Riesz (n 77) 162, 170. Interestingly, the scope and limits of article 8 CFR follow the regulations in the EU's secondary law, in the GDPR and its precursor, the Data Protection Directive. That is, the GDPR (and before the Data Protection Directive) serve as interpretation aids for the fundamental right.

the digital realm. The subsequent discussion evolves around the right to protection of personal data.

In the decisions of *Digital Rights Ireland* and *Schrems*, the CJEU demonstrated how it perceives the rights to privacy and to protection of personal data as the rights most immediately affected by surveillance. The two rights "provide a proxy for assessing fundamental rights intrusions by surveillance."[108] The scope of protection of the provision is rather broad. Not only does it provide individuals with protection from public authorities, but it also conveys positive duties on the State to protect citizens with regards to data processing by private parties.[109] This contrasts with article 7 CFR that clearly provides protection against interference by public and private parties,[110] a negative right. Since it is predominantly private parties like Clearview that engage in surveillance, it would not satisfy the value of and desirable legal advancement immanent in article 8 CFR if it could only encompass positive rights of the State towards citizens. In fact, if there is one provision that must be opened in favour of horizontality for the sake of effectively safeguarding the fundamental right to privacy in cyberspace, it is the right's *lex specialis* in the form of the right to data protection, and not the general right to respect of private and family life. In order to secure privacy to the furthest possible extent, the scopes of protection of both rights have to be combined. The expression "protection" (from article 8 CFR) should not be interpreted narrowly but also in the sense of "respect" (from article 7 CFR).[111] If private companies like Clearview were constitutionally obliged to protect data, clandestine surveillance could hardly be interpreted as being legitimate.

5.2. The current horizontal application of fundamental rights in the EU

The horizontal application of fundamental rights is not an innovative concept. The foundations for the horizontal application of fundamental rights were laid as early as the

[108] David D Cole, Federico Fabbrini and Stephen Schulhofer (eds), *Surveillance, Privacy and Transatlantic Relations* (Hart studies in security and justice, Hart Publishing, Oxford UK, Portland OR 2017) 19; Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] (CJEU); Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] (CJEU); also see the European Commission, *Proposal for a Regulation of the European Parliament and of the Council on Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC* (Brussels 2020) 13, in which general online monitoring obligations are prohibited. Although the reasoning is the protection of internet users' freedom of expression and freedom to receive information, the prohibition of surveillance will also protect the users' right to privacy.
[109] Riesz (n 77) 180.
[110] See Cole, Fabbrini and Schulhofer (eds) (n 108) 217.
[111] Without going into detail, the concepts laid down in article 25 GDPR, data protection by design (1) and data protection by default (2), are only addressed towards tech firms. The concepts are deprived of effectiveness if the responsible parties are not bound by the right to data protection. If they were, they would have a constitutional obligation to take technological measures to ensure privacy from the outset. This is of particular importance in the case of surveillance with facial recognition technologies.

1970s.[112] The most important CJEU cases on the matter have treated problems in the area of employment, where the recourse to fundamental rights allowed strengthening the weaker party's (i.e. the employee's) position.[113] According to article 51(1) CFR, all organs and bodies of the EU as well as Member States are bound by the fundamental rights guaranteed in the CFR when they are implementing Union law. Therefore, a common argument is that the CFR cannot establish horizontal effects and that private parties cannot fulfil the conditions of article 52(1) CFR, which states that limitations on the rights and freedoms guaranteed by the CFR must have a legal basis and are subject to the principle of proportionality.[114] These arguments against horizontality are not convincing. Horizontal effect is not explicitly excluded in article 51 GDPR: in *Fransson*, the CJEU clearly advocated a broad interpretation of the CFR's scope and recognised that horizontal situations can be a part of such broad interpretation.[115] This view is in line with the Court's ruling in *Defrenne*: "[T]he fact that certain provisions […] are formally addressed to the Member States does not prevent rights from being conferred at the same time on any individual who has an interest in the performance of the duties thus laid down."[116] The Court reasoned that the mandatory nature of the right to equal pay of women and men leads to the prohibition on discrimination of public authorities and private parties alike.[117] The focus on the fundamental law's mandatory nature leads to the assumption that the decision was based on a substantive constitutional point. In *Defrenne*, the CJEU demonstrated that it was even in favour of a wide-ranging applicability of horizontality.[118]

Although *Defrenne* was decided long before the CFR was introduced, it has not been overruled, quite the contrary.[119] More recently, the CJEU ruled that "the fact that certain provisions of primary law are addressed principally to the Member States does not preclude their application to relations between individuals."[120] In the *Mangold* case, the CJEU argued that general principles of EU law could have a horizontal effect. The exception based on general principles was established with regard to the non-horizontality rule.[121] In the subsequent *Kücükdeveci* case, the Court showed that the right to non-discrimination (article 21(1) CFR)

[112] Eleni Frantziou, *The Horizontal Effect of Fundamental Rights in the European Union* (Oxford Studies in European Law Ser, Oxford University Press, Oxford UK 2019) 60-61.
[113] Walkila (n 102) 199.
[114] See for example Case C-282/10 *Maribel Dominguez v Centre informatique du Centre Ouest Atlantique, Préfet de la région Centre* [2012] (CJEU), Opinion of AG Trstenjak, para 83.
[115] Case C-617/10 *Åklagaren v Hans Åkerberg Fransson* [2013] (CJEU), paras 18-21; Frantziou (n 115) 84-85.
[116] Case 43/75 *Gabrielle Defrenne v Société Anonyme Belge de Navigation Aérienne Sabena* [1976] (CJEU) para 31.
[117] ibid, para 39.
[118] Frantziou (n 112) 62.
[119] Thus, article 23 CFR, stating the equality between women and men, equally enjoys horizontal application. In the matter, the horizontal effect of the fundamental right has not been questioned on grounds of article 51(1) CFR.
[120] Case C-684/16 *Max-Planck-Gesellschaft zur Förderung der Wissenschaften eV v Tetsuji Shimizu* [2018] (CJEU), para 77.
[121] Case C-144/04 *Werner Mangold v Rüdiger Helm* [2005] (CJEU), paras 74-78.

could produce horizontal effect.[122] Frantziou correctly states that the fundamental protections in titles I to IV of the CFR guarantee minimum individual rights in a universal manner. A specification that they only apply to governmental authorities cannot be deduced from the provisions.[123] Therefore, it appears that the tendency goes in the direction of the horizontal application of mandatory and unconditional provisions of the CFR.[124] As a reaction to the concern of senior courts in some Member States about horizontality exceeding Treaty articles, including the CFR, the CJEU imposed restrictions on the concept. Especially as far as directives are concerned, they are not horizontally applicable.[125] But the horizontal application of fundamental rights (primary law) in the area of employment has allowed individuals to realise rights that they could not have enjoyed by reference to directives only.[126] It was shown above that the GDPR, a regulation, couldn't effectively protect individuals from privacy infringing surveillance carried out with facial recognition technology. In analogy to the area of employment regarding power asymmetries between private parties, the recourse to horizontality might remedy this deficient secondary law protection of the fundamental right to privacy.

5.3. The horizontal application of the fundamental right to privacy

Fundamental rights historically represented a defence for citizens against state power. But currently, citizens are confronted with equally severe threats posed by private entities exhibiting substantial social or economic power,[127] the case of Clearview serving as a striking example. In the area of employment, where mostly the legal relationship between two private parties is concerned, the horizontal application of fundamental rights does not appear far-fetched. The same holds true for data protection. Taking the abovementioned *ratio legis* of the counterbalance to power asymmetry, powerful private tech companies must be obliged to respect fundamental rights. Article 8 CFR cannot develop its full (and necessary) potential if its application is not adapted to the change in power relations of the internet. It has to be ascribed mandatory nature like the right to equal pay of women and men.

[122] Case C-555/07 *Seda Kücükdeveci v Swedex GmbH & Co. KG* [2010] (CJEU), paras 27, 43. The ruling is in line with article 6(3) TEU, which holds that fundamental rights represent general principles of EU law. In *Kücükdeveci*, the CJEU showed this for the first time, hence the case's significance.
[123] Frantziou (n 112) 86.
[124] See Eleni Frantziou, '(Most of) the Charter of Fundamental Rights is Horizontally Applicable, ECJ 6 November 2018, Joined Cases C-569/16 and C-570/16, Bauer et al' (2019) 15 Eur Const L Rev 306.
[125] Jeremias Adams-Prassl and Sanja Bogojević, *Great Debates in EU Law* (Great Debates in Law, Macmillan International Higher Education, Red Globe Press, London UK 2021) 96.
[126] ibid 111.
[127] Walkila (n 102) 199. Also see Anderson (n 104) 111-12.

As was written above, several legal scholars argue that article 8 CFR cannot directly bind private parties.[128] Riesz claims that article 8 CFR unfolds indirect third-party effect through data protection by secondary law that also addresses private parties.[129] The fundamental right's content therefore becomes enforceable between private entities through secondary law.[130] Riesz further argues that in the area of data protection this is of eminent importance because private enterprises can jeopardize the privacy of data subjects just as much as state authorities.[131] Nevertheless, he does not take into consideration that article 8 CFR has to unfold direct third-party effect in order to address the jeopardy he fears. For the value of fundamental rights does not change whether they are violated by the activities of a governmental body or a private party, the protection of private parties should not be limited to vertical relations between citizens and state.[132] According to Anderson, the ones being the subjects of rules must be protected from the ones making the rules by the constitution, no matter which party belongs to which sphere (private or public).[133] Although Anderson makes the argument in connection with societal constitutionalism, his reasoning is well applicable to cyberspace, where the rules are predominantly made by tech firms. For example, the ones subjected to Clearview's facial recognition tool have to be protected by the constitution, that is, by fundamental rights like article 8 CFR. In its famous *Google Spain* case from 2014, the CJEU declared that the rights to privacy (article 7 CFR) and to data protection (article 8 CFR), in conjunction with the Data Protection Directive, give individuals the possibility to request to have their personal data removed from internet search engines within the EU.[134] The Court then failed to assess why a violation of articles 7 and 8 CFR by private parties, *in casu* Google, undermines the effectiveness of the fundamental right to privacy.[135] In turn, it asserted that the obligation to delete data could directly be applied to search engine operators.[136] Hence, in general, the grounds for the CJEU's decision can be viewed as approval of a horizontal application of the right to privacy.[137]

[128] See for example Riesz (n 77) 213.
[129] ibid.
[130] See Case C-131/12 *Google Spain v AEPD and Mario Costeja González* (n 79), para 69.
[131] Riesz (n 77) 214.
[132] Walkila (n 104) 174; Adams-Prassl and Bogojević (n 129) 102. Several Advocates General of the EU have called for the distinction between public and private to be abandoned in case of non-implemented directives. See for example Case C-152/84 *M. H. Marshall v Southampton and South-West Hampshire Area Health Authority (Teaching)* [1986] (CJEU), Opinion of AG Van Gerven, 4388.
[133] Anderson (n 106) 146-47.
[134] Case C-131/12 *Google Spain v AEPD and Mario Costeja González* (n 79), para 97.
[135] Frantziou (n 114) 111.
[136] Case C-131/12 *Google Spain v AEPD and Mario Costeja González* (n 79), para 17.
[137] Frantziou (n 114) 111.

The effectiveness of personal data protection can be substantially enhanced if individuals have the ability to directly invoke fundamental rights, rather than if the value is indirectly expressed in statutes ("secondary laws" in EU terminology). The EU provides an illustrative example of this claim: in case of the absence of transposition measures for a directive in a Member State, it would be impossible for the latter's national courts to interpret national law in harmony with the directive. Instead, fundamental rights would represent an additional and practical means for the CJEU to resolve a case without individuals only having the possibility to bring an action against the State to claim their basic rights.[138] Walkila's argument can be generalised, also for situations in which harmonising regulations like the GDPR are applicable: invoking fundamental rights always represents the direct way to claim the violation of fundamental rights. Additionally, the problem of territoriality could be circumvented, as fundamental rights apply to everybody, regardless of their nationality. One of the problems leading to futile actions against Clearview could thus be addressed more efficiently. With reference to the argument of the right to privacy taking precedence over economic fundamental rights in "digital society", it is argued that if a private company like Clearview had to respect the fundamental right to personal data protection, it would be far easier to prosecute it for the violation of this right. The tech firm's commercial interests would not be balanced against the data subjects' privacy rights, as balancing suggests equality between parties. Applying the right to privacy horizontally would mean that it would first be assessed if a technology allowed for a reasonable respect of privacy. Only if the latter could be ensured, the commercial interest of the developing tech company would be taken into consideration.[139] Before drawing an affirmative conclusion in light of the horizontal application of the right to privacy, the discussion has to be complemented with unresolved problems.

5.4. Unresolved problems

Lodging a claim against a fundamental rights violation of another private party can be seen as a jurisgenerative act. The blurring of the division between public and private leads to the situation that subjects of a constitutional framework become the latter's co-authors.[140] This can be viewed as a consequence of the internet's generativity. Adams-Prassl and Bogojević

[138] Walkila (n 104) 204.
[139] The criteria to check whether a private company has breached its data subjects' privacy has to happen in analogy to criteria that apply to the State: For example, if the State carried out the same machinations as Clearview, would it violate citizens' right to personal data protection? The analogy can be made because, again, power relations are comparable in the physical and cyberspace.
[140] See Frantziou (n 114) 131.

fear that legal uncertainty is the outcome of this co-authorship.[141] The aspect of jurisgeneration equally applies to courts. Since it would be precedents that would legally establish the horizontal application of the right to data protection, we would deal with judge-made law. Separation of power would be undermined to a certain degree; the scope of democratically made legal statutes would be exceeded. The abstract nature of fundamental rights and the fact that they therefore have to be balanced against each can also endanger legal certainty that legal statutes are able to guarantee.

Walkila argues that the horizontal effect of fundamental rights is justifiable precisely because of the blur, that is, the entwinement of the private and public sphere in the digital realm, despite current inconsistencies and a lack of structure.[142] In principle, the argument is to be followed. New societal structures require adjustments. Legal certainty and genuine separation of (all) powers can otherwise not be secured in the long term. In order to control the proliferation of horizontality and to keep it as specific as possible, it is only the very narrow right to data protection, in its national specificities, that is to enjoy horizontality. In judicial systems without such a *lex specialis*, the establishment of horizontal application of the right to privacy would have to be carried out even more carefully. The right to privacy is not absolute after all, other fundamental rights can outbalance it under given conditions. Moreover, fundamental rights are not the solution to every (novel) problem society faces. But due to their fundamentality, they have a stabilising and legitimising effect. To address the challenges their scope extension provokes, democratic debates as well as interdisciplinary educational work regarding power asymmetries in cyberspace and the resulting privacy endangerment have to follow.

6. Conclusion

Under the guise of providing society with a security-enhancing tool, Clearview clandestinely allows the surveillance of its data subjects in deliberate disregard of their fundamental right to privacy. A business model that is based on the violation of the right to privacy can only exist and operate (even after societal disapproval has been voiced) if there are no laws prohibiting the machinations or if the existing legal provisions turn out to be ineffective. With regards to facial recognition technologies, especially in the case of the one developed by Clearview, the law has appeared to be unable to protect personal data and therefore privacy. During the last

[141] Adams-Prassl and Bogojević (n 125) 108.
[142] Walkila (n 104) 198-200.

two years, different judicial systems, with the EU being among the most advanced ones, have started to address the perils of facial recognition technologies with more focus. These approaches are steps into the right direction but have turned out to be paper tigers. They represent a reaction to private regulation of society in the online world that does not meet the challenge of new power asymmetries within the private sphere.

Rather than reaction, fundamental action is required to meet the challenges of the destabilizing tendencies generative cyberspace has. Fundamental rights apply to all human beings; they do not depend on citizenship. Considering the absence of borders in cyberspace, invoking universal rights is crucial to prevent legal hotchpots that make it impossible to sustainably prosecute private tech firms. The case of Clearview shows how facial recognition technologies enable surveillance – surveillance that rhizomatically spreads through society and allows for social control. Faces of human beings are de-humanised as they are used to generate monetisable data. Privacy is deprived of its value, for both individuals and society. The unprecedented space of development of the internet does not correspond to an equally fast change of fundamental values. In fact, the broad right to privacy must be further strengthened in light of unilateral economic behaviour. Regarding the CJEU, its jurisdiction concerning the horizontality of fundamental rights is to be extended to the right to data protection. Although there are unresolved problems with regards to the practical implication of this extension, it represents the best way forward to consider the power of private tech companies.

Clearview has done irreversible damage to the fundamental right to privacy. It is now important to at least learn from the Clearview case and to acknowledge that tech companies have the same regulatory power in cyberspace as state authorities have in physical space. The wheel does not have to be reinvented; it is the reliable concept of fundamental rights that must be adapted to the conditions of cyberspace. The raised research question can therefore be answered as follows: the horizontal application of the fundamental right to privacy ensures a (more) effective protection against business models being based on the violation of the fundamental right to privacy to the extent that it addresses the root of the problem, which is the significant power asymmetry between tech companies and their data subjects within cyberspace.