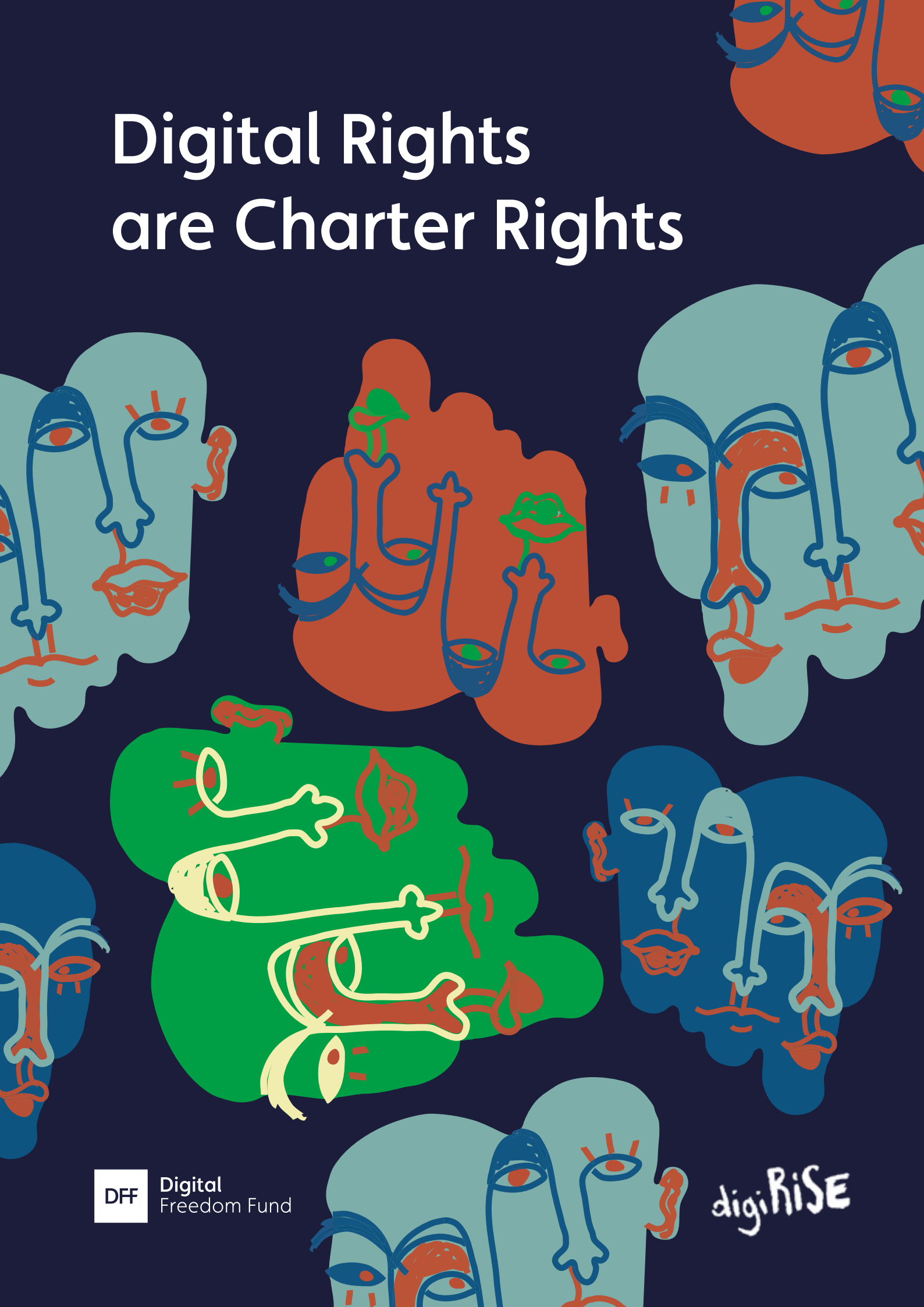
Digital Rights are Charter Rights



DFF Digital Freedom Fund

digiRISE

digiRiSE

Developing Information, Guidance, and Interconnectedness for (Charter) Rights Integration in Strategies for Enforcement

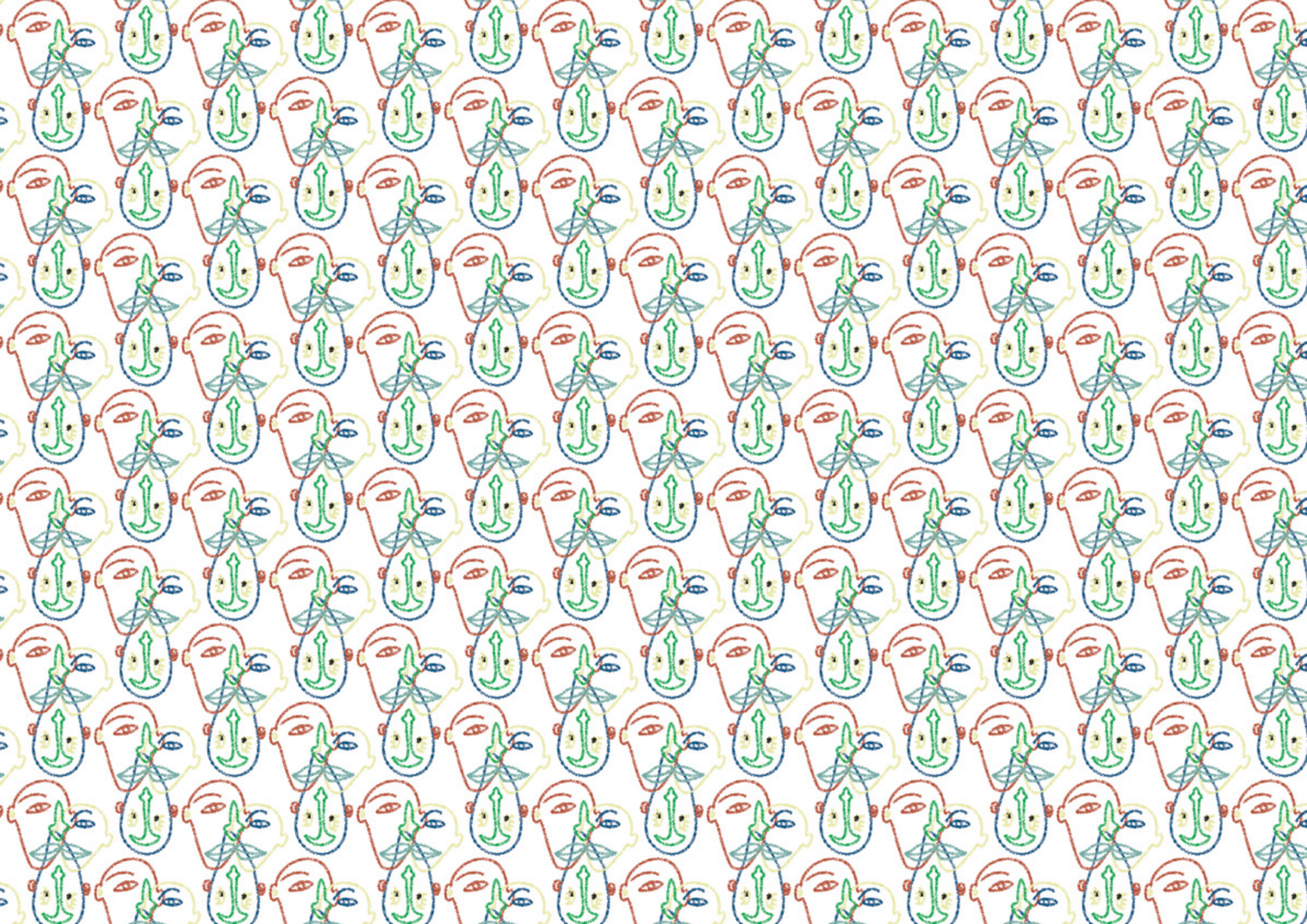


Table of Contents

Editorial

by Alexandra Giannopoulou

A considerable number of everyday interactions and relationships between individuals, public and commercial entities have shifted online and are mediated by digital technological infrastructures. These new means of interactions and mutual engagement in the digital realm are emerging at a scale and speed previously unattainable. Among the research that articulates, analyses, and criticizes the adverse effects of informational and technological systems on individual citizens, emerges also a discussion on systemic societal harms. Alternative visions and proposals to counter these systemic harms provoked by or amplified through technological and informational systems are making their way in contemporary policy, academic, community, and civil society fora.

This essay series highlights the link between digitalisation, datafication and fundamental rights. This digital transformation brings, according to the European Commission, "new opportunities to make fundamental rights more effective but also brings challenges".[1] Through the essays, we invite the reader to contemplate the importance of fundamental rights protections in the digital sphere as well as the instrumental role of the EU Charter of fundamental rights (EU Charter) in countering systemic oppressions, harms, and injustices which appear encoded in technologies at hand. The emancipative potential of the EU Charter as a means of resistance in technological bias and oppression sits at the core of this series.

The EU Charter, drafted at the turn of the Millennium, represents an important contribution to the canon of binding legal instruments that make up the European human rights framework. It exists in addition to and alongside other international and European human rights instruments like the Universal Declaration of Human Rights (UDHR), the European Convention on Human Rights (ECHR), a range of subject-matter specific instruments as well as national constitutions and "bills of rights".

The Charter is binding on EU institutions as well as Member States when they act within the scope of EU law. It can therefore play a role in filling gaps in and between existing national and international human rights frameworks and provide an additional layer of protection. With the entry in force of the Treaty of Lisbon, the Charter became a legally binding instrument, with the same legal value as the Treaties. The Charter is therefore becoming the primary avenue for rights-based claims since it can offer tangible opportunities for individuals to directly enforce fundamental rights enshrined therein before the courts, including in regulating relationships between private parties.

The Charter is becoming the primary avenue for rights-based claims since it can offer tangible opportunities for individuals to directly enforce fundamental rights enshrined therein before the courts, including in regulating relationships between private parties.

However, it has been shown in practice that "references to the charter are formal, declaratory, even decorative and combined with references to the ECHR, without distinction".[2] Therefore, it becomes clear that the potential of many provisions is still in need of further exploration.

The host of rights and freedoms that the Charter of fundamental rights articulates are creating the image of a modern (digitally aware) human rights instrument. It is the only international binding legal instrument with a distinct mention to a right to data protection, clearly distinguished from the right to privacy. As evidenced in case law and discussed in many of the essays, articles 7 and 8 of the EU Charter appear as primordial foundational rights around which most digital rights cases are built. However, and as evidenced by the essays included in this series, there are many Charter rights and freedoms which are or can be a solid foundation to build digital rights strategic litigation.

The Charter's potential for protecting digital rights goes even further and includes a host of other rights and freedoms that - in the face of the ongoing digitisation and datafication of everyday tasks/lives - are likely to be of growing importance and utility in the digital sphere. These rights and freedoms, like all human rights, are designed to uphold European Union values and the rule of law, and ultimately to protect individuals and groups from being subject to injustice, discriminatory treatment, and exclusion from opportunity. Importantly, such abuses can now increasingly be observed in the digital domain in connection with the use of artificial intelligence (AI), access to and (selective) provision of digital goods and services, the establishment and expansion of data-extractive business and revenue models and the growing reliance on technology-mediated decision-making processes by both public and private entities.

Many of the cases discussed in the essays included in this series address direct harms and highlight the impact of fundamental rights violations incurred by invasive techno-social systems. Creating a corpus of texts which attempts to showcase the link between fundamental rights and digital rights is ultimately an attempt to address the legacy of power in the context of digital technologies as well as an opportunity to provide critique on the value of fundamental rights protections in certain contexts or environments.

Relating to issues carrying a high ideological charge, the essays cannot maintain a claim of universality but rather an attempt to map out important fields where impact is or can quickly become visible. We have invited authors stemming from different legal, policy, academic or other fields, covering issues including (but not limited to) the digitalisation of asylum processes, freedom of expression and content moderation, equality and algorithmic non-discrimination, digital welfare and digitalised public services in general, collective bargaining and platform workers. The essays included in this series present an array of legal, social, and technological discourses, but they all share a common approach towards solidifying the critical thinking that supports the importance of fundamental rights protections in digital technological systems. We hope this special issue inspires more sustained, critical, and reflexive thinking, and a deeper encounter with fundamental rights in the digital field as we strive for respect with regard to digital rights protections.

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Strategy to strengthen the application of the Charter of Fundamental Rights in the EU", COM(2020) 711 final, 2 December 2020, p. 2.

[2] J. Adams-Prassl & M. Bobek, Introduction in M. Bobek & J. Adams-Prassl (eds.), The EU Charter of Fundamental Rights in the Member States, Hart publishing, 2022, p.7.

Article 11: When public becomes private and everybody is a suspect - freedom of expression and information in early 21st century

Anna Mazgal, *Wikimedia Europe*

Introduction

Art. 11 on freedom of expression and information is rooted in the European paradigm of open and free discourse that privileges taking risks by allowing people to communicate freely and perhaps cross boundaries of what is accepted over preventive censorship. This paradigm is also founded on a belief that in exercising this right, citizens may require special protection from the state's attempts to manage dissent. The online communication landscape is mainly intermediated by platforms. This creates a challenge for the exercise of our freedom of expression and, at the same time, a need to expand the free speech protection to include corporations and their algorithmic speech-moderation machines. That exercise comes with trade-offs.

Internet-accelerated exchange of information poses a challenge to both users and legislators in Europe because of the need to apply a proportionate and appropriate balance of all rights that might be affected by online information moderation. While legislators have been developing legal frameworks aiming to eliminate illegal speech, users, and particularly racialised and queer communities, are most affected by harmful speech. This harmful speech often becomes its own form of censorship because it is recognised as a form of suppression through violent silencing[1]. For these reasons, there is a need for robust protections of the legal forms of expression, not only by not interfering with it but through positive obligations of the state.[2]

The amount of the information produced, disseminated, and exchanged through intermediating platforms far exceeds any human processing capacity. So, European legislators opted to task internet intermediaries, or platforms, to take day-to-day decisions on what is and what isn't allowed within their services. A privatised system of curating freedom of expression online has therefore emerged.

Code is law, but so are the terms of service

A quick look at the legislation emerging in the EU in the last 5 years provides mounting evidence that the online platforms' terms and conditions (T&C) have become key in setting up governance frameworks for the regulation of freedom of expression. These contractual obligations between an intermediating platform and its users, especially if and when resulting from legal obligations, create an ecosystem of private enforcement online.[3]

For instance, platforms must incorporate the copyright exceptions referred to in the Directive on copyright in the Digital Single Market (Copyright Directive) in their T&Cs. Its article 17 allows a user to use or refer to a copyrighted work of a third person for example for the purpose of quotation, criticism, review as well as use for the purpose of caricature, parody or pastiche. At the same time article 17 creates a content moderation obligation under which platforms can use automated content moderation on uploaded content to enforce copyright protection. This obligation turns T&Cs into a framework for balancing conflicting rights of a rightsholder and of a user benefitting from a copyright exception to both ensure freedom of expression and eliminate illegal content.

Similarly, the regulation on addressing the dissemination of terrorist content online (TERREG) creates obligations for platforms to include provisions in their T&C addressing the misuse of their services through dissemination of terrorist propaganda (article 5(1)). It means that the implementation of legal provisions in their internal systems and enforcement are left for the platforms to determine. While that makes sense from the perspective of the freedom to conduct a business, it shifts the decision-making power in qualifying terrorist content entirely to a private company.

In an attempt to limit the potential for overreach of content policing, legislators oblige the platforms to apply "specific measures" with consideration to users' fundamental rights concerning freedom of expression and information (article 5(3)(c)). This practice derives from a specific normative framework which highlights the importance of ensuring fundamental rights respect within big private platforms: on a global level, the Guiding Principles on Business and Human Rights adopt such objectives. These principles are referred to directly in recital 12 of another landmark EU legislation, the Digital Services Act (DSA). The impact of these normative frameworks is difficult to estimate without evidence-based research.

The DSA seems to provide an interesting reinforcement for free expression because it states that the mandatory internal complaint-handling system can be used for complaints not only against specific decisions by a platform, but also against fundamental rights violations.[4]

Sauron's eye

What exactly is required of the platforms to weed out undesired content? In the case of TERREG and the Copyright Directive, the focus is on ensuring the unavailability of illegal material. Both legal acts point to a range of measures to ensure removal or blocking of the illegal content. Notably, throughout the legislative process, the provisions requiring platforms to use algorithmic tools to sift through all content in search for illegal bits were considered extremely controversial for each of these European legal acts. In the case of the Copyright Directive, article 17 generated vehement opposition from civil society and a number of street protests. Wikipedia's Spanish, Italian, and Polish language versions were turned off in protest.[5]

The use of software to match uploads with a database of illegal content (in both cases of copyright and terrorist propaganda) is similar to an airport security scan: the point is to "see" illegal material; but the machine reveals all the content that goes through it. The mere existence of such systems makes them ripe for abuse, opponents of the introduction of these systems argue. In both TERREG and Copyright Directive, the language used for these measures is marked with circumlocution: while the copyright directive mentions "best efforts to ensure the unavailability of specific works", TERREG outlines "technical measures" that need to be bound with "appropriate and effective safeguards, in particular through human oversight and verification".

The TERREG and Copyright Directive either mandate or enable platforms to use content filtering, respectively. The algorithms used for content filtering by these platforms are all proprietary, so little can be said about their actual effectiveness, accuracy, and ability to understand context. For this reason, human oversight is extremely important. However, based on known practices in human content verification by platforms, such as very short time to evaluate a piece of content and little knowledge of cultural and social context by the moderators,[6] it is difficult to say if it can be effectively performed.

Encryption may become the next victim to this generalised approach amounting to a risk management strategy in which it is better to look at everything in order to catch online illegal content. The proposal for a regulation laying down rules to prevent and combat child sexual abuse imposes an obligation on platforms to scan private communications of all users, including communications protected by encryption. While safety and wellbeing of children is of paramount importance, the proposed "chat control" has been heavily criticised by civil society, the European Data Protection Supervisor as well as the German government.[7]

Platforms play a role in various types of enforcing freedom of expression limitations. For example, payment blockades crippled Wikileaks of 95% of its revenues when PayPal, Mastercard and Visa stopped accepting donations and no legal proceeding was ever initiated against Wikileaks.[8] More recently, the Council of the EU suspended broadcasting licences of Russia Today (RT) France (among others) across the EU, citing excessive propaganda and distorting facts that became a threat to international security after Russia's invasion in Ukraine. While the decision was upheld by the General Court of the European Union, some experts argue that the measure lacked legitimacy and was not proportionate, because it concerned not only illegal content but also an ability to provide access to information that wasn't illegal.[9]

A new, clean internet?

It seems that through a concerted legislative effort to ensure elimination of illegal content, freedom of expression is taking a hit. The exercise of the right to freedom of expression online can only be done when one expresses oneself. So, any algorithmic tool that preemptively filters our online speech on upload will be in direct breach of article 11 of the Charter.

The balancing exercise grounded in politically charged concepts such as public security and safety on the one hand and in corporate secrecy of proprietary technology on the other hand, creates legislation that is looked upon in other parts of the world and copied in jurisdictions that have a disastrous track record in safeguarding human rights and freedoms. Decisions such as the ban on broadcast of RT France provide an extremely dangerous precedent also in Europe, where many Members States face rising authoritarianism and disregard for the rule of law, and where such decisions can be taken about the media - and community-led projects, such as Wikipedia - that provide verified information and enable public debate.

We need to ask ourselves a question to what extent these general preventive measures deprive us of the possibility of a healthy public debate? To what extent do they simply sanitise the internet from what is difficult and complex, from what stems from systemic injustices and European imperialism, both historically and now?

Recently adopted legislation attempts to provide safeguards amidst the generalised and standardised approach to speech policing, also through the guidelines on complaints mechanisms and obligations to include fundamental rights in T&Cs. Racialized and queer communities, immigrants and refugees and other groups experiencing systemic oppression face barriers of access that won't be alleviated via this law-making. There is a danger that being content enough by these safeguards we are mirroring a rather shocking opinion by Voltaire who wrote: "We have never claimed to enlighten shoemakers and servant girls."

Finally, the secrecy of algorithms and algorithmic amplification create a bubble of reinforcement of disinformation and divisive content. These are the features of the surveillance-based business model that, along with the right to privacy, chips away at our freedom to express ourselves. None of the legal acts described above, and none beyond - including the Digital Markets Act - tackle this cause of today's issues with freedom of expression. Since the EU legislation does not attempt to break the status quo, we need to thoroughly consider if bringing human rights into business-to-client relationships does not inadvertently legitimise the existence of surveillance capitalism, as good a development as binding corporations to mind human rights it may be.

"We need to ask ourselves (...) to what extent these general preventive measures deprive us of the possibility of a healthy public debate? To what extent do they simply sanitise the internet from what is difficult and complex."

Article 18: Digital rights and the protection of the right to asylum in the Charter of the European Union

Romain Lanneau, *Statewatch*

The right to asylum, as delineated in Article 18 of the Charter of Fundamental Rights of the European Union (EU) ('the Charter'), does not grant the right to asylum to every individual seeking it. Instead, it articulates that everyone is entitled to have their application for international protection examined in line with international and EU law.[1] This principle is reinforced by Article 19 of the Charter, which strictly prohibits collective expulsions and forbids the removal, expulsion or extradition of any person 'to a State where there is a serious risk that he or she would be subjected to the death penalty, torture or other inhuman or degrading treatment or punishment'.[2]

Over the past two decades, asylum proceedings in the EU have been increasingly infused with digital technologies. The majority of these developments were initiated with the aim of controlling, monitoring and policing asylum seekers, and preventing their arrival in the EU . However, some civil society initiatives have also, endeavoured to leverage digital technologies as a means of assisting individuals with their applications[3] or safeguarding people from pushbacks.[4]

Despite their potential implications, digital rights within the context of asylum proceedings are frequently overlooked by legal practitioners, asylum seekers and civil society actors. These rights are seldom given priority, especially when facing potential detention or deportation. But authorities have remained resolute in their drive to increase the deployment and use of digital technologies, data and artificial intelligence (AI), with the dual objective of mitigating the entry of asylum seeker into EU territory and evaluating the claims of those who do submit an application. The right to asylum is now inextricably linked to digital technologies. This article seeks to explore the intricate relationship between these two concepts and to examine how digital rights can be leveraged to protect the rights of asylum seekers.

"...digital rights within the context of asylum proceedings are frequently overlooked by legal practitioners, asylum seekers and civil society actors."

"The right to asylum is now inextricably linked to digital technologies."

The right to privacy: Safeguarding asylum seekers against invasive technology and 'junk science'

The right to privacy, enshrined in Article 7 of the Charter, is designed to guard against unwarranted, unnecessary and disproportionate invasions into people's private lives.[5] However, it can be curtailed by public authorities in accordance with the principle of proportionality as articulated in Article 52.[6] For instance, within the EU, all passport applicants are obligated to provide their fingerprints to authorities for more accurate identification,[7] notwithstanding that it 'is not decisive' that this method is 'not wholly reliable'.[8]

Within the context of asylum claims, where authorities often endeavour to amass as much information as possible about each applicant, the protection of privacy is paramount. This is particularly relevant given the access to huge volumes of digital data that is now available on individuals. The EU's highest court has acknowledged the prevention of illegal entry into the EU as a matter an objective of general interest.[9] This stance necessitates asylum seekers to compromise their privacy for a chance to secure protection. The question then arises of how much authorities should be able to probe into an applicant's private life.

One of the primary objectives of authorities when evaluating asylum claims is to verify the identity of the individuals and the veracity of their claim. While some identity features – such as fingerprints – are straightforward for authorities to collect, others are more challenging to obtain. Age and sexual identity are two such examples. It is often impossible to validate an asylum seeker's claim of being a minor or identifying as homosexual through documentation. Yet, these factors can significantly influence the final decision, as well as the conduct of interviews and the individual's accommodation.

Public authorities have long sought a definitive test that would separate the wheat from the chaff. Before the Court of Justice of the European Union (CJEU) imposed limitations on national practices in 2014, asylum seekers were forced to deal with the most private and sordid questioning during attempts to validate their story. For example, Dutch authorities often suggested that applicants bring their own porn video to their asylum hearings as evidence of their claimed sexual orientation. Though officially a choice, Advocate General Sharpston entertained 'serious doubts [that the] vulnerable party in the procedure of applying for refugee status, could really be deemed to have given fully free

and informed consent to the competent national authorities in such circumstances',[10] particularly given the power dynamics at play. The CJEU eventually abolished this practice in the ABC ruling, citing infringements on human dignity (Article 1 of the Charter) and the right to private life (Article 7).[11]

National asylum authorities have resorted to 'junk science' in their search for a truth serum to identify individuals deserving protection.[12] The 2018 case F v Hungary, which examined the use of 'projective personality tests' to determine an individual's sexuality, was particularly contentious. The CJEU declared that such a test 'may be accepted only if it is based on sufficiently reliable methods and principles in the light of the standards recognised by the international scientific community'.[13] In assessing an individual's sexuality, projective personality tests fall dramatically short of meeting these standards. The Court also highlighted in its ruling that 'consent is not necessarily given freely, being de facto imposed under the pressure of the circumstances in which applicants for international protection find themselves'.[14]

More recently, national courts have encountered instances where asylum authorities have requested applicants' phones[15] to extract and examine stored data for evidence supporting the individual's claims. In Germany, a court ruled this practice illegal unless less intrusive alternatives had been considered. The judges made clear that the use of new technologies must be both necessary and suited to the intended purpose.[16]

Looking forward, it is plausible that authorities might resort to AI to ascertain an individual's identity.[17] However, assertions that machine vision technologies can determine an individual's sexuality are more reminiscent of pseudoscience than offering any credible reassurance. The EU's AI Act, currently under negotiation, fails to adequately address and prevent potential harms arising from the use of AI in the context of migration.[18] As a result, legal challenges rooted in the right to privacy will remain crucial in defining the boundaries of acceptable digital practices within asylum procedures.

The right to individual data protection: A prerequisite for an effective remedy against automated and semi-automated decision-making

The EU has established a mille-feuille of databases[19] designed to identify all individuals who either seek to or do enter the EU. These information systems are intended to support migration and police authorities in their decision-making concerning individuals, such as their right to entry or stay pending an asylum decision.[20] Article 8(2) of the Charter confers upon any individuals whose data has been collected by a European authority the right to individual data protection. This includes the right to access data stored about them and to rectify or delete any incorrect data.[21]

Asylum seekers are progressively forced to surrender increasing amounts of personal information. The latest Eurodac system will collect the facial images and personal information of asylum seekers (and other foreign nationals) aged as young as six.[22] National authorities massively collect and exchange individuals' personal data, who largely remain unaware of it until the data is used as the basis for a decision on their case.

While the surge in new and expanded databases is purported to assist in decision-making, they cannot serve as the sole source of information for a decision. In the 2006 case Spain v Commission, the CJEU ruled that authorities should not make automated decisions based solely on information stored in a European information system. Decisions must rest on an individual assessment of the person's situation, including an evaluation of the legal grounds for denying entry.[23]

Nevertheless, the practice of denying entry and deporting individuals perceived a risk to national security persists, with states often not providing access to the reasons for those decisions. In 2020, the CJEU clarified that an individual has the right to obtain minimum reasons for their refusal of entry into the Union. Article 47 of the Charter,[24] espousing the principle of equality of arms requires national authorities to disclose the state that shared information used as the basis for the decision, as well as the specific grounds for the risk assessment.[25] This disclosure allows applicants to seek effective remedy against the decision. Similarly, under Article 8(2) of the Charter, the right of access serves as a 'gatekeeper enabling data subjects to take further action'[26] such as requesting removal or rectification of wrongful accusations that impact their right to a fair trial.

Despite these provisions, access to information is far from being uniformly respected by member states. All too often, asylum seekers find that 'secret' evidence is being used against them. In some instances, the country from which a person is seeking asylum is the one that supplies the data on which the authorities base their decision.[27] Even though data sharing with a third country should adhere to EU protection standards,[28] including the prohibition of usinginformation obtained from torture, this is not adequately monitored in practice.[29]

The risk of national authorities relying on inaccurate or illicit data has been amplified with the implementation of the latest information systems regulation[30] and the Europol Regulation.[31] Nonetheless, data protection standards for asylum seekers fall short of those provided to EU citizens. This was exemplified by the recent 'Processing of Personal Data for Risk Analysis' (PeDRA) scandal, in which Frontex proposed the collection of intrusive personal data, fragrantly violating data protection rights.[32] At the same time, the European Data Protection Supervisor (EDPS) contended that the rules governing the agency are vague regarding the 'conditions or limits for sharing data with other agencies, states and third countries, and on available remedies for individuals'.[33]

As the EDPS pointed out, 'Privacy and data protection are part of the human rights too often suspended at the borders of the European Union'.[34] This sentiment underscores a recurring theme in asylum, migration and border regulation, illustrating the tendency to view certain migrant groups as security concerns and undeserving of the protections afforded to citizens or other categories of foreign nationals.[35]

Digital asylum rights: A call for increased safeguards amidst the digitalisation of procedures

Public technologies are often employed by authorities with the expectation of enhancing efficiency and mitigating or eliminating biases that emerge from human decision-making. However, studies on the impacts of these technologies frequently show the exact opposite.[36] Issues of discrimination and racism persist, yet they become entwined within the complexity of technical systems. This makes it increasingly challenging to substantiate when and how rights violations occur.

The EU's current legislative negotiations set to further expand the use of digital technologies in asylum and migration procedures. Nevertheless, these negotiations also present opportunities for enhanced safeguarding. The proposed Screening Regulation potentially offers an avenue for bolstering the protection of asylum seekers' right to privacy. This can be achieved through the inclusion of an independent mechanism designed to monitor the protection of individuals' fundamental rights during their identification by border authorities. However, this regulation is yet to be approved, and it will ultimately fall under the jurisdiction of the Fundamental Rights Agency and Member States in their jurisdiction, to clarify the procedure of this new mechanism.[37]

The digitalisation of asylum and immigration proceedings is poised to become ever more deeply entrenched in the years to come. It is therefore of paramount importance to amplify understandings of privacy, data protection and other digital rights among asylum seekers, migrants and migration activists, legal professionals and non-governmental organisations.

Article 20 : Digital inequalities and the promise of equality before the law

Jens Theilen, *Helmut-Schmidt-University Hamburg*

Digital and historical inequalities

In his book Black Skin, White Masks, anti-colonial philosopher and revolutionary Frantz Fanon describes what he calls the 'white gaze' and its effects: 'not only must the black man be black; he must be black in relation to the white man. [...] The image of one's body is solely negating. It's an image in the third person'.[1] Over half a century later, Fanon's account echoes eerily in the experiences of Joy Buolamwini, a Black researcher at the MIT Media Lab. Working on a project that involved projecting digital masks onto her reflection, she realised that the facial recognition technology she was using could not sufficiently detect the contours of her face – unless she donned a white mask. Fanon's juxtaposition of Black skin and white masks in the title of his book thus took on an unexpectedly literal meaning. Buolamwini called this phenomenon the 'coded gaze': a form of algorithmic bias with discriminatory effects, for example when facial recognition software is applied by law enforcement and misidentification leads to increased surveillance and arrests.[2] In a subsequent publication with Timnit Gebru, Buolamwini analysed three commercial gender classifiers and found that 'male subjects were more accurately classified than female subjects', 'lighter subjects were more accurately classified than darker individuals', and 'all classifiers performed worst on darker female subjects'.[3]

"...inequalities (...) are rooted in historical practices of surveillance and data processing used as tools of slavery, colonialism, patriarchy, and other forms of domination."

The continuities between Fanon's notion of the 'white gaze' and Buolamwini's reworking of it as the 'coded gaze' make it abundantly clear that oppressive structures like racism and (cis)sexism remain central in digital contexts. The internet has not created a utopian space free of inequalities, and placing our hopes in technology as an easy fix to societal problems remains a misplaced strategy. Conversely, however, it is unhelpful to think of digital inequalities as entirely new problems that emerged only because of technological advances; rather, they are rooted in historical practices of surveillance and data processing that have long since been used as tools of slavery, colonialism, patriarchy, and other forms of domination. As surveillance scholar Simone Browne has put it: 'Surveillance is nothing new to black folks. It is the fact of antiblackness'. She therefore cautions against seeing surveillance as 'something inaugurated by new technologies, such as automated facial recognition or unmanned autonomous vehicles (or drones)', instead arguing that it is continuous, ongoing, and sustained by racism, antiblackness, and other oppressive practices, performances and policies.[4] Digital inequalities are a continuation of historical inequalities.

The promise of equality

Against inequalities of all kinds, the law holds up the promise of equality. Article 20 of the Charter of Fundamental Rights of the European Union (EU) ('the Charter') contains a succinct formulation of this promise: 'Everyone is equal before the law'. This very general phrasing takes more concrete form in the non-discrimination clause that follows it in Article 21 (as well as various acts of secondary legislation), which prohibits any discrimination based on a lengthy list of grounds including but not limited to sex, race, religion, disability, age or sexual orientation. The need for lists like this makes it clear that while equality and non-discrimination may nowadays be widely accepted as abstract ideals, their promise remains very much unfulfilled in practice. A dishearteningly large number of examples confirms that this holds true for digital contexts and the use of new technologies: predictive policing that disproportionately targets people of colour and poor people; hate speech on social media platforms geared at queer people, women, and particularly trans women and women of colour; discrimination of women on the job market based on algorithmic decisions; racist and sexist stereotypes reflected in the results of online search engines; and many other examples besides.[5]

The disconnect between ideal and reality means that there is potential for change: we can use the promise of equality to challenge inequalities, including their manifestations in digital contexts. The equality and non-discrimination clauses of EU law hold significant untapped potential in that regard, especially since they arguably apply to private actors as well as public bodies. Traditionally, fundamental rights and human rights are directed against the state, but do not – at least not directly – constrain the actions of private actors.[6] In our current juncture of surveillance capitalism,[7] however, the power to generate and sustain digital inequalities lies not only with the state, but also with private actors like multinational corporations: the companies that offer and use generic facial recognition software, that run social media platforms and search engines and

decide who gets banned for hate speech and who doesn't, which algorithms get used to generate search results, and so on. EU law differs from international human rights law by holding private actors like these to the promise of equality, at least in some cases.[8]

Is 'everyone' equal before the law?

The law is no panacea, however, and the promise of equality may end up indefinitely deferred for some. One common line of criticism against non-discrimination law is that it tends to see grounds of discrimination like gender and race as distinct, homogenous categories.[9] In contrast to this, using intersectionality as a framework of reference illustrates the ways in which oppressive systems such as racism and (cis-)sexism intersect and impact upon different people in different ways.[10] For example, as mentioned above, Buolamwini and Gebru's analysis of commercial gender classifiers not only found decreasing accuracy along the lines of race and gender, but also the worst performance when these lines intersected in the case of women of colour. Algorithms may also pick up on cultural representations and stereotypes that pertain specifically to Black women or other women of colour, as when Google's top hits for 'Black girls' were filled with pornographic results before changes were made after sustained public pressure.[11]

Despite an increasing awareness of the importance of intersectional analysis, a recent report by the Center for Intersectional Justice found that 'European legal bodies are currently underequipped to address cases of intersectional discrimination'.[12] Drastic improvements on this front would be needed to combat inequalities in a way that does not side-line those who are most impacted by them: as Aisha Kadiri put it, 'taking into account the unique type of bias data subjects face, requires the recognition of intersectionality from the get-go'.[13] While legal doctrine sees it as subsidiary to more specific non-discrimination clauses, **the promise of equality for 'everyone' in Article 20 of the Charter should serve as a reminder that discrimination cannot be siloed into separate grounds of discrimination but must be considered holistically.**

There are no easy fixes

Taking an intersectionally informed approach to combatting digital inequalities also means asking who profits and who loses out when new technologies are deployed. For example, a few years ago the main public transport company of Berlin used automated gender classification at some of its ticket machines to grant a discount to women on International Women's Day. What seems at first to be a benign project to counteract the pay gap in a small way turns out, however, to be advantageous only for some women at the expense of others. Not only do studies like that of Buolamwini and Gebru imply that women of colour would face greater likelihoods of losing out on the discount, the very notion of attributing binary gender to people based on the physical appearance of their face is fundamentally trans-exclusionary. Automated gender classification contributes to normalising the idea that gender is readable from physical appearance and thus stands opposed to a self-determined gender identity – which is why many trans persons resist the technology as such, rather than focussing on reform to make it more inclusive.[14] The example shows that **new technologies are not only implicated in creating inequalities between groups but also, by virtue of the way they categorise people and normalise certain ways of thinking, in the very processes of gendering and racializing.**[15]

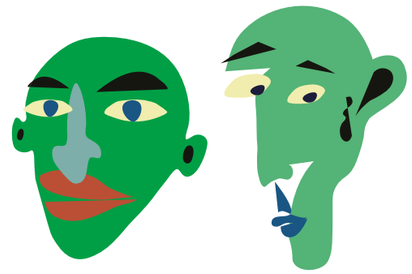
Understanding just how deep the problems go is important because it points to a recurring issue with regard to digital equalities: often, there is no easy fix since these inequalities are intricately tied up with the technology at issue. This is not only the case with trans-exclusionary understandings of gender, but it also relates to many forms of technology once viewed in the broader context of their development, use, and institutionalisation. Historians of technology have demonstrated that, time and time again, new technologies have not only served the interests of those in power but have been purposefully developed and used to support efforts of domination, policing, and surveillance. Whether through schemas of gender and race classification or other methods, inequalities are built into the very foundations of the digital infrastructures that now seem so familiar to us: 'sexism is a feature, not a bug',[16] and 'anti-Black racism, whether in search results or in surveillance systems, is not only a symptom or outcome, but a precondition for the fabrication of such technologies'.[17] Bugs, symptoms and outcomes might be amendable to easy fixes, but the problems go deeper.

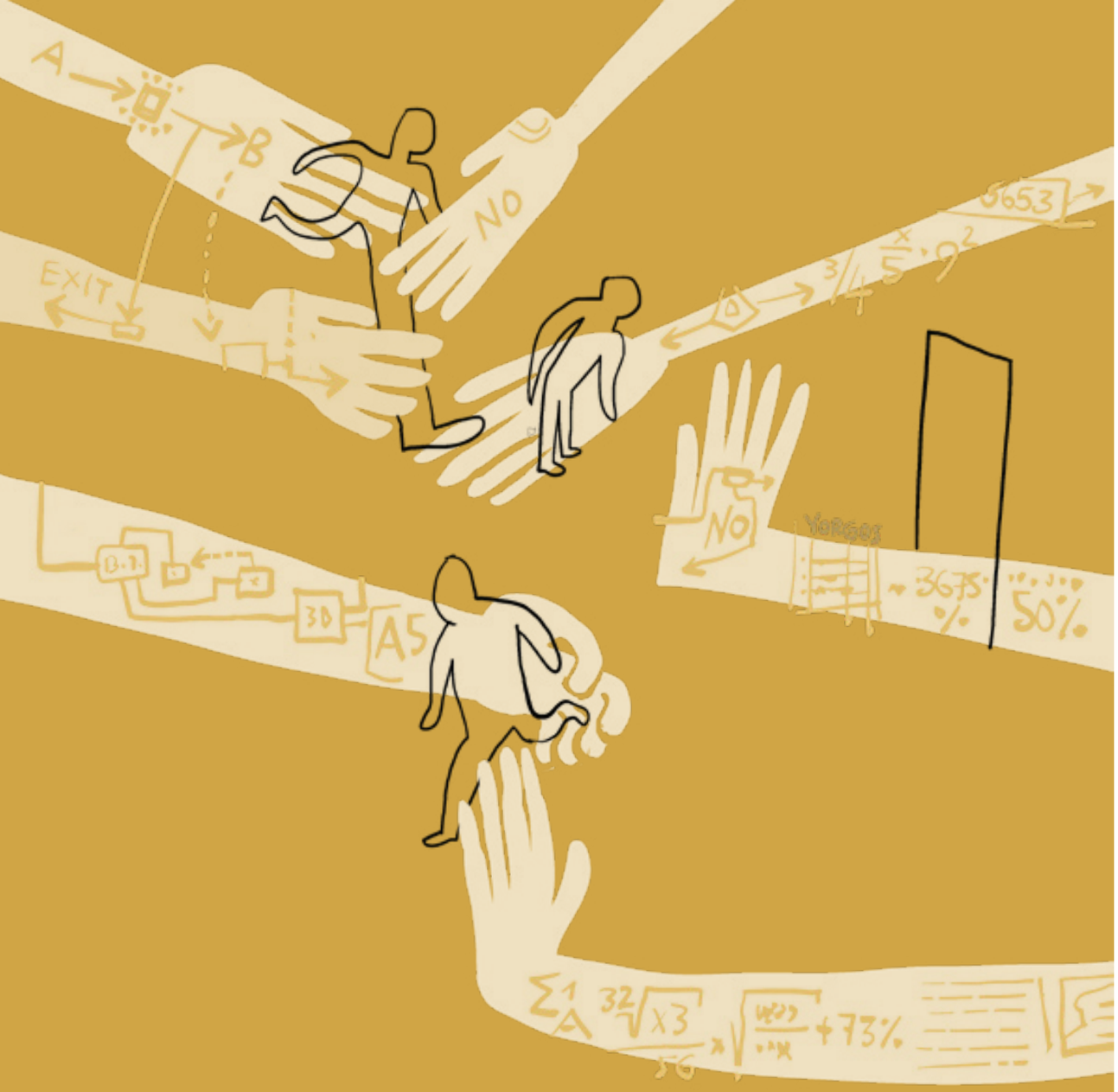
The limitations of equality claims

The language of equality and non-discrimination runs the risk of merely claiming inclusion and accuracy in outcomes, while ignoring the central relevance of oppressive structures like racism and (cis-)sexism for the very existence of digital technologies, as well as the political, institutional, and economic contexts of their use. To come back to the example of facial recognition, it quickly becomes clear that besides the commercial purpose of its use, these technological systems primarily appeal to law enforcement agencies like the police and border control (although these are often reliant, in turn, on private technology and consultancy big tech companies). These institutions are saturated in racism and antiblackness; the policing of Europe's borders, in particular, is built on violent colonial logics that consider Black lives expendable.[18] It is difficult to capture problems like this in the legal language of equality and non-discrimination – as legal scholar and trans activist Dean Spade puts it, structural issues like wealth disparities, targeting in criminal punishment, environmental harm, immigration enforcement and others are 'cast as neutral by the discrimination principle'.[19] Claims to equality before the law may thus end up legitimising deeply unjust institutions even as cosmetic changes are made on the level of symptoms or outcomes. More accurate facial recognition would indeed, on the face of it, be more equal along the lines of gender and race; but, seen in the context of its use by law enforcement, the promise of equality loses its allure.

Let's come back to Frantz Fanon's notion of the 'white gaze' and Joy Buolamwini's reworking of it as the 'coded gaze'. Vision, in these and other references to the 'gaze', is tied up with power – there is, as Black feminist bell hooks says, 'power in looking'. She develops the notion of the 'oppositional gaze' to also capture the power in defiantly and courageously looking back: 'Not only will I stare. I want my look to change reality'.[20] How can we change reality by means of equality claims? As I argued above, we can use the promise of equality to challenge inequalities, including their manifestations in digital contexts. We need to be aware of its limitations, however. At its best, equality would mean reciprocity, a mutual regard based on even footing, Blackness no longer constituted in relation to whiteness. But claims to equality before the law typically fail to achieve this kind of reciprocity. It is difficult to use them to force a reconsideration of whose gaze it is that has the power to constitute racialised and gendered subjects in the first place, and whose interests are coded into our digital infrastructures and new technologies. In many cases, we should resist the pull of accuracy and inclusion that equality so easily slips into, and concentrate on opposition and refusal. As a collective of authors put it in the Feminist Data Manifest-No: 'We refuse to cede that convincing unjust institutions and disciplines to listen to us is the only way to make change. We commit to co-constructing our language and questions together with the communities we serve in order to build power with our own'.[21] The promise of equality before the law should not exhaust the horizon of our collective imaginations and actions.

"The promise of equality before the law should not exhaust the horizon of our collective imaginations and actions."





Article 21 : An exploration, or the right to algorithmic non-discrimination

Raphaële Xenidis, *SciencesPo Law School*

Introduction

Article 21 of the Charter of Fundamental Rights of the European Union (EU) (hereinafter 'the Charter') safeguards the fundamental right to non-discrimination. It encompasses two paragraphs: Article 21(1), an open-ended non-discrimination clause modelled on Article 14 of the European Convention on Human Rights (ECHR), prohibits '[a]ny discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation'; and Article 21(2) prohibits 'any discrimination on grounds of nationality' '[w]ithin the scope of application of the Treaties, and without prejudice to any of their special provisions'.

A rich body of research has shed light on the ubiquity of bias and inequality in algorithmic systems.[1] In this context, the protections and assurances provided by the fundamental right to non-discrimination are of paramount importance. This essay explores how the right to non-discrimination enshrined in Article 21 could be interpreted and applied within a digital context. Section 1 first explores the relevance of the fundamental right to non-discrimination within an algorithmic society and introduces the real-world example of racial bias in proctoring software used by some universities during the Covid-19 pandemic. Subsequently, Section 2 highlights interpretive queries emerging from the 'transposition' of the right to non-discrimination into an algorithmic context. Finally, Section 3 elucidates how Article 21 could serve as an instrument to prevent and redress algorithmic discrimination.

The relevance of the fundamental right to non-discrimination in an algorithmic society

Due to the scope of the Charter, as expressed in Article 51(1), the prohibition of discrimination applies to 'the institutions [and] bodies […] of the Union' as well as 'the Member States only when they are implementing Union law'. Hence, the EU has a comprehensive obligation to refrain from any form of discrimination based on all grounds listed in Article 21. For instance, this implies that Frontex, an EU agency, cannot utilise border control software that discriminates against individuals based on factors like skin colour, ethnic origin or language.

The obligation for member states, however, is more limited: the non-discrimination clause contained in Article 21 only applies when there is a 'direct link' with EU law.[2] Within the material scope of the EU's four anti-discrimination directives (Directives 2000/43/EC, 2000/78/EC, 2004/113/EC and 2006/54/EC), EU secondary law provisions prohibit discrimination on grounds of sex or gender, race or ethnic origin, sexual orientation, disability, religion or belief and age.[3] Article 21 of the Charter, embodying the general principle of equal treatment, applies within the specific framework defined by these Directives.[4] Yet, where the Directives cannot, in principle, apply directly to private parties, the Court of Justice of the European Union (CJEU) has recognised horizontal direct effects to Article 21(1) of the Charter.[5] To illustrate this, Article 21 bars private employers within the EU from deploying algorithmic recruitment tools that unduly put women or candidates with disabilities at a disadvantage.

In scenarios where the situation falls outside the scope of EU secondary law but maintains a direct link with EU law,[6] Article 21 operates in a subsidiary manner.[7] For instance, Article 21 precludes a member state from implementing a discriminatory algorithmic system for purposes such as the processing of personal data, which is regulated by the EU General Data Protection Regulation.[8]

Let us consider a concrete example. In 2022, a Dutch student named Robin Pocornie, supported by the Racism and Technology Centre, filed a discrimination claim with the Dutch equality body and national human rights institution, the College voor de Rechten van de Mens (the Institute for Human Rights). Pocornie argued that the Vrije Universiteit Amsterdam's use of proctoring software to prevent cheating during exams taken at home during the Covid-19 pandemic in 2020 discriminated against her on grounds of race. The application repeatedly failed to recognise her face, which made her participation in exams difficult and imposed undue stress. Based on the evidence she collected, this issue was not experienced by students who were not racialised. Her claim echoes academic research showing that commercial facial recognition systems perform significantly worse when attempting to identify the faces of individuals (and particularly women) with darker skin tones.[9] When these systems are used to control access to resources, services, institutions or benefits, their subpar performance for certain demographic groups generates unjust disadvantages.

Applying Article 21 to algorithmic bias

This section explores the legal interpretation of Article 21 in relation to algorithmic bias. In the case of the biased proctoring application, the system was utilised to invigilate exams, which are integral to educational courses and grant access to future opportunities. From the perspective of EU law,[10] this case falls within the scope of the Race Equality Directive 2000/43/EC, which extends to the field of education.[11] The general principle of equal treatment inscribed in Article 21 also applies to this case because the Directive establishes the link by which member states are regarded as implementing EU law. As per the decision of the CJEU in Egenberger, the prohibition of discrimination is directly effective against both public and private entities.[12] Article 21 of the Charter therefore bestows the applicant with a directly enforceable right to algorithmic equal treatment against the Vrije Universiteit Amsterdam.

Nevertheless, transferring the fundamental right to non-discrimination to the context of algorithmic bias poses some challenges in the legal qualification of such bias. For instance, in its interim judgment on 7 December 2022, the Netherlands Institute for Human Rights highlighted the difficulties faced by Pocornie in presenting evidence that the proctoring tool worked differently for students with different skin colours.[13] The Institute pointed out that because 'logs were not provided to exam takers', '[t]he applicant […] had no insight into any notifications that the software logged in her case and therefore could not link them to any particular event or action (or lack thereof) on her part'. This emphasises the challenge faced by victims of algorithmic bias in raising a reasonable suspicion of discrimination. The lack of access to comprehensible information about how the system operates and the 'atomisation' of individual experiences in the online environment obstruct traditional comparative heuristics that underpin the enforcement of non-discrimination law. However, the Netherlands Institute for Human Rights analysed the applicant's experience with the proctoring software in the context of existing research on bias in facial recognition software to establish a presumption of discrimination. This presumption shifted the burden of proof onto the defendant, in this case, the university (and the software provider).[14]

The Netherlands Institute for Human Rights classified the case as one of indirect discrimination, deeming it 'plausible that the face detection algorithms […] will, in practice, particularly affect persons of darker skin colour'. Under EU secondary law, a finding of indirect discrimination triggers an open-ended proportionality test, where a prima facie discriminatory practice can be justified if it serves a legitimate aim through appropriate and necessary means. However, from the perspective of Article 21 of the Charter, proportionality must be evaluated through the criteria outlined in Article 52(1). This provision stipulates that '[a]ny limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms', and that 'limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others'. This results in a second issue related to transposing the parameters of the proportionality test to the operation of an algorithmic system. In the proctoring case, the defendant contended that 'the distinction made is […] justified by the legitimate interest to prevent fraud in examinations against the background of the [COVID-19] pandemic' and that '[t]he use of proctoring software was both appropriate and necessary in this regard'. A defendant might argue that ensuring fairness in examinations and upholding merit in education is an objective of general interest, and that given the circumstances, the use of proctoring software was both appropriate and necessary. Furthermore, a defendant could claim that proportionality stricto sensu is maintained because flagging might not meet the threshold for qualifying as discriminatory harm, particularly if it does not result in any subsequent disadvantage. Conversely, the Netherlands Institute for Human Rights, referencing the case law of the European Court of Human Rights, asserted that flagging in and of itself constituted a discriminatory harm and that 'the alleged lack of materially adverse consequences due to the fact that the examination time was extended [wa]s irrelevant'.[15]

Harnessing the strengths of Article 21 to address algorithmic discrimination

While Section 2 illuminated some of the issues encountered in addressing algorithmic bias through the lens of the fundamental right to non-discrimination, Article 21 of the Charter also contains a number of interesting features that can be harnessed to interpret the provision purposively within the context of algorithmic systems.

First, Article 21(1) provides an open-ended list of protected characteristics that could be leveraged in the context of systemic algorithmic differentiation.[16] For instance, 'social origin' and 'property' are explicitly mentioned in Article 21 as protected grounds, which could serve as bases to confront algorithmic discrimination predicated on income or socio-economic profiling. Nonetheless, this pertains exclusively to situations where member states are implementing EU law, but that fall outside the material scope of the non-discrimination directives. Indeed, in the case of FOA, the CJEU affirmed that 'the scope of [EU anti-discrimination directives] should not be extended by analogy beyond the discrimination based on the grounds listed exhaustively'.[17]

The open-ended nature of the non-discrimination clause in Article 21 of the Charter could also facilitate the redress of intricate patterns of algorithmic discrimination,[18] a phenomenon that research has shown to be widespread.[19] However, the reluctance shown by the CJEU in Parris to tackle intersectional discrimination, if mirrored in interpreting Article 21, could curtail the effectiveness of the Charter in addressing algorithmic discrimination.[20]

Second, in principle, the application of Article 21 does not necessitate the conventional distinction between direct and indirect discrimination.[21] For situations that exhibit a direct link with EU law but fall outside the scope of EU secondary anti-discrimination law, a unified justification regime follows from Article 52(1). Given the difficulty of qualifying algorithmic bias as either direct or indirect discrimination,[22] and the likely obstacles in substantiating cases of direct algorithmic discrimination, the unified justification framework attached to Article 21 of the Charter could present an interesting pathway for redress. However, in practice, the CJEU is prone to integrating the bifurcated analytical framework foreseen by the EU's anti-discrimination Directives in relation to justifications into the interpretation of the prohibition of discrimination as defined by the Charter.[23]

Restrictions to the fundamental right to equal treatment under Article 21 can only be condoned if they are 'provided for by law and respect the essence of [the] rights and freedoms', as guaranteed by the Charter. This inherently curtails the latitude of private companies, as any discriminatory system must align with a legal mandate and honour the 'essence' of the right to non-discrimination. Moreover, the Charter's embedded proportionality test dictates two conditions: limitations must be 'necessary' and 'genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others'. Considering the case of the algorithmic proctoring tool, one could argue that the system's infringement on students' rights to non-discrimination was not mandated by law, did not respect the essence of the fundamental right safeguarded by Article 21, did not genuinely align with the objectives of general interest recognised by the EU, and was not necessary to protect the rights and freedoms of others.[24] The regime established in Article 52(1) therefore considerably restricts the set of justifications permissible even before any analysis of proportionality stricto sensu is conducted. This unique aspect of the right to non-discrimination, as enshrined in Article 21 of the Charter, could thus help to pre-empt and circumvent some of the challenges related to reviewing the proportionality stricto sensu of decisions made in the context of trade-offs between fairness and accuracy in algorithmic systems.[25]

Conclusions

To echo the title of this essay series, the awareness that Charter rights are digital rights and vice versa is of paramount importance within the context of an algorithmic society. Indeed, fundamental rights protected by the Charter, such as non-discrimination, should operate seamlessly across the boundary between the physical and digital realms. A teleological interpretation of these rights is essential to ensure that socio-technical transformations, such as the pervasive deployment of algorithmic risk assessment and decision-making systems, do not compromise the normative balance embedded in legal frameworks. Therefore, to ensure the effective protection of fundamental rights, it is necessary to re-evaluate existing regulations in light of how technological advancements alter power dynamics and redistribute societal costs and benefits.

"…fundamental rights protected by the Charter, such as non-discrimination, should operate seamlessly across the boundary between the physical and digital realms. "

Acknowledgments

The research conducted in this article is linked to a project that has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 898937.

Article 7: The right to privacy as a gatekeeper to human rights

Nadia Benaissa, *Bits of freedom*

Space to be and to become: Privacy as the foundation for growth

As stipulated in Article 20 of the Charter of Fundamental Rights of the European Union (EU) ('the Charter'), all individuals are equal and stand equal before the law. Yet, equality does not entail homogeneity. We perceive, communicate, and love in countless ways. We carry within us unique family histories, navigate varying power structures, and bear the historical and social significance of our race and gender from the day we are born. And we constantly brace ourselves for political interpretations of how we express ourselves, what we stand for, and what we believe in.

We are all equal, but not identical.

Therefore, we require space. Space to explore, to falter, to make up our minds and change them again, to persist and to persevere. Space to understand who we were, who we are, and who we aspire to be. Space to get to know our inner selves, without the interference, patronisation or belittlement of others. And space to live our truth, even if that truth is not popular, loved or even understood.

This space is the lifeblood for our personal development and for a free and open society. It is granted, in part, by the right to privacy, as stipulated in the Charter: 'Everyone has the right to respect for his or her private and family life, home and communications'. The right to privacy is inextricably linked to other human rights. For instance, the processing of data pertaining to gender, religion or ethnicity could infringe upon an individual's rights to equal treatment or freedom of religious expression. Consequently, the right to privacy acts as a gatekeeper for other human rights. This essay delves into several recent cases in the Netherlands where infringement on the right to privacy has precipitated violations of other human rights.

Identities reduced to stereotypes: Data processing and the dangers of stereotypical reductionism

With the advent of seemingly limitless technological capabilities in data processing, the right to privacy is under considerable strain. Data containing personal information is being processed, analysed and interpreted on an unprecedented scale. Insights and conclusions drawn from such data are disseminated and exchanged. The multifaceted aspects that construct identities are simplified, categorised and packaged into predetermined profiles, a process that reduces complex identities to mere stereotypes.

Indeed, profiling might simplify the prediction of an individual's receptiveness to advertising strategies or the success of medical treatments. But how appropriate is it to estimate, based on profiling, the political persuasions of a swing voter, the likelihood of someone's involvement in 'suspicious transactions', or who might commit benefit fraud?

Automated decision-making based on profiling was heralded with the promise of simplicity, efficiency and efficacy. Unfortunately, the opposite appears to be true, and the consequences becoming increasingly apparent, as we observe various fundamental rights being undermined due to breaches of the right to privacy.

Compounded discrimination: The cumulative impact of bias

A striking example of the infringement of privacy leading to other human rights violations can be found in the realm of digital welfare. The Dutch digital welfare system gave rise to the now notorious childcare benefits scandal.[1] In 2018, it came to light that many parents who received childcare benefits from the Dutch Tax Administration had been wrongly identified as committing fraud. This incorrect classification forced parents to repay thousands of euros to the state, plunging many into severe financial distress, homelessness, and acute stress and poverty. In an alarming revelation, as many as 2090 children of affected parents were taken into care between 2015 and 2022.[2]

Of the affected parents, a disproportionate number were found to be from immigrant backgrounds. This was corroborated by subsequent investigations, which revealed that the Tax Administration was processing data related to parents' nationalities. The Dutch

Data Protection Authority[3] confirmed this claim and identified three illicit processing operations. First, dual nationalities were being processed. Second, nationality data was employed as an indicator for the risk classification model. Third, this model was being utilised to detect organised fraud. It was concluded that there had been discrimination based on nationality. Amnesty International's[4] further investigation discovered that discrimination was perpetrated not only on the grounds of nationality but also ethnicity. Indeed, the use of nationality data facilitated the discriminatory targeting of ethnic minorities by the risk classification model. As Amnesty highlighted in its report, 'ethnic profiling violates the prohibition of discrimination. It leads to the criminalisation of certain groups of people and it reinforces historical stereotypical associations between fraud and ethnicity'.

Additionally, the investigation revealed that people who received higher benefits were more likely to be labelled as committing fraud. This led to individuals from low-income households being disproportionately affected owing to their greater dependence on benefits and the larger sums they received. Moreover, lower-income parents found it more difficult to repay the vast sums demanded by the Dutch government. Amnesty's assessment classified the situation as intersectional discrimination[5], as those most affected were typically ethnic minority groups who are generally more likely to have low incomes. Compounding the issue, it later emerged that religious profiling[6] was also occurring, with individuals who had made donations to mosques being deemed higher risk.

The childcare benefits scandal starkly illustrates the intersectional nature of discrimination, where multiple axes of bias reinforce one another. This is not a new phenomenon. As early as 1989, Crenshaw[7] highlighted how intersecting political and social layers within our identities can render us more vulnerable to discrimination or privilege. Factors such as gender, ethnicity, class, sexual orientation, religion, weight and disability can all affect one's position within the spectrum of power in society. The intersection of multiple factors can either consolidate a position of privilege or expose an individual to compounded discrimination. This phenomenon is exemplified in the childcare benefits scandal. For example, individuals who were Muslim, had a lower income and possessed at least one non-Dutch ethnicity were thrice-penalised based solely on these classifications, with no consideration to their individual circumstances.

Criminalisation prior to transgression: The cost of presumptions

These distinct forms of discrimination arise when data aggregators, such as the Tax Administration Office of the Dutch government in our earlier example, construct profiles based on collected data. While individuals may suspect that their data could be used to make assumptions about them, in this instance, these assumptions were used to predict the likelihood of the individual to commit social security fraud. Moreover, the propensity to suspect individuals even before (or despite the absence of) rule-breaking suggests that the assumed actions of a person's assigned group are paramount in establishing their risk profile. It is critical to note that the Dutch government justified its implementation of algorithmic profiling on the grounds that it would contribute to effective fraud detection and prevention, thereby serving the public interest. This raises the question of whether an argument of public interest should supersede the rights and interests of individual citizens.

In 2020, The Hague District Court[8] contested this notion, ruling that the pursuit of preventing and combating fraud for the sake of economic welfare must be balanced against intrusions on individuals' private lives. The Court evaluated whether the Systeem Risico Indicatie (SyRI) legislation, which permitted the confluence of diverse data to combat fraud, was in breach of Article 8 of the European Convention on Human Rights. The court determined that the SyRI legislation failed to meet the 'fair balance' standard necessary to justify the violation of the right to privacy for the defence of broader interests. Additionally, the Court noted that the use of SyRI offered little safeguard owing to its lack of transparency and verifiability. As the legislation violated European law, it was deemed unlawful and non-binding. Litigation brought forward by civil society organisations, including the Dutch Jurists Committee for Human Rights and the Platform for Civil Rights, sent a clear message: Intrusions into individuals' private lives, particularly through the collection, combination and sharing of personal data, must be judiciously scrutinised by courts and governments.

The right to privacy: The sentinel of human rights

The implications of large-scale data aggregation and processing are substantial. After all, individuals who are classified as high-risk must face the repercussions, whether they know about the classification or not. The childcare benefits scandal exemplifies the human cost of such violations. Moreover, while benefits were abruptly discontinued and demands for repayment piled up, parents were left without answers as to why they had been labelled as committing fraud, and requests for information[9] were met with heavily redacted files. Even legal protection proved insufficient. According to the Judicial Council,[10] families were forced into an unequal struggle against a far more powerful government.

According to the EU Charter of Fundamental Rights, human dignity is inviolable and must be respected and protected (Article 1), and discrimination is prohibited (Article 21). Individuals are entitled to freedom of thought and belief (Article 10), freedom of expression (Article 11), equality before the law (Article 20), the right to protection and care for children (Article 24), the right to social security if self-provision is unfeasible (Article 34) and the right to legal protection (Article 47). People have the right to be presumed innocent until proven guilty. All these rights safeguarded by the Charter were threatened in the childcare benefits scandal, which began with the unlawful processing of personal data. It is not without reason that one of the central objectives of the General Data Protection Regulation is to protect all fundamental rights and freedoms, particularly (though not exclusively) the right to the protection of personal data. The violation of privacy through the processing of personal data can infringe on other fundamental rights. Thus, we refer to the right to privacy as a 'gatekeeper' for other human rights. This emphasises why we must continue to advocate for the right to privacy as a fundamental right – it is crucial to safeguarding an open and free society in which everyone is equal, and whose differences are maintained, respected and valued.

"The violation of privacy through the processing of personal data can infringe on other fundamental rights. Thus, we refer to the right to privacy as a 'gatekeeper' for other human rights."

Article 8 of the Charter of Fundamental Rights of the EU

Ioannis Kouvakas, *Privacy International / Vrije Universiteit Brussels (VUB)*

General remarks

Article 8 of the Charter of Fundamental Rights of the EU (CFREU) expressly embodies a right to the protection of personal data, which is distinct from the right to privacy enshrined in Article 7 of the Charter and has no equivalent in the European Convention on Human Rights (ECHR).[1] It contains a set of obligations and limitations that aim to govern the processing of individuals' personal data, including the requirement that personal data are processed "fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law", while establishing a right of individuals to access and rectify personal data collected about them (Article 8(2)). The Court of Justice of the EU (CJEU) has also interpreted a right to be forgotten into Article 8.[2] Article 8(3) CFREU subjects compliance with data protection rules to the oversight of an independent authority. The EU data protection acquis is further complemented by secondary legislation, including the General Data Protection Regulation (GDPR)[3] and the Law Enforcement Directive (LED).[4]

Focusing on the case law that shaped the interpretation of Article 8 of the Charter, this essay discusses selected issues pertaining to the application of the right and its relationship with Article 7 CFREU in the digital era.

Scope of application

Article 8 applies to the "processing" of "personal data". Both these terms, defined in secondary EU legislation,[5] have been interpreted widely by the CJEU. "Personal data" encompasses all kinds of information relating to an identified or identifiable individual, regardless of whether it is sensitive or private in nature,[6] as well as subjective information such as opinions and assessments.[7] The identity of the person does not need to be already known; what matters is whether the entity responsible for processing them is reasonably able to identify the individual. In Breyer, the CJEU ruled that dynamic IP addresses[8] could constitute personal data even though the additional information necessary to identify the user of a website were not held by the online media services provider collecting the IP addresses. Similarly, "processing" should be understood as any operation performed on personal data, including collection, retention, transfer, erasure etc.[9]

As with every other Charter right, Article 8 binds both EU bodies and member states when they implement EU law (Article 51(1) CFREU). In Tele2, the CJEU examined the validity of national law imposing obligations upon telecommunications service providers to retain certain telecommunications data for law enforcement purposes.[10] Although law enforcement activities were explicitly excluded from the scope of the ePrivacy Directive, which guaranteed the confidentiality of communications,[11] the Court held that the EU law still covered the retention of the data by service providers as well as access to them by authorities, because, inter alia, the ePrivacy Directive imposed obligations to guarantee the confidentiality of communications and provided for possible restrictions, including law enforcement.[12]

The same conclusion was reached in Privacy International,[13] which concerned similar measures, this time for the purpose of safeguarding national security, a field that "remains the sole responsibility of each Member State" (Article 4(2) TEU). Applying its Tele2 reasoning, the Court held that legislative measures regulating the activities of telecommunication services providers fall within the scope of the ePrivacy Directive (and, consequently, EU law) because they entail the processing of personal data by those providers under that very Directive.[14]

Relationship with Article 7 of the Charter

The CJEU does not apply a consistent approach to distinguish between Articles 7 and 8 of the Charter, usually stating that data protection "is closely connected with the right to respect of private life".[15] When examining whether there has been an interference with Articles 7 and 8, the CJEU often focuses its analysis on whether there is an interference with the right to privacy and then states that there is also interference with the right to data protection because the measure at issue involves the processing of personal data.[16]

Likewise, the Court has placed unnecessary emphasis on first establishing an interference with Article 7 before later ruling that Article 8 is also engaged.[17] In Schecke, for example, which dealt with the validity of EU law requiring the publication of details about the beneficiaries of agricultural funds, the Luxembourg Court failed to distinguish between the two rights and treated both Articles 7 and 8 as a single "right to respect for

private life with regard to the processing of personal data".[18] This approach, heavily influenced by the case-law of the European Court of Human Rights (ECtHR), which in order to assert its jurisdiction needs to first establish an interference with the right to respect for private life under Article 8 ECHR, seems to treat data protection as a subset of the right to privacy and could compromise the existence of data protection as an independent Charter right.

Conversely, the wide scope of Article 8 CFREU might provide for a more successful avenue to trigger the applicability of the Charter, or even establish an interference with Article 8 ECHR, before national courts, since the processing of personal data in the digital context will often also constitute an interference with the right to privacy.[19] For instance, in deciding that facial recognition in public amounted to an interference with Article 8 ECHR, the UK Divisional Court also placed emphasis on the terms 'personal data' and 'processing' contained in Article 8 CFREU:

> 58. The [CJEU] has also repeatedly emphasised that the right to protection of personal data is "closely connected with the right to respect for private life", and that "the right to respect for private life with regard to the processing of personal data" is founded on both Articles 7 and 8 of the Charter of Fundamental Rights of the European Union and extends to "any information relating to an identified or identifiable individual".[20]

Limitations

Article 52 of the Charter horizontally sets out a series of conditions that possible limitations on the exercise of Charter rights need to satisfy. Limitations must be provided for by law, respect the essence of the rights and freedoms and be proportionate; they may be made only if they are necessary and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others (Article 52(1)). As Article 8 of the Charter merely provides for a system of checks and balances that the processing of personal data must satisfy, applying Article 52(1) to it means assessing the limitations imposed upon the essential elements of that right. Nevertheless, the CJEU has been more comfortable with applying Article 52(1) of the Charter in the context of Article 7 instead.[21]

Regarding the essence of the right to data protection, the Luxembourg Court will usually hold that this is respected provided that the measure in question contains certain provisions on data protection, in particular on data security. In Digital Rights Ireland, the CJEU found that obligations imposed upon communication services providers requiring the retention of certain communications data did not violate the essence of the rights in Articles 7 and 8 of the Charter.[22] With regard to Article 8, it underlined that "Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data".[23] If the essence of data protection is a minimum core, the impairment of which makes it impossible to exercise that right[24] or, as the Court has put it, "calls into question" the fundamental right as such,[25] an inquiry into technical or security measures will likely be insufficient to satisfy the requirements of Article 52(1) CFREU.

Contrary to the ECtHR, the CJEU has applied the principles of necessity and proportionality in quite a more structured way, requiring that any limitation imposed upon Article 8 of the Charter be strictly necessary.[26] The Court does not only examine whether the intended objective could be achieved by less restrictive means, but also often suggests alternative legislative approaches.[27] When it comes to balancing between data protection and other rights or interests, the CJEU has adopted an overly protective stance towards Article 8, upholding the protection of personal data against the econom ic interests of big tech companies,[28] as well as public access to documents.[29]

Conclusion

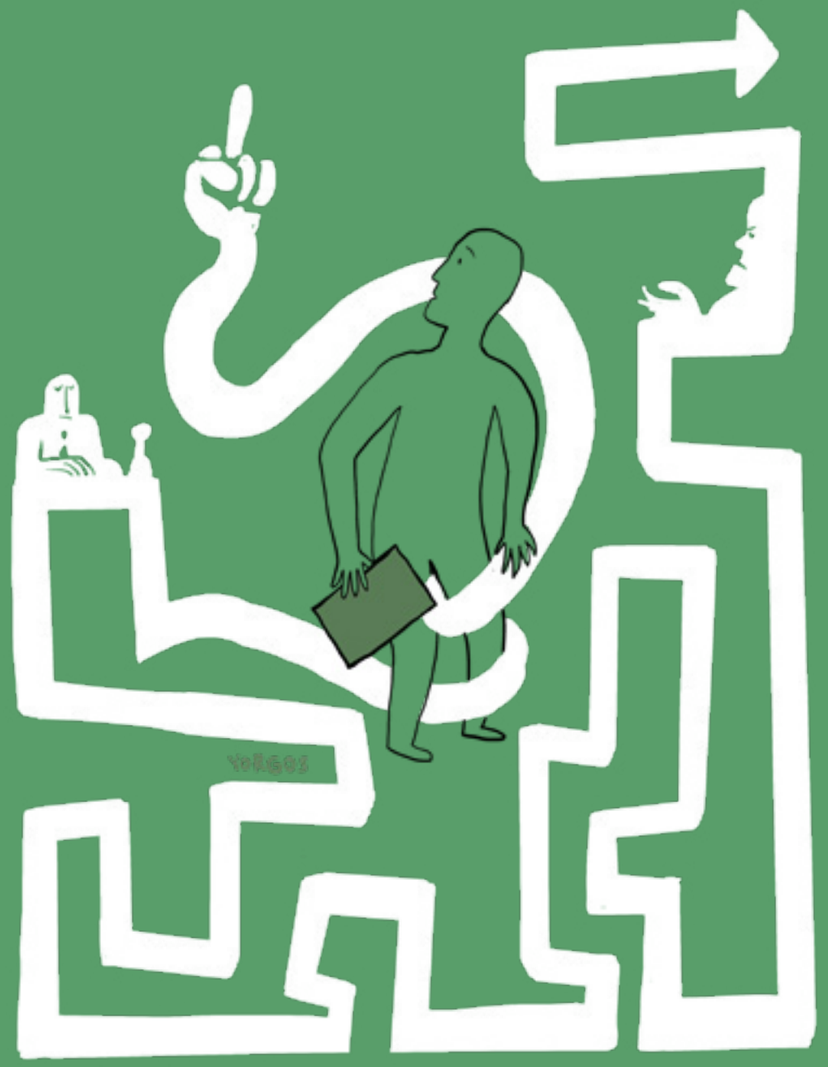
In all, Article 8 of the Charter gives data protection its own constitutional footing in the EU as a fundamental right, establishing a set of checks and balances to govern the processing of individuals' data. While the CJEU has not hesitated to interpret the provisions of Article 8 widely and uphold data protection against several other interests, it has nevertheless failed to consistently distinguish the right from that enshrined in Article 7 of the Charter and provide some clear guidance around how its requirements, including its essence, ought to be interpreted in light of Article 52(1). Despite these shortcomings, Article 8, thanks to its wide scope, remains a key provision in defending digital rights before both national and European courts. More importantly and as the case-law examined above suggests, Article 8 cases remain a valuable tool to achieve objectives that are not just limited to data protection rights but can have a wider impact, in the context of digital rights litigation.

"...Article 8 cases remain a valuable tool to achieve objectives that are not just limited to data protection rights but can have a wider impact, in the context of digital rights litigation."

Article 41: The right to Good Administration

Melanie Fink, *Leiden Law School*

Giulia Gentile, *LSE Law School*



The authors contributed equally to this work and are listed in alphabetical order.

The right to good administration, safeguarded under Article 41 of the Charter of Fundamental Rights of the European Union (EU) ('the Charter'), enshrines the analogous general principle developed in EU case law[1] into constitutional law. This right embodies the EU's position as a rule-of-law community, wherein individuals are protected from arbitrary administrative decision-making and entitled to fundamental guarantees in their interactions with EU institutions and bodies designed to ensure just and fair administrative procedures.

Under the framework of good administration, Article 41 bundles together several procedural rights. While each of these rights may have implications for the digital environment, some are particularly relevant in this context, including the right to be heard, the right to a reasoned decision, the right to damages, and the broader principle of transparency. This essay first outlines the scope of application of this provision, and subsequently discusses each of these rights in turn, culminating in a broader reflection on Article 41's relevance in the digital context.

Scope of Obligations under Article 41

Article 41's reach is confined to the EU administration in the strict sense, encompassing EU institutions, bodies, offices and agencies. By excluding member states as recipients of the obligations, Article 41 deviates from the more generally applicable rule in Article 51(1), wherein the Charter also applies to member states 'when they are implementing Union law'. On occasion, the Court of Justice of the European Union (CJEU) has seemingly implied a broader scope of application of Article 41 (see, for instance, MM v Minister for Justice, paras 81-94[2]). However, more frequently, the CJEU adopts a literal interpretation, excluding member states from the purview of Article 41 (see, for instance, R.N.N.S and K.A v Minister van Buitenlandse Zaken, para 33[3]).

Article 41, frequently perceived as a codification of the general principles of law shaped by EU courts, has significant overlap with these principles. However, contrary to Article 41, the right to good administration applies not only to the EU itself, but also to member state authorities when they operate within the ambit of EU law. This was explicitly indicated by the CJEU in R.N.N.S. and K.A. (para 34[4]). By extending the right to good administration to the entirety of the EU administration, these general principles fulfil an independent role from Article 41.

While the right to good administration solely applies to EU public authorities, a pertinent question in the digital context is whether the right itself – or the values enshrined therein – can be extended to private entities. This query becomes especially relevant when such entities collaborate with public authorities, or when they employ large-scale digital technologies that significantly impact individuals' lives, leading them to exercise powers of a quasi-public nature. Various references to the principle of good administration have been included in the proposed EU Artificial Intelligence Act (AI Act), suggesting the applicability of this principle within the remit of the regulation, and hence to private entities.

"... a pertinent question in the digital context is whether the right itself – or the values enshrined therein – can be extended to private entities. This query becomes especially relevant when such entities collaborate with public authorities, or when they employ large-scale digital technologies that significantly impact individuals' lives, leading them to exercise powers of a quasi-public nature"

The Right to be Heard

Article 41(2)(a) confers upon every person the right to be heard prior to the imposition of any individual measure that would adversely affect them. This right stipulates that individuals should have the opportunity to present their perspectives to the authorities during the actual procedure within which the relevant measure is decided (Technische Universität München, para 25[5]). Further, these views must be considered by the authorities, and must be reflected in the statement of reasons for the decision (Elf Aquitaine, para 167[6]). By permitting the affected individual to influence the decision-making process by sharing their views, the aim is ultimately to ensure more equitable decisions. By infusing elements of procedural fairness into the interaction between individuals and administrative bodies, Article 41(2)(a) is intimately tied to Article 47 of the Charter, which safeguards the rights to a fair trial and effective remedy.

Integrating the right to be heard under Article 41 into the digital landscape presents distinct challenges. One such challenge is determining how to ensure that an individual's views are considered in decision-making processes that incorporate some degree of automation. In this context, it is also necessary to address whether an individual needs to be heard by a human or if an automated tool can sufficiently meet this requirement. Of note in this respect is Article 22 of the General Data Protection Regulation (GDPR), which mandates the involvement of a human in most instances of automated decision-mak-

ing. As suggested by Article 22(3) of the GDPR, human intervention may be instrumental in preserving the right to be heard in the digital landscape.

A pertinent example is the European Travel Information and Authorisation System (Regulation (EU) 2018/1240), which is set to become operational at the end of 2023 and (partially) automates[7] the decision regarding the entry of third-country nationals into the EU. While the current regulations[8] only stipulate a right to appeal in the case of refusal, Article 41(2)(a) of the Charter will be instrumental in ensuring that individuals can effectively be heard before a travel authorisation refusal becomes final.

The Right to a Reasoned Decision

Article 41(2)(c), rooted in Article 296 of the Treaty on the Functioning of the European Union (TFEU), stipulates that the right to good administration includes 'the obligation of the administration to give reasons for its decisions'. According to the CJEU, the statement of reasons must be sufficiently clear and unequivocal so as to allow the Court to assess the legality of a decision and to equip the affected parties with adequate information to discern whether the decision is sound and contest it if it appears otherwise (Elf Aquitaine, paras 147-148). Therefore, the duty to state reasons is not merely a standalone obligation for transparency; it is instead designed to foster accountability and facilitate individuals' access to justice. In this regard, the CJEU often cites Article 47 of the Charter, the right to effective remedy, to bolster the requirement of reason-giving (R.N.N.S. and K.A., para 43).

There is a tension between the duty of the administration to articulate the reasons for its decisions and the incorporation of artificial intelligence (AI) to assist the decision-making process. The crux of this issue lies in the possibility of AI systems becoming so complex that humans cannot comprehend how or why a system reached its conclusion (referred to as the 'black box' problem[9]). Human decision-makers may struggle to clarify the specific reasons that underpin a decision heavily influenced by a 'black box'. Consider an individual denied entry to EU territory based on an AI system's[10] designation of them as a 'security risk'. If the AI system's internal processes are too opaque for the officer relying on it to understand what factors contributed to that classification, the officer's explanation cannot extend beyond 'because the AI system said so'. Such justification fails to meet the standards delineated under Article 41[11].

"Article 41 of the Charter, alongside the corresponding general principle of law, offers the most robust protection of the right to demand a reasoned decision from EU public authorities."

In recent years, an animated debate has unfolded about whether the GDPR creates a 'right to an explanation' (for[12] and against[13]). However, its existence and precise content remain uncertain. Moreover, it would not be applicable to all AI use-cases in the public sector. The proposed AI Act delineates responsibilities for manufacturers to make high-risk AI intelligible to humans (Article 13), thereby facilitating the right to explanation. Nevertheless, it does not lay down any obligations for AI users to justify or explain their decisions to those affected by them, much less a corresponding right for individuals to demand such explanations. Therefore, currently, Article 41 of the Charter, alongside the corresponding general principle of law, offers the most robust protection of the right to demand a reasoned decision from EU public authorities.

The Right to Damages

Article 41(3) guarantees every individual the right to reparation for any damage caused by the Union 'in accordance with the general principles common to the laws of the Member States'. This provision echoes Article 340(2) of the TFEU, under which the Court has consistently ruled that liability only arises for breaches deemed sufficiently serious, meaning that the authority in question has 'manifestly and gravely disregarded the limits on its discretion' (Bergaderm, para 43[14]).

The crucial question lies in how the decision to employ digital tools such as AI to support decision-making would affect the evaluation of the seriousness of an authority's mistake. The CJEU has previously determined that a reasonable reliance on another authority's assessment constitutes a pertinent factor (see, for instance, British Telecommunications, para 43[15] and Robins, para 81[16]). It remains to be seen whether this principle – that authorities may trust specific sources of information without verification – is applicable in the digital context and, if so, under what conditions. This would significantly increase the threshold for breaches of the law by decisions based on an AI system's recommendations deemed serious enough by the CJEU to warrant liability. Consequently, the prospects of successfully contesting such decisions could be slim.

In September 2022, the European Commission proposed an AI Liability Directive with the aim of adapting non-contractual liability rules to accommodate the unique challenges posed by AI systems. This directive would introduce disclosure rules and rebuttable presumptions to counteract the evidentiary difficulties that victims of damage caused (partially) by AI may encounter, particularly given the complexity and opacity of some AI systems. The Directive does not directly modify the liability rules under Article 340 of the TFEU or, by extension, Article 41(3) of the Charter. However, it may eventually influence the EU's public liability regime by impacting the 'general principles common to the laws of the Member States', which form the foundation for Article 340 of the TFEU. Additionally, the rationale underpinning the AI Liability Directive may guide the development of a more fitting approach to AI liability, especially in relation to damage caused by the EU administration through the use of AI systems.

Transparency

The principle of transparency is intimately intertwined with the right to good administration. Certain rights mentioned in Article 41 are intrinsically tied to transparency rights themselves, notably Article 41(2)(b), which guarantees everyone access to their own file, as well as the right to a reasoned decision. Beyond these specified rights, however, the principle of transparency, which is presented as a general objective of the EU throughout the Treaties, is a fundamental prerequisite for good administration.

Within the digital landscape, algorithmic opacity – whether resulting from intellectual property rights, a lack of expert knowledge, or the characteristics of the algorithm itself – poses a significant challenge to the principle of transparency. While much debate has centred on explanation rights, a pressing question is whether the principle of transparency would require much broader rights,[17] such as access to training data, source codes, or other information pertaining to the algorithm itself.

Digital sector-specific legislation often incorporates explicit transparency-related rights. For example, the GDPR outlines various information rights. These include a right to information regarding the existence and implications of automated decision-making, as well as 'the logic involved' in it (Article 13, GDPR). The proposed AI Act mandates a certain level of algorithmic transparency, but solely to enable system users to interpret the algorithms (Article 13, AI Act). Individuals impacted by the actual use of the algorithms only have a limited right: to be informed when they are interacting with an algorithm rather than a human (Article 52, AI Act). The principle of transparency, in conjunction with the right to good administration, including the right to access one's own files, may provide a more robust legal foundation for extending broader rights to the recipients of administrative algorithmic decisions.

Conclusion

The right to good administration holds significant value in regulating the use of technology by the EU administration. Specifically, by ensuring that individuals are heard and administrative decisions are reasoned, it operates as a tool for exercising the right to an effective remedy under Article 47 of the Charter.

Nevertheless, its significance extends well beyond this instrumental role. Article 41 of the Charter establishes the conditions for administrative decision-making that strikes a fair balance between societal and individual interests. This balance is particularly important in light of the profound changes in public administration ushered in by the rapidly increasing use of digital technologies, particularly when these technologies are developed and marketed by private entities.

Importantly, ensuring that administrative decision-making is reasoned and fair also enhances the likelihood of the resultant decisions conforming to the law. This conformity reduces the need for costly litigation before already overtaxed judicial institutions. Therefore, the right to good administration plays a pivotal role in ensuring that the adoption of new technologies does not undermine administrative justice and, more broadly, the rule of law.

Article 47: The age of digital inequalities

Nawal Mustafa, *Public Interest Litigation Project (PILP)*

Introduction

The Charter of Fundamental Rights of the European Union (the Charter) entered into force with the Treaty of Lisbon in December 2009. With this Charter, fundamental rights that were scattered in various national and international legal document merged into one document which serves as the single common standard for fundamental rights in Europe. The Charter is one of the primary sources of EU law. Articles 51-54 specify the criteria under which the Charter can be invoked and how the provisions of the Charter are to be interpreted. An important aspect of the Charter is the fact that it can only be invoked in cases where Member States and EU institutions are implementing EU law. As one of the main instruments of EU law, the Charter fulfills multiple roles. First, as a general principle of EU law, the Charter can be used as an interpretation tool since both national laws and EU secondary law within the scope of EU law have to be interpreted in light of the Charter. Second, it functions as an instrument of judicial review, which means that the Court of Justice of the European Union (CJEU) has power to assess the compatibility of laws, acts, and measures with the fundamental rights guaranteed by the Charter. Thus, the CJEU can overrule any national law falling within the scope of EU Law that infringes upon the fundamental rights laid down in the Charter. Third, the Charter also serves as platform for the expression and advancement of evolving general principles of EU law.

In this essay, I reflect on the legal case against the usage of the System Risk Indication program (SyRI) by the Dutch government and demonstrate how Article 47 of the Charter and the different roles of the Charter can be utilized in the context of digital rights. Since this system processed personal data, it promoted profiling and had the potential to infringe upon the fundamental right of individuals. Therefore, it had to be subjected to a number of safeguards based on the Charter and other EU legislation aimed at regulating data processing, while limiting infringements on the rights contained in Articles 7 and 8 of the Charter.

Rapid technological developments and innovations have transformed the ways in which our societies and our institutions' function. Traditional ways of working have become almost obsolete because of developments in information technology, the continuous digitalization of almost every aspect of public and private life as well as the current rise of the usage of artificial intelligence. Consequently, policymakers and legislators are capitalizing on the availability of digital data from people's utilization of technological devices. Both data-driven working and the rise in the use of AI have created numerous benefits but they also produce many negative consequences that need further critical considerations. Some of the negative implications associated with these technological developments are the loss of jobs through automation, growing inequalities in income, loss of privacy, digital racism, and what some scholars have called 'digital slavery'.[1] It is vital to recognize and mitigate the potential harms of tech developments in order to ensure that the benefits are equitably distributed. Furthermore, the legal and ethical frameworks needed to curtail the negative consequences of tech usage by public authorities are virtually none-existing. However, many of the already existing legislation can be utilized in a way that enables the reduction and prevention of harms caused by the use of tech by expanding the scope of application.

There are different legal sources from the EU relevant in the context of digital rights, data processing, and data protection.[2] The purpose of this essay is to reflect on how Article 47 of the Charter, that relates to the right to an effective remedy and a fair trial can be applied to digital contexts. The essay is divided into two sections. The first section discusses the System Risk Indication (SyRI) case in general and reflects on the relevance of this case in light of Article 47. The second part addresses the scope of application of Article 47 and attempts to highlight aspects that are becoming relevant in the digital context. Last, a brief yet concise conclusion outlines the opportunities Article 47 provides for protection against digital rights violations.

System Risk Indication (SyRI)

The Dutch government used the SyRI system in its efforts to combat and prevent social security fraud, illegal labor, and tax fraud.[3] This system was based on the so-called Landelijke Stuurgroep Interventieteams (LSI) which consisted of the close collaboration between different municipalities, the Ministry of Social Affairs and Employment, police, the Public Prosecution Service, immigration services, and the welfare and tax authorities. The exchange and analysis of digital personal data was essential for the prevention,

"Effective legal remedies that provide victims of data infringement cases with the tools they need to safeguard their rights is essential for the protection and enjoyment of fundamental rights."

detection, and investigation of fraud and other illicit activities within the framework of this collaboration.[4] The data gathered through LSI, the projects and experiments stemming from it, and the methodologies employed by the LSI, including the utilization of the 'Black Box' system, were foundational for the SyRI system.[5]

SyRI was enshrined in law in 2014 through Articles 64 and 65 of the SUWI Act, while Chapter 5a of the Decree SUWI sets out the rules and procedures of application.[6] The Ministry of Social Affairs and Employment is responsible for the use of SyRI. The reasons for providing a legal basis for SyRI were mainly to reinforce the stringent approach in combating benefit fraud by leveraging digital technologies and data analysis. Legislators and policymakers within the Dutch government also anticipated that by grounding SyRI within the law, longstanding concerns raised by regulatory bodies regarding violations of privacy rights and data protection would have to be definitively addressed.

For the purpose of this contribution, the SyRI case is important due to several compelling reasons. First, it is one of the first cases that fundamentally challenged the systematic and legislatively authorized use of digital technologies in the welfare state for the prevention and detection of welfare fraud based on human rights considerations.[7] Second, this case showed that mass surveillance technologies such as SyRI tend to disproportionately target impoverished and disadvantaged neighborhoods with higher concentrations of marginalized groups.[8] Third, the involvement of a diverse group of civil society organizations in legal proceedings against SyRI, reflect a widespread concern about the likelihood of such systems encroaching upon the rights of everyone.[9] The way different organizations collaborated in the legal procedure in fighting the SyRI system is inspiring from the perspective of access to legal remedies and fair trial.

Data privacy infringements cases such as that of SyRI cause many material and immaterial harms for which victims should be able to claim damages. Some of these harms such as depression, anxiety disorder, and Post Traumatic Stress Syndrome fall within the official categories of the Fifth Diagnostic and Statistical Manual of Mental Disorders (DSM 5). Others, such as emotional harm, stress, to damage to name and reputation can be seen as psychological harms that can lead to mental disorder. Effective legal remedies that provide victims of data infringement cases with the tools they need to safeguard their rights is essential for the protection and enjoyment of fundamental rights.

The principles and scope of article 47 Charter

When invoking Article 47, the first step is to determine whether the Charter applies at all under the test of Article 51 (1) Charter.[10] If this is the case, effective judicial protection has to be ensured by the Member States and institutions, bodies, offices of the European union when they are implementing Union law.[11] The right to an effective remedy and a fair trial are key general principles of European law. The Court of Justice of the European Union, therefore, applies these provisions in a broad and general manner so that it provides individuals with adequate judicial protection and access to justice.[12] Both administrative and procedural measures fall within the scope of article 47.[13] In order for individuals to challenge the violations of their rights and to seek redress, Member States must ensure both effective access to legal remedies and independent, impartial courts.

The rights contained in article 47 consist of the rights in Articles 6 and 13 of the European Convention on Human Rights and their interpretation by the European Court of Human Rights. Therefore, article 47 should be interpreted in conjunction with these provisions as well as in combination with other Charter rights, EU legislation and international human rights provisions. Furthermore, a key characteristic of Article 47 is the fact that its application and interpretation must prioritize and promote the realization and protection of fundamental rights.

One way it does this is by the principle of minimum effectiveness, which requires that national rules must not make the exercise of EU rights impossible in practice (effectiveness) and must not be less favorable than those governing similar domestic actions (equivalence).[14] Although, requirements of effectiveness and equivalence usually focus on national procedural rules, they can also be applied to the interpretation of substantive law such as the rights enshrined in article 7 and 8 of the Charter. Moreover, Article 47 requires that courts have to determine in every case they review whether effective remedies were available. According to the CJEU, there is a violation of the principle of effectiveness in cases where authorities refuse access to data relevant to the facts of a case.

Every time a Member State or EU institutions appear to limit the protections granted by the right to effective remedy and fair trial, the proportionality test ensures the (il)legality

of the provision. According to its preconditions, the limitation in question has to be necessary, reasonable, and proportionate to achieve a legitimate aim. Any restriction of the rights in this Article should, therefore, be concrete and not go beyond what is needed to protect public interest or other rights.'

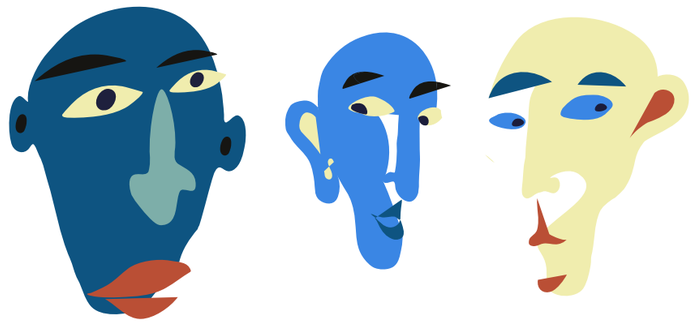
The negative aspects of data-driven working and the use of AI by authorities fundamentally change legal debates about data protection, privacy, and the right to effective remedy and fair trial. In cases of data infringement, when determining proportionality, an argument can be made based on article 47 that burden of proof should shift from the individual whose data is being collected to the authorities who are collecting the data. The reason for this is that it would be virtually impossible or excessively difficult for individuals to go against state authorities that collect and use their data without them even knowing. It is very difficult to substantiate for individuals what kinds of actual immaterial harms they experience when their fundamental rights are violated.

There does not exist specific case law directly addressing digital rights under article 47. However, the CJEU has developed a solid case law addressing digital harms with regard to articles 7 and 8.[15] This case law can provide guidance on how article 47 can be applied and interpreted in the context of digital rights.

"... the CJEU has developed a solid case law addressing digital harms with regard to articles 7 and 8. This case law can provide guidance on how article 47 can be applied and interpreted in the context of digital rights. "

Conclusion

The collection and processing of personal data is regulated on a European level. However, the essay considers that the fundamental concerns raised in the SyRI case fall within the scope of Article 47. Although the case did not reach the CJEU, and the focus of the litigation was mostly based on whether SyRI system unlawfully limited the rights enshrined in Articles 7 and 8, the judicial review contained in article 47 provides a fruitful venue for future litigations. National courts could ask the CJEU to assess whether laws that enable systems such as SyRI are compliant with the rights enshrined in the Charter. Moreover, litigation based on Art 47 can contribute to the development and evolution of EU law in the digital rights context by clarifying its scope, enhancing protection of fundamental rights, and promoting the rule of law. It can serve as a powerful tool for advocacy, highlighting human rights abuses, and fostering legal reform at both the national and European levels.



Article 34: 'Digital Welfare' and the fundamental Rights to Social Security and Social Assistance in the EU

Divij Joshi, *University College London*

Introduction

In his seminal 2019 report to the United Nations, Philip Alston, the Special Rapporteur on Extreme Poverty, issued a stark warning that 'humankind [...] must avoid stumbling zombie-like into a digital welfare dystopia'.[1] This compelling statement was the conclusion of a pioneering study on the global integration of emerging digital technologies such as biometrics, computerised data processing and algorithmic decision-making systems into social security and welfare administration. The report found that the use of digital technologies in welfare administration often resulted in practices that likely infringed upon human rights, including the rights to social security, life with dignity and privacy.

Despite this sobering report, governments worldwide, including in the European Union (EU), have not heeded the Special Rapporteur's call for greater introspection in their adoption of digital technologies in delivering social security. This essay explores how EU member states have employed data-driven and algorithmic digital technologies in designing and implementing their social security and welfare systems and discusses the potential and real harms that such systems entail. In addition, it assesses the role of the EU Charter of Fundamental Rights of the EU ('the Charter'), particularly Article 34 on social security, in evaluating the legality and legitimacy of digital welfare systems.

Digital Welfare in the EU

Social welfare administration has long incorporated computer-assisted processes and digital information processing. However, this 'digitalisation' of welfare administration has been pursued more rigorously in recent years, in line with the rise of computerisation and the internet, leading to significant changes in the ways in which states fulfil their obligations to provide social security. Eager to adopt new data-based technologies to enhance their governance capabilities, governments have strived to make their citizens more 'legible' and thus more governable. However, as various scholars have noted, the enhanced legibility offered by datafication and digitalisation often comes at the cost of increased surveillance,[2] population-based experimentation,[3] and over-reliance on potentially flawed statistical methodologies.[4]

"The digitalisation of welfare systems has the potential to systematically reduce government transparency, promote arbitrary and discriminatory decision-making, and undermine procedural safeguards against governmental abuses of power. "

Empirical research suggests a rising trend of welfare digitalisation across the EU, manifested in varying degrees and forms. For instance, several studies have documented how Denmark, the Netherlands, Portugal, France and Poland have implemented algorithmic systems to combat 'welfare fraud' in sectors such as taxation, universal benefits, healthcare and education. Such systems process personal data for risk-based scoring and classification, which are used to predict the likelihood of benefit fraud in a given scenario.[5] Trelleborg, a municipality in Sweden, introduced an ambitious system aimed at 'fully automat[ing]' social welfare applications and entitlements. This included using rule-based algorithmic systems to process citizen data and determine eligibility for benefits such as financial aid.[6] In Slovenia, digitalisation has been leveraged to create comprehensive citizen profiles to increase legibility. This has enhanced visibility into how citizens are using social services across various domains and is thus used to inform social security policy.[7]

The process of digital adaptation and transformation has led to an increase in technologically mediated exclusion from social security and welfare systems, an issue that states have failed to adequately address. The case of Systeem Risico Indicatie (SyRI), a data-based risk calculation system deployed by the Dutch government, is a compelling example of how such data processing systems can jeopardise social security. SyRI linked citizen data across administrative agencies and served as input for computational models that predicted welfare fraud risk. However, the nature of the information used, the risk calculation model, and the computational algorithms were neither publicly disclosed nor communicated to affected individuals. This lack of transparency meant that individuals could be flagged for fraud investigations without sufficient explanation. The legislation and implementation of SyRI were subsequently challenged in a Dutch Civil Court, which deemed the system illegal on the grounds that it violated various rights guaranteed by the European Convention on Human Rights, including the right to privacy.[8] However, despite a court-ordered injunction against SyRI, subsequent investigations revealed that the Dutch government had continued to experiment with comparably risky digital welfare systems, demonstrating the deep entrenchment of digital technologies within welfare administration in certain states.[9]

As exemplified by the cases above, digital technologies are extensively used in automated decision-making systems, where the outputs either replace or supplement human decision-making in tasks such as identifying and authenticating social security recipients, determining benefit eligibility, calculating benefit amounts, and detecting fraud.[10] The deployment of these systems profoundly influences the relationship between citizens and the state and, consequently, the fundamental rights of EU citizens.

The digitalisation of welfare systems has the potential to systematically reduce government transparency, promote arbitrary and discriminatory decision-making, and undermine procedural safeguards against governmental abuses of power. This issue stems partly from the complex nature of these information processing systems, which can be difficult to comprehend or scrutinise and frequently lack sufficient documentation or explanation to ensure transparency and accountability.[11] The opacity of SyRI is a case in point; the government failed to disclose the types of personal data used to profile citizens or the way that such profiles were constructed. Another potential risk arises from discriminatory and arbitrary data processing.[12] For example, in Austria, an employment assistance allocation program reportedly assigned lower scores to individuals based on gender identity and disability status, potentially compromising their ability to make claims on the scheme.[13] This underscores the fact that digital welfare systems can employ data in ways that are discriminatory, either overtly or through the use of proxies. Furthermore, these systems are frequently implemented in contexts that lack adequate and systematic accountability or oversight. This implies that individuals could lose access to social security without prior notification or the opportunity to participate in, appeal, or challenge decisions regarding their entitlements.[14]

Article 34 and the Right to Social Security

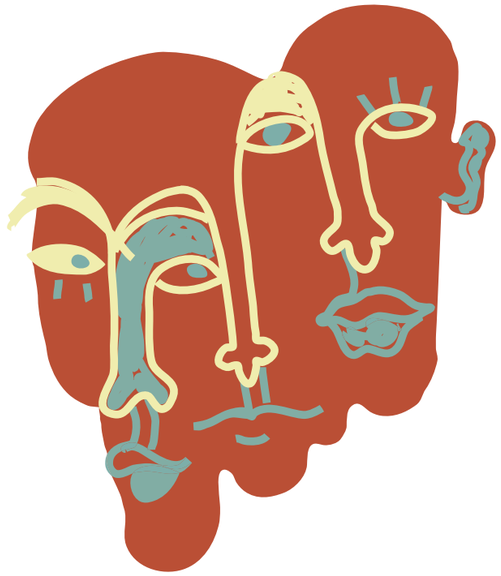
The Charter, which is binding for all EU member states, distinctly stipulates a right to social security within Article 34 on solidarity. The scope and applicability of Article 34 as a right to social security is specified as being 'in accordance with community law and national laws and practices'. This article should be interpreted in conjunction with Articles 51 and 52 of the Charter, as well as the Treaty on the Functioning of the European Union (TFEU). Under this context, Article 34 is only pertinent in the implementation of EU law, or within the Union's areas of legislative competence. Articles 34(1) and 34(3) of the Charter serve as guiding principles, rather than prescriptions, for the EU and its institutions, mandating that any implementation of EU law must conform to their requirements. Currently, as there is no Union law that stipulates minimum social security benefits, it is only Article 34(2) which provides a subjective entitlement (or a right) for all persons 'residing and moving legally' within the EU. Nonetheless, the right in Article 34(2) is effectively confined by and incorporated within Regulation 883/2004, which coordinates social security systems across member states. Consequently, as some scholars contend, Article 34 in itself does not provide a justiciable right against member states' social security instruments or administration, for example, to claim minimum entitlements for housing, employment or social assistance. However, in the context of artificial intelligence, the European Fundamental Rights Agency interprets Article 34(1) of the Charter as offering protection against measures restricting or abolishing existing social security rights.[15]

Case law before the Court of Justice of the European Union (CJEU) provides scant assistance in interpreting the scope of Article 34. Article 34(1) has not been substantively analysed by the CJEU. Still, according to Advocate General Mengozi's opinion in Melchior and Wojciechowski, Article 34(1) can only serve as an 'interpretative reference or as parameters for ruling on the legality' of implementing legislation. In cases like Melchior, Wojciechowski and Dano, the CJEU found the Charter inapplicable as the cases concerned national legislation, not union law. Nevertheless, in Kamberaj, a case involving the refusal of housing assistance to a third-country national, the CJEU invoked Article 34(3) to aid in interpreting EU Directive 2003/109, which defines the entitlements of third-country nationals. This Directive mandates that states must observe equal treatment in providing core benefits for social protection. Within the context of Article 34(3), the Court interpreted 'core benefits' as those that fulfil the purpose of social security protection under Article 34(3) and which would 'ensure a decent existence for all those who lack sufficient resources'. Some scholars have also noted how non-specific provisions of the Charter have been relied upon to secure social security rights, such as the Right to Dignity in Article 1.[16] Overall, although some disagreement exists regarding the Charter's scope of application in relation to social security measures,[17] Article 34's provisions may still be expansively interpreted by the CJEU and in future developments concerning social security entitlements at an EU level.

Despite the limitations of Article 34 as a justiciable right to social security in the EU, its potential utility lies in mitigating the negative effects of digital welfare schemes on individuals and evaluating their legality within the broader framework of EU fundamental rights. Particularly, when positioning Article 34 within the broader context of EU fundamental rights and international human rights law, we propose that a right to social security should require that state interventions in digital welfare systems comply with obligations of transparency, non-discrimination and non-arbitrariness. Invocations of a right to social security in international human rights law, such as Article 9 of the International Covenant on Economic, Social and Cultural Rights (ICESCR),[18] provide some guidance as to this right's substantive content considering states' social security provisions. The Committee on Economic and Social Rights at the United Nations, for example, has recognised that a right to social security encompasses the ability to enjoy social security benefits without discrimination, whether in law or fact; transparency as to the conditions that qualify or disqualify beneficiaries, and that such qualifications must be reasonable and non-arbitrary; and the ability of beneficiaries to participate in social security administration, such as through receiving notice of claims and other information about their entitlements.

Even though the interpretation of Article 34 as a justiciable right to safeguard against the harms of digital welfare schemes remains limited, it provides an essential benchmark against which these emerging systems should be tested. Regardless, EU member states must ensure that their forays into digital welfare systems align with the intents and purposes of the right to social security, countering the insecurity, opacity, and precarity these systems engender.

"Regardless, EU member states must ensure that their forays into digital welfare systems align with the intents and purposes of the right to social security, countering the insecurity, opacity, and precarity these systems engender."



Article 28: The right to collective bargaining and the case of platform workers

James Farrar, *Worker Info Exchange*

Many trade unionists have a healthy scepticism of the law and for good reason given the history of the criminalisation of the class struggle since the industrial revolution.

In the 1830's, six leaders of an emergent agricultural trade union in southern England were arrested and sentenced to seven years transportation to the penal colony of Australia. The fate of these Tolpuddle martyrs gave rise to the birth of the modern trade union movement in Britain.

Trade union activity was considered a criminal conspiracy and a restraint of trade in Britain until the passing of the Trade Union Act of 1871[1] but even then, picketing and striking remained a criminal offence until 1875.[2]

To this day, trade union activists continue to face similar perils the dichotomy where the freedom of association is observed but the freedom let alone right to protest and strike most definitely is not.[3] And so, the state has ridden roughshod over the right to strike for generations. In 1972, twenty-two UK trade unionists were convicted of the criminal offence of 'conspiracy to intimidate' and imprisoned after staging strikes on building sites around Shrewsbury. In 2021, the convictions were finally overturned. In 1984, ninety-one striking miners at Orgreave were charged with riot and violent disorder offences only for the cases to be dismissed against all after massive police misconduct in the cases was revealed.

Into current times, resistance from the state continues. The Police, Crime Sentencing and Courts Act of 2022[4] applies strict new criminal sanctions on the right to protest in the UK which leaves striking workers and public protesters in continued jeopardy. In recent days we have seen violent state repression of striking workers in France protesting the raising of pensionable age. And although class solidarity is a fundamental principle of the struggle for worker rights, secondary strike action remains illegal in many countries in the EU as it is in the UK.

But it was ever thus. We must recognise the historic reality that strike action and collective action is carried out within the context of continued class conflict between the capitalist ruling class and the working class. The rights and freedoms we have were hard won but are still strictly controlled, moderated and reduced by the ruling class. The good news, is that the permanent revolution can, must and will carry on regardless because the struggle is far from over.

Misclassification and the resistance of capital against so called gig-economy workers

Misclassification in the gig economy is most associated with platform employers who use mischievous contracts with workers to wrongly label them as independent contractors to avoid employment obligations. But there are other affects that are just as damaging to the long-term collective interests of workers. In attempting to form the App Drivers & Couriers Union (ADCU) in 2020, we were immediately faced with three obstacles to our recognition by the government regulator. First, we had to prove we were already acting as a trade union before we could be recognised as one – a chicken and egg conundrum. Second, we had to show the union was acting in the collective interests of member workers in the regulation of the relationship between the workers and employers like Uber. This was almost impossible, given the asymmetry of power between the union and the might of a platform company like Uber or Deliveroo and their absolute refusal to acknowledge our rights to collectively bargain. Eventually, we satisfied the regulatory by demonstrating sufficient collective action on behalf of the workers in the establishment of our data trust for workers with the objective of building collective bargaining power by making earnings and work allocation more transparent to union members.

Finally, upon certification we were warned by the government regulator that if we failed in our case at the Supreme Court to be recognised as workers, our trade union certification would be revoked. This is because under British trade union law unions must be made up primarily of workers. So, if misclassification had been held up under the technicality of law as it has been thus far for Deliveroo couriers, those in most need of trade union protection of the collective would be denied it. As it is, the ruling class and the courts absurdly consider Deliveroo couriers to be part of the capitalist class because they are as yet denied recognition as workers. This is because the law generally recognises the right of substitution as a key test in determining whether someone is a worker or an independent contractor. For drivers delivering passenger services such substitution is usually strictly forbidden by local transport licensing conditions. In food delivery, the right is offered not because further outsourcing is desirable or necessary from a business perspective but because it is a means of defeating employment claims. The tragic side effect is the rise of greater industry precarity and modern slavery conditions. In one case

examined by Worker Info Exchange, a data subject access request revealed that forty-nine workers were linked to a single bank account on the platform.

Yet, without the limited protection of worker or employee status, trade unions or employee groups place themselves in peril if they take collective action. In 2018, the GMB union was forced to abandon strike action against an Amazon delivery service provider after they were threatened with tort action to sue for damages resulting from strike action undertaken by drivers not classified as workers.[5]

Similarly in Spain, taxi driver members of Elite Taxi and Taxi Project have been threatened with a fine of EUR 120,000 after a complaint was made that their protest action against Uber was a restraint of trade damaging to Uber.[6] Without employment or worker status, the most precarious of workers are exposed to these formidable legal risks.

Large platforms have been quick to ingratiate themselves and align their interests with government and the ruling class. In California, gig economy platforms successfully allied to lobby for the inclusion of a proposition on the ballot of a general election. The proposition was effectively a referendum to single out gig workers and deny them the employment rights they had established in the courts under state law. This cruel ballot was successful although the legal challenge of its constitutionality carries on.

"...despite the rights and freedoms to strike and engage in collective bargaining in Europe, in practice such rights are under threat."

In Europe, Uber and other ride share platforms have driven a strategy of determined integration into the mass public transport system offering. This includes not only ride share services but also micro mobility services such as scooters and bicycles. At the same time the power of platform of platform intelligence has proven very valuable indeed to police and intelligence forces[7] as well as for central government strategic planning in the response to Covid[8]. While there is some distance still to travel, it is easy to see how platform companies ultimately become not only too big to regulate, but they also appear indispensable to society to the point that strike action might be limited in ways 'such as are prescribed by law and are necessary in a democratic society in the interests of national security or public safety, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others.'

Make no mistake, despite the rights and freedoms to strike and engage in collective bargaining in Europe, in practice such rights are under threat. In 2022, the International Trade Unions Congress reported that the right to strike was under attack due to increased criminalisation of striking workers while the right to collectively bargain was also under serious erosion.[9]

"In the gig economy, misclassification and misinformation has muddied the waters on progress towards collective bargaining."

In the gig economy, misclassification and misinformation has muddied the waters on progress towards collective bargaining. In 2021, Uber reached a recognition agreement with the GMB union[10]. Crucially, the deal falls short of a collective bargaining agreement to tackle the problem of chronically low pay and the failure to recognise waiting time as payable working time. In 2022, the GMB signed a recognition deal with Deliveroo which concedes that couriers for the company are not workers but are independent contractors.[11] In the case of Uber, the current driver contracts expressly deny any collective bargaining element of the contractual agreement. Similar deals have been signed in the US, Canada, Australia and Belgium.

In such agreements perhaps we see tactics of big union, industrial bargaining methods of another era applied in the service economy with employers not acting in good faith and not yet willing or ready for true partnership in collective bargaining. Too often the result of this top-down approach is ineffective union agreements with the employer or low paid service workers are simply left behind.

In Sweden, despite the long history of the famous Swedish social model, gig economy workers find themselves firmly outside of collective bargaining either at the enterprise or sectoral level and outside of state protection also as a result. In Sweden, much of the management of labour relations is not legislated for but remains in the domain of the social partnership between unions and employers. For this reason, Sweden has not seen the need to legislate for minimum wage.

Indeed, in December 2022 the Swedish government strongly objected to the proposed EU platform work directive on grounds that it would interfere with the Swedish social model including collective bargaining.[12]

It is clear the stability attained by well organised, and state influenced collective bargaining arrangements can backfire and end up being counterproductive. Such circumstances arise, when the objectives of such collective bargaining become disconnected and remote from the true underlying class struggle.

Worker Info Exchange and the App Drivers & Couriers Union has waged a long battle for worker rights against Uber. They have also waged a parallel battle for algorithmic transparency and worker access to personal data at work against Uber and Ola Cabs as a means towards building collective power of platform workers. Ola Cabs has argued before the courts that such objectives amount to an abuse of rights under Article 15 and Article 20 of the General Data Protection Regulation (GDPR). The lower courts rejected this argument saying that as long as the objective of the data subject included the exercising of the right to inspect and check data for accuracy it mattered not if the secondary objectives were to share the data with their trade union for the purposes of building a worker data trust. The lower court went on to point out that one of the objectives of portability guaranteed to workers by Article 20 was "to further strengthen the control over his or her own data"[13] and so transferring personal data to a trade union or a worker data trust was perfectly compatible with the law.

Ola Cabs appealed this point and the Amsterdam Court of Appeals also rejected Ola Cabs' suggesting the collective use of data amounting to an individual abuse of process. "The fact that the present requests also pursue certain trade union interests or strengthen the drivers' bargaining position does not alter the fact that the appellants were free to submit the present requests under the GDPR without having to prove any interest. After all, Articles 15 and 20 of the GDPR do not require such an interest. In this regard, the court points to the case-law of the Court of Justice of the EU (hereinafter: CJEU), which emphasises that the GDPR aims, in particular, to ensure a high level of protection of natural persons within the Union and that, in that regard, the general legal framework created by the GDPR gives effect to the requirements arising from the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter of Fundamental Rights of the European Union, in particular the requirements expressly laid down in paragraph 2 of that article."[14]

Article 28 of the EU Charter of Fundamental Rights (CFR) provides a clear right to collective bargaining and strike action but both rights remain heavily restricted by member state governments. However, we must recognise that these rights exist within the context of an ongoing class conflict, a state of permanent revolution where even the trade unions themselves and institutions of government are subject to forces of reform and renewal in line with the manifest class struggle. The rights to strike and collective bargaining therefore must serve to facilitate the class struggle, not merely to contain or restrict it.

Article 37: Environment protection, internet infraestructure and the data economy

Fieke Jansen, *Critical Infrastructure Lab – University of Amsterdam / Green Screen Climate Justice and Digital Rights coalition*

The datafication of everyday life has transformed digital rights from a niche to a transversal issue that cuts across all aspects of society and is seen as a prerequisite for people to have the ability to exercise their human rights. This societal shift has also had an impact on how digital rights issues are approached. Where in the past discussions on surveillance technology were firmly rooted in the right to privacy and data protection, these have since then become tied to issues around racialized policing[1] and the xenophobic nature of fortress Europe[2]. Debates about competition moved from net neutrality principles to the data economy - the centralization of money, power and wealth in the hands of a few technology companies. This article will discuss another emerging nexus, digital rights and the right to environmental protection, article 37[3] of the European Charter of Fundamental Rights. It will start by illuminating intersections between climate, environment and technology. After this, it will engage with article 37 and the foundations that are needed to use this fundamental right to curtail the extractivist nature of the internet and its data economy.

The environmental implications of the internet

Rising sea levels, wildfires, droughts, heat waves, and other weather changes are impacting communities, animals, and plants around the world. These events should not be approached as singular issues but as interconnected manifestations of the era of environmental degradation and climate crisis[4], we are currently living in. Our economies and industries, including the data economy and big tech, are designed to exacerbate systemic inequalities and rapidly deplete the planet. To stay within planetary boundaries, we need to make a rapid and unprecedented change to a more just and sustainable society. This includes understanding and acting on the nexus of environment, climate and technology.

To this end, a loose coalition of individuals, climate justice and digital rights practitioners, funders, and academics came together two years ago. The Green Screen Climate Justice and Digital Rights coalition started by exploring what it means to centre climate justice in digital rights[5] and grasp the environmental impacts of the internet. We are now in the process of convening, building coalitions between the different movements, and identifying actionable pathways forward on a number of topics, litigation could be one of them. This article is based on the work, research, and discussions we have had in the past two years with community organizers, activists, artists, funders, and academics.

Initial research[6] commissioned by the Green Screen coalition highlighted that at the nexus of climate justice and digital rights are disputes over natural resources, rampant greenwashing misinformation by fossil fuel companies, and extraction of critical raw materials for hardware that result in tremendous ecological impact. It is important to note that these are some of the many complex problems at the intersection of climate and technology. Other topics that have since then surfaced are the need to identiying and challenging false and misleading climate solutions[7], extractivism, and the need for solidarity – standing next to climate, environment, and land activist Below I will elaborate on the natural resources conflict and data centres and the mining of critical raw materials.

Research shows that in 2020 internet and communication technologies represent between 1.8% and 2.8% of global greenhouse gas emissions[8] and are estimated to jump to 14% in 2040[9]. In addition, data centres are becoming one of the internet's frontiers in conflict over land, electricity[10] and water[11] rights, between data companies and local residents. In the Netherlands, Meta's planned data centre was estimated to gobble up twice the energy usage of the city of Amsterdam[12], and Microsoft's data centre will be the sole consumer of a large-scale windmill park[13]. The residents of the Dutch countryside feel cheated[14] as they were promised local renewable energy production for local consumption, but politicians prioritized the technology industry over household needs. Similarly, Meta's desire to expand its data centre in Los Lunes, New Mexico, USA raised conflict over access to water[15]. In this water-scarce area, the water needs of Meta were prioritized over the basic rights of citizens.

The extractivist nature[16] of our data economy. The internet is not a cloud[17], it is a material infrastructure of cables, wires, switches, and end-user devices. It is an infrastructure that is designed, maintained, and regulated by people and institutions for the purpose of interconnectivity, speed, efficiency, and resilience. The cloud metaphor obscured the extractivist nature of the internet and the reliance on critical raw materials. APC reports[18] that "minerals used in the manufacture of technology continue to be sourced from areas and regions where environmental destruction and human rights abuses and conflicts occur, and where reprisals against environmental and land defenders by state

"The environmental movement has a long history of strategic litigating through which they have forced companies and states to reduce carbon emissions, assign responsibility and claim damages after a gas or oil leak contaminated land and water that lead to loss of property value, physical and mental harm, and to halt the issuing of new fossil fuel extraction permits."

and private actors are common". Critical raw materials needed for the internet and its data economy are considered scarce in the global supply chain[19] and are primary sources from China, Turkey, South Africa, and the Lithium Triangle[20] in Chile, Argentina and Bolivia.

These examples highlight the nexus and the connection between environmental degradation, climate crisis, and the internet and the data economy. There is a nascent and growing field that has started to discuss these issues, challenge misleading tech climate solutions, and work towards sustainable and equitable internet infrastructures. Yet, the urgency of the climate crisis, the environmental disaster of mining and e-waste, and the exclusion of those disproportionately impacted in solutions to the problems require us all to act. In the next section, this article will discuss how to move towards connecting environmental protection to digital rights issues.

Article 37 Environmental protection

The internet and its data economy have a demonstrable impact on the environment, yet the European Commission[21] positions technology as a way out of the climate crisis. Investments in smart city technologies and artificial intelligence are seen as ways to mitigate and adapt to the climate crisis. The underlying assumption is that technology will make other industries more efficient and less polluting and create early warning systems that allow states to mitigate rising sea levels, forest fires, droughts, and other weather changes. There is no critical reflection on how these infrastructures and technologies contribute and exacerbate to environmental degradation, climate change and social crisis.

In siloing the twin transition – the Green New Deal and the digitization agenda - and prioritising technical fix over rapid industrial changes the European Union and its nation-states are prioritising economic interest and geopolitical standing over social and environmental protection. The question is how do this relate to article 37 Environmental protection[22] of the European Charter of Fundamental Rights? Article 37 states that "a high level of environmental protection and the improvement of the quality of the environment must be integrated into the policies of the Union and ensured in accordance with the principle of sustainable development". Legal analyses of article 37 foreground a number of challenges.

> "Its wording differs strikingly from that of a classical right provision: the term 'right' itself is omitted, as are similar terms used in other Charter provisions that do grant and protect individual rights"

What this boils down to is that article 37 is a declaration of principles. It does not stipulate any individual judicial rights to environmental protection or a healthy environment, nor does it specify any beneficiaries. The article gives vague administrative guidelines, it lays down the duties of public authorities to include environmental considerations in policy-making and implementation without defining or operationalizing concepts such as 'high level of environmental protection' and 'principles of sustainable development'. As such, each public authorities can flexibly interpret these broad and undefined concepts. Finally, article 37 also did not encode procedural environmental rights, failing to guarantee the rights of access to information and public participation in decision-making processes around their environment, as stipulated in the Arhuus convention.

There is no case law that uses the article 37 to challenge the environmental impact of internet infrastructures and new technologies. Which is not surprising as addressing the environmental and climate impact of the internet is an emerging issue. This article can therefore not illustrate how Article 37 has been applied to curtail the extractivist nature of this industry. However, it will draw on the work of the Green Screen Coalition to highlight conditions for cross movement collaboration, that could allow the movement to utilize the EU Charter's potential to defend and protection digital and environmental rights. Building a climate justice and digital rights coalition requires investment in articulating a joint entry point, building a community, articulating a political ideology, finding common ground, learning from each other, and defining a joint actionable agenda.

Cross movement collaboration

Articulating an entry point. In their book, Pollution is Colonialism[23], Max Libioron argues that we need to study up and move away from a focus on harm to one on violence. A harms frame centres on why a certain industry is polluting at a certain time and space, i.e. x amount of renewable energy is prioritized over the needs of households or x amount of lithium and water is used in the production of a computer. This approach creates technocratic openings to find conditions under which pollution is deemed acceptable. A violence frame argues that with the scale of the internet and the data economy, we can assume it will use x amount of energy and water to operate and x amount of critical raw materials to exist. As such, this industry in itself is a polluter.

BUILDING A DIGITAL RIGHTS AND CLIMATE JUSTICE NETWORK. Most people who are starting on this nexus are either experts in the digital rights, climate justice or environmental justice field. As such, the breadth and depth of this issue area require the different movements to work together, find strategic moments to connect, leverage opportunities for joint actions, and shared learning and experiences on specific topics.

BUILDING A COMMUNITY THAT RESEMBLES THE COMPLEXITY OF THE PROBLEM. We need voices and expertise from those most impacted, the environmental and climate movement and the digital rights community to stop extractive practices, find solutions, and actively influence the upcoming chips act and critical raw materials act. This requires an approach that respectfully centres communities most impacted by the climate crisis, pollution, environmental mismanagement, and harmful industry practices to ensure solutions do not repeat existing systems of oppression.

ARTICULATING A POLITICAL IDEOLOGY.[24] Diversity of voice brings together a myriad of needs, perspectives, priorities, privileges, and approaches. This requires an articulation of a theory of power. Historically, the two movements have had different relationships with the market and the state. For example, companies were natural allies to the digital rights community in the early days of the internet, while the climate and environmental movement has a critical and adversarial relationship to the market and specifically fossil fuel companies. Even though these dynamics have changed and the relationship with Big Tech has become more adversarial, coalitions need to discuss their theory of power.

FINDING COMMON GROUND. The different movements have their own unique histories, struggles, vocabulary, communities, and action repertoire. To connect the nexus of environmental protections and digital rights it is important to find common ground. This requires curiosity and humility to learn from each other movements and find a shared cause to rally around. A natural theme could be extractivism[25] which refers to the extraction of critical rare minerals needed for digital devices, consumption of other natural resources, such as water in both the mining and the data process, and the broader profit-driven extractivist approach of the technology sector.

LEARNING FROM EACH OTHER. The environmental movement has a long history of strategic litigating through which they have forced companies and states to reduce carbon emissions, assign responsibility and claim damages after a gas or oil leak contaminated land and water that lead to loss of property value, physical and mental harm, and to halt the issuing of new fossil fuel extraction permits. Recently Urgenda won a court case against the Dutch state for not upholding their duty of care to protect and improve the environment in relation to their lack of action on greenhouse gas emissions reduction. Practically, this meant that in 2020 the Court of Appeal in The Hague ruled that the state has to reduce CO2 emissions by 25% compared to 1990.

Conclusion

The urgency of the climate crisis requires every industry to centre a sustainable and equitable future in their current activities. This includes the data economy and requires this industry to fundamentally shift away from its extractivist nature, the strive for infinite growth, and misleading tech solutionist fixes to wicked problems. This will not happen naturally. Article 37 of the EU Charter, articulating the right to environmental protection, could be an avenue to force those investing, running and profiting from the internet and its data economy to change. To get there we need to invest in building a coalition of those impacted, the environment, climate justice and the digital rights movement.

Acknowledgements

This article could not have been written without the endless conversations I had with Michelle Thorne, Maya Richman, the Green Screen coalition, the authors of the landscape analysis and issue briefs[26], participants of the Berlin and San Jose meeting, and many others.

"Article 37 of the EU Charter, articulating the right to environmental protection, could be an avenue to force those investing, running and profiting from the internet and its data economy to change. To get there we need to invest in building a coalition of those impacted, the environment, climate justice and the digital rights movement."

Article 38: Sugar-coating or real operational instrument?

Alexandre Biard, *BEUC – The European Consumer Organisation*

All views expressed here are personal.

Article 38 of the EU Charter states that "Union policies shall ensure a high level of consumer protection". Together with other articles on healthcare, environmental protection, or social security, it is part of a broader Title IV on "Solidarity", which sets out the fundamentals of EU policies. Art. 38 is based on Art. 169 of the Treaty on the Functioning of the European Union (TFUE).[1] However, whereas Art. 169 TFUE provides for additional information as to the way the Union must ensure a high level of consumer protection, the wording of Art. 38 remains short and abstract. Like the whole Title IV, the legislative history of Art. 38 was tumultuous.[2] The initial version of the Charter referred to "a high level of protection as regards the health, safety and interests of consumers".[3] Later amendments went as far as proposing to remove Art. 38 in its entirety[4] or turning it into a subjective right for consumers.[5] The final agreed version was finally described as a compromise.[6]

At first sight, the role of Art. 38 seems double-sided. On the one hand, its insertion in the Charter conveys a strong symbolic message as it establishes consumer protection as one of the fundamental goals of EU policies. It also acknowledges the growing role that consumer protection has been playing in the EU. On the other hand, the operational dimension of Art. 38 raises several questions. First, although included in the EU Charter of Fundamental rights, Art. 38 tends to merely establish a principle and not a right which could be invoked by individuals directly. Second, its broad wording raises questions as to the extent it truly guides the intervention of EU policymakers when preparing new legislative proposals. Beyond these doubts, the question is whether and how Art. 38 could have a more practical role to play in the future.

A (limited) relevance ex ante from a policymaking perspective

Art. 38 establishes "high level of consumer protection" as an overarching objective guiding EU policy. The question is whether reference to Art. 38 by EU institutions when designing new policies is meaningful and well-thought or whether simply amounts to a form of sugar-coating. A careful attention to the preparatory works which accompanied several recent EU legislations with relevance in the area of consumer protection can help shed some light on this issue.

Consider first the proposal for a European Directive on representative actions (EU Directive 2020/1828). In its explanatory memorandum, the European Commission highlighted that "the proposal contributes to ensuring a high level of consumer protection (Article 38 of the Charter)".[7] Yet it did not provide any additional clarifications as to what this meant in practical terms. The contrast is strong when considering the following paragraph dedicated to Art. 47 of the EU Charter where the European Commission concretely explained why and how the legislative proposal met the requirements of Art.47.[8]

The same observation holds as regards the proposal on better enforcement and modernisation of EU consumer protection rules (EU Directive 2019/2161). Its explanatory memorandum merely stated that "the proposal is in accordance with Article 38 of the Charter of Fundamental Rights according to which the EU must ensure a high level of consumer protection" but failed to clearly define what this entailed in practice. Finally, also consider the proposal for an AI Act. The explanatory memorandum explains that "as applicable in certain domains, the proposal will positively affect the rights of a number of special groups, such as the workers' rights to fair and just working conditions (Article 31), a high level of consumer protection (Article 38) (...)". However, beyond high-level statements, the AI Act, as proposed by the European Commission, does not contribute to a high level of consumer protection. As BEUC highlighted:

> "Beyond the declarative non-binding layer in the recitals, consumer protection is lacking in the proposed AI Act. The proposal does not refer to protection of consumers from the adverse impact of AI among the legislative objectives of the AI Act. Consumers are not granted horizontal rights under the proposal and are excluded from the conceptual framework as definition of 'user' in the proposal is only defined as an institutional or business user".[9]

Because of its vague wording, which can be interpreted in many different ways combined with the difficulty to define what a "high level of consumer protection" concretely entails, the normative function of Art. 38 appears limited in practice, with a risk that its reference by EU policymakers often remains an empty shell.

A (growing) relevance ex post from an enforcement perspective

When drafting the Charter, the Convention thought of Art.38 as a principle and not a substantial right for individuals.[10] This comes with some consequences as Art. 51 provides that the rights under the Charter must be respected while principles must only be observed. The question now is whether it may be possible to go beyond this original assumption and turn Art. 38 into as a useful instrument which could be actionable by individuals and civil society organisations. Interestingly, in its 2020 report, the Agency for Fundamental Rights seemed to already blur the lines by referring to a "right to consumer protection" and using consumer protection in the context of strategic litigation:

> "Civil society organisations (CSOs) and others active in the field of fundamental rights, such as NHRIs, NGOs or lawyers specialising in human rights and other human rights defenders, can use the Charter in all the different aspects of their daily work. This includes strategic litigation and advocacy, awareness raising, education, monitoring and research. The Charter's supranational nature and its explicit wording make it an important tool for strategic litigation. The right to data protection, the right to consumer protection, and the right to a fair trial serve as examples."[11] (emphasis added)

A look at the case law of the Court of Justice of the European Union (CJUE) provides for some guidance as to the way Art. 38 may be actioned. In two decisions concerning air passenger rights, the CJUE used Art.38 to balance and restrict the application of other rights also at stake. Specifically, case C-12/11 (Mc Donagh v Ryanair)[12] was about a dispute between an air carrier and a passenger who had been refused the care provided for under EU legislation 261/2004 after a volcano eruption had caused the cancellation of flights. Among others, the airline argued that the obligation to provide care for passengers as foreseen in EU law impaired its fundamental rights under Art. 16 (freedom to conduct a business) and 17 (right to property) of the EU Charter. Consequently, the airline argued, the relevant EU law provisions were invalid. The Court referred to Art. 38 to limit the scope of the trader's fundamental rights. First, the Court highlighted "the necessity to consider Art. 38 of the Charter seeking to ensure a high level of consumer protection for consumers, including air passengers, in European Union policies",[13] and then ruled that "the importance of the objective of consumer protection, including the protection of air passengers, may justify even substantial negative economic consequences for certain economic operators". This approach was then confirmed in another decision (case C-28/20 Airhelp) where the Court ruled that "freedom to conduct a business and the right to property are not absolute rights and (…) that they must be reconciled with Art. 38 of the Charter which, like Art. 169 TFEU, seeks to ensure a high level of protection for consumers, including air passengers, in EU policies".[14]

Also at national level, courts have considered the application of Art. 38 of the Charter. One case in Czech Republic dealt with the situation of an individual who had concluded an online contract with a company for the proofreading of a thesis. The person was not satisfied with the final result and therefore withdrew from the contract without paying the agreed fee. The company filed a complaint against the individual and the district court ruled in favour of the company. As the sum at stake was low, the judgment was not subject to appeal. The individual filed a complaint before the Constitutional Court invoking the right to consumer protection based on Art. 38 of the Charter. The constitutional Court ruled that the district court should have – in the light of Art. 38 of the Charter - applied those provisions of the Czech Civil Code relating to the protection of consumers and consequently upheld the plaintiff's right to consumer protection and overturned the first judgement of the district court.[15] In Slovakia, a regional court used (inter alia) Art. 38 to declare unlawful a contractual clause imposing a penalty fee on a consumer. As the court highlighted:

> "The contractual penalty was not individually agreed on, it is a standard contract that creates major disproportion in rights and obligation of contractual parties, disadvantaging customer, it is in conflict with the protection of customer rights, in conflict with the Charter of Fundamental Rights of the European Union (art 38), according to which to fulfil one of the fundamental rights of the European Union, state policies shall ensure high standard of customer protection, and thus it is possible to use all effective means to protect consumers to increase the trust of the consumers into the market that should not burden consumers with unreasonable practices".[16]

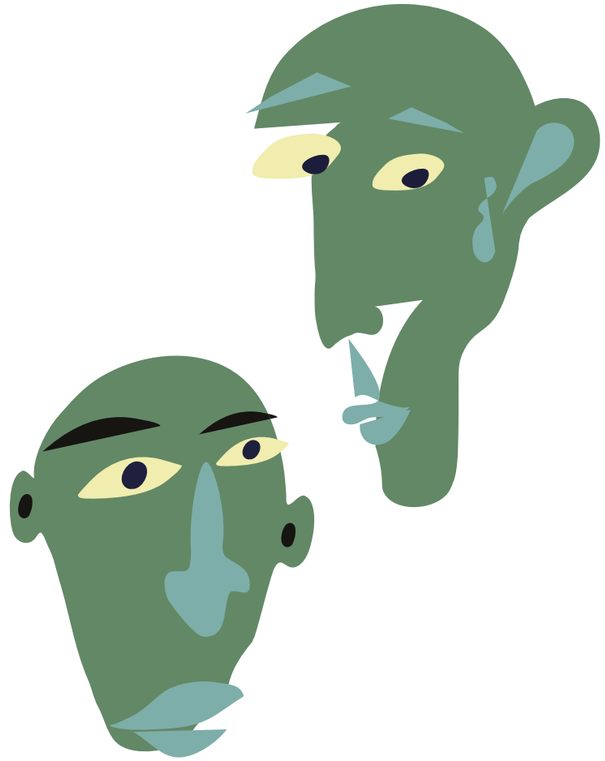
Art. 38 has yet to develop its potential through case law and doctrinal analysis, but its added value already seems promising.

A potential to unlock

Art. 38 recognizes the importance of consumer protection as a fundamental EU value. However, its operational effect remains paradoxical. First, Art. 38 was initially thought as a principle guiding EU policies. Yet in practice, its normative impact seems to be often limited. Second, Art. 38 was initially not conceived as giving subjective rights and yet experience tends to show that Art. 38 has been invoked to defend consumer interests.

Ultimately, the principle of consumer protection in Art. 38 may be used in conjunction with other substantive rights,such as Art. 47 (on remedies) or Art. 8 (on data protection) . One of the key upcoming challenges will be to progressively build a new understanding of EU consumer protection policy and Art. 38, by taking into account other key fundamental rights protected by the Charter, such as the right of non-discrimination (Art.21) (for instance important in the context of the development of artificial intelligence), rights of the child (Art. 24), of the elderly (Art. 25) and persons with disabilities (Art.26) (important for the protection of vulnerable consumers). These fundamental rights must be fully considered when regulating markets and help build a renewed and modern definition of consumer protection in the EU.

"One of the key upcoming challenges will be to progressively build a new understanding of EU consumer protection policy and Art. 38, by taking into account other key fundamental rights protected by the Charter."



Endnotes

Article 11

1 HRC 2018, p. 16 "Meaningful guarantees of non-discrimination require companies to transcend formalistic approaches that treat all protected characteristics as equally vulnerable to abuse, harassment and other forms of censorship." Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression recognises here that abuse and harassment, thorough their silencing effect constitute a form of censorship.

Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, HRC/38/35, 6 April 2018 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement> (retrieved on 20-02-2023)

Human Rights Council, Guiding Principles on Business and Human Rights, 2011, <https://unglobalcompact.org/library/2> (retrieved on 20-02-2023)

2 Quintais et al.; 2022 p. 24 "it must be noted that an important element of Article 10 ECHR and Article 11 Charter is the principle of positive obligations. Under the right to freedom of expression, States not only have a negative obligation to "abstain" from interfering with free expression, but they also have a positive obligation to protect free expression, "even in the sphere of relations between individuals", including between an individual and a "private company"

Quintais, João Pedro and Appelman, Naomi and Fahy, Ronan, Using Terms and Conditions to Apply Fundamental Rights to Content Moderation (November 25, 2022). German Law Journal (Forthcoming), <https://ssrn.com/abstract=4286147> (retrieved on 20-02-2023)

3 Frosio, Husovec; 2020 p. 15 "As a result of the liability safe harbours, the providers are partially freed from responsibility for their users' content. Thus, they effectively have power to decide about the content which users post. However, this power is not supplement by a responsibility towards their users to respect their speech rights in some particular form. This has famously led Tushnet to call it 'power without responsibility'."

Frosio, Giancarlo and Husovec, Martin, Accountability and Responsibility of Online Intermediaries (September 10, 2019). in Giancarlo Frosio (ed.), The Oxford Handbook of Online Intermediary Liability (Oxford University Press, 2020), Available at SSRN: <https://ssrn.com/abstract=3451220> (retrieved on 20-02-2023)

4 Quintais et al.; 2022 p. 26 "Article 20(4) seems to imply that users can complain directly to the platform about the way in which their fundamental rights have been considered in a platforms' content moderation decision. This would mean the platform does not only need to review whether the conduct or content was illegal or in violation of their T&Cs, but also review its own enforcement and application process and whether the user's fundamental rights have been weighed appropriately."

5 Business Insider, 2018; according to Jimmy Wales, co-founder of Wikipedia "One of my biggest concerns with the mandated upload filters is it would just be entrenching the power of Google and Facebook who already have the technical capacity to do this sort of thing, and smaller players, start-ups, all the other platforms people are using, are gonna be a bit shut out,"

Hamilton Asher, Isobel, Wikipedia is blacked out across Europe in protest against laws that could change the internet forever (July 5 2022) Business Insider < https://www.businessinsider.com/wikipedia-is-protesting-new-eu-copyright-laws-with-a-blackout-2018-7>(retrieved on 20-02-2023)

6 As described in a documentary "The Cleaners" (by Hans Block and Moritz Riesewiec, 2018)

7 Politico, 2022 "The German government in the past weeks repeatedly slammed the bill as an attack on privacy and fundamental rights, with its digital minister Volker Wissing warning this week that the draft law "crosses a line."

Goujard, Clothilde and Westendarp, Louis, Germany forces EU into damage control over encryption fears (June 10 2022) Politico <https://www.politico.eu/article/germany-eu-damage-control-encryption-abuse-online/> (retrieved on 20-02-2023)

8 Frosio, Husovec, 2020, p. 6 "payment blockades crippled Wikileaks of 95% of its revenues, when PayPal, Moneybookers, Visa and MasterCard stopped accepting public donations. No legal proceeding was ever actually initiated against Wikileaks."

9 Ó Fathaigh, Voorhoof: 2022, p. 13 "The wholesale blocking of broadcasting, distribution and access, as implemented against RT France, indeed has the practical effect of extending the scope of the ban far beyond the allegedly unlawful content which is targeted. It is hard to maintain that the ban, with its far-reaching impact, constituted the least intrusive measure available from the perspective of the right to freedom of expression under Article 10 ECHR."

Ó Fathaigh, Ronan and Voorhoof, Dirk, Freedom of Expression and the EU's Ban on Russia Today: A Dangerous Rubicon Crossed (December 2022). Communications Law, 2022, Volume 27, Issue 4, pp. 186-193, Available at SSRN: https://ssrn.com/abstract=4322452 (retrieved on 20-02-2023)

Article 18

1 Article 18, Right to asylum, The Charter of Fundamental Rights of the European Union [2008] 2000/C 364/01: 'The right to asylum shall be guaranteed with due respect for the rules of the Geneva Convention of 28 July 1951 and the Protocol of 31 January 1967 relating to the status of refugees and in accordance with the Treaty on European Union and the Treaty on the Functioning of the European Union (hereinafter referred to as "the Treaties")'.

2 Article 19, the Charter, Protection in the event of removal, expulsion or extradition: "1. Collective expulsions are prohibited. 2. No one may be removed, expelled or extradited to a State where there is a serious risk that he or she would be subjected to the death penalty, torture or other inhuman or degrading treatment or punishment."

3 An example of initiative is MyAidbyFAR that aims to help individuals make informed decisions about them migration procedures and assist members of the civil society in providing them with information. It was presented during a conference on Friday 17 of March, 2023 at the Vrij Universiteit Amsterdam, https://vu.nl/en/events/2023/legal-technology-a-stance-for-social-justice, accessed 3 April 2023.

4 LeaveNoOneBehindProject link the phone location of people with a picture to provide proof of their presence in the EU.Mathias Monroy, LeaveNoOneBehind project: An app for the right to asylum (digit.site36, 17 October 2022), https://digit.site36.net/2022/10/17/sea-watch-an-app-for-the-right-to-asylum/, accessed 3 April 2023.

5 Article 7, the Charter: Respect for Private and Family Life.

6 Article 52, the Charter: Scope of Guaranteed Rights.

7 Case C-291/12, Michael Schwarz v Stadt Bochum [2013] CJEU, EU:C:2013:670.

8 Schwarz, para 43.

9 Schwarz, paras 36-37.

10 Joined Cases C-148/13 to C-150/13, A, B, C v. Staatssecretaris van Veiligheid en Justitie [2014] Opinion of Advocate General Sharpston, EU:C:2014:2111.

11 Joined Cases C-148/13 to C-150/13, A, B, C v. Staatssecretaris van Veiligheid en Justitie [2014] CJEU, EU:C:2014:2406.

12 Junk science, according to the Oxford dictionary, is 'used to refer to ideas and theories that seem to be well researched and scientific but in fact have little evidence to support them', first read in the context of this blog post: Nuno Ferreira and Denise Venturi, Tell me what you see and I'll tell you if you're gay: Analysing the Advocate General's Opinion in Case C-473/16, F v Bevándorlási és Állampolgársági Hivatal (eumigrationlawblog.eu, 24 November 2017), https://eumigrationlawblog.eu/tell-me-what-you-see-and-ill-tell-you-if-youre-gay-analysing-the-advocate-generals-opinion-in-case-c-47316-f-v-bevandorlasi-es-allampolgarsagi-hivatal/, accessed 03 April 2023.

13 Case C-473/16, F v Bevándorlási és Állampolgársági Hivatal [2018] CJEU, EU:C:2018:36, para 58.

14 Case C-473/16, F v Bevándorlási és Állampolgársági Hivatal [2018] CJEU, EU:C:2018:36, para 53.

15 Ozkul, D. 2023, Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe, Oxford: Refugee Studies Centre, University of Oxford pp. 50-53. EU deportations organized on the basis of social media profiles (Statewatch, 13 February 2023), https://www.statewatch.org/news/2023/february/eu-deportations-organized-on-the-basis-of-social-media-profiles/, accessed 03 April 2023.

16 Dr. Francesca Palmiotto and Dr. Derya Ozkul, 'Like Handing My Whole Life Over': The German Federal Administrative Court's Landmark Ruling on Mobile Phone Data Extraction in Asylum Procedures (Verfassungsblog, 28 February 2023), https://verfassungsblog.de/like-handing-my-whole-life-over/, accessed 03 April 2023.

17 Nuno Ferreira and Denise Venturi, Tell me what you see and I'll tell you if you're gay: Analysing the Advocate General's Opinion in Case C-473/16, F v Bevándorlási és Állampolgársági Hivatal (eumigrationlawblog.eu, 24 November 2017), https://eumigrationlawblog.eu/tell-me-what-you-see-and-ill-tell-you-if-youre-gay-analysing-the-advocate-generals-opinion-in-case-c-47316-f-v-bevandorlasi-es-allampolgarsagi-hivatal/, accessed 03 April 2023.

18 Joint statement: The EU Artificial Intelligence Act must protect people on the move (Statewatch, 06 December 2022), https://www.statewatch.org/news/2022/december/joint-statement-the-eu-artifical-intelligence-act-must-protect-people-on-the-move/, accessed 03 April 2023.

19 Niovi Vavoula, 'Databases for Non-EU Nationals and the Right to Private Life: Towards a System of Generalised Surveillance of Movement?' in Francesca Bignami (ed), EU Law in Populist Times: Crises and Prospects (Cambridge University Press 2020), 229.

20 New online map of the EU's 'interoperable' immigration and policing databases (Statewatch, 09 November 2022), https://www.statewatch.org/news/2022/november/new-online-map-of-the-eu-s-interoperable-immigration-and-policing-databases, accessed 04 April 2023.

21 Article 8, the Charter: Protection of personal data.

22 Amended proposal for a regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of biometric data for the effective application of Regulation (EU) XXX/XXX [Regulation on Asylum and Migration Management] and of Regulation (EU) XXX/XXX [Resettlement Regulation], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulations (EU) 2018/1240 and (EU) 2019/818 [2020] COM/2020/614 final.

23 Case C-503/03, Commission of the European Communities v. Kingdom of Spain [2006] CJEU EU:C:2006:74.

24 Article 47, the Charter: Right to an effective remedy and to a fair trial.

25 Joined Cases C-225/19 and C-226/19, R.N.N.S. and K.A. v Minister van Buitenlandse Zaken [2020] CJEU EU:C:2020:951.

26 Norris, C., de Hert, P., L'Hoiry, X., & Galleta, A. (Eds.) (2017). The unaccountable state of surveillance: Exercising access rights in Europe. (Law, Governance and Technology Series; Vol. 34). Springer International.

27 Hungarian Helsinki Committee, The Right to Know – Comparative Report on Access to Classified Data in National Security Immigration Cases in Cyprus, Hungary and Poland (September 13, 2021) https://helsinki.hu/en/comparative-report-on-access-to-classified-data-in-national-security-immigration-cases/ accessed 03 April 2023.

28 Case C-362/14, Maximillian Schrems v Data Protection Commissioner [2015] CJEU EU:C:2015:650.

29 Laura Dreschler (2021)Wanted: LED adequacy decisions: How the absence of any LED adequacy decision is hurting the protection of fundamental rights in a law enforcement context, International Data Privacy Law, 11(2), 182-195.

30 Due to the increase in data stored and exchanged in the European information systems on migration and asylum.

31 Jane Kilpatrick, Chris Jones (2022) Empowering the police, removing protections: the new Europol Regulation, Statewatch, https://www.statewatch.org/publications/reports-and-books/empowering-the-police-removing-protections-the-new-europol-regulation/, accessed 03 April 2023.

32 Luděk Stavinoha, Apostolis Fotiadis and Giacomo Zandonini, EU's Frontex Tripped in Its Plan for 'Intrusive' Surveillance of Migrants, (Balkan Insight, July 7, 2022), https://balkaninsight.com/2022/07/07/eus-frontex-tripped-in-plan-for-intrusive-surveillance-of-migrants/, accessed 03 April 2023.

33 Formal comments of the EDPS on the Proposal for a Regulation on the European Border and Coast Guard (30 November 2018, EDPS), https://edps.europa.eu/data-protection/our-work/publications/comments/formal-comments-edps-proposal-regulation-european_de, accessed 03 April 2023.

34 Wojciech Wiewiórowski Privacy and data protection too often suspended at EU borders (27 January 2023, Euractiv), https://www.euractiv.com/section/data-privacy/opinion/it-is-time-to-tear-down-this-wall/, accessed 03 April 2023.

35 Teresa Quintel, Managing Migration Flows by processing Personal Data within the adequate Data Protection Instrument: Scoping Exercise between general and law enforcement Data Protection Rules applicable to Third Country Nationals, Upsala Universiteit and Université du Luxembourg, Doctoral Thesis 2021. p. 290. http://uu.diva-portal.org/smash/record.jsf?pid=diva2%3A1569545&dswid=135, accessed 03 April 2023.

36 Petra Molnar, Technological Testing Grounds: Border tech is experimenting with people's lives (9 November 2019, EDRI and the refugee law lab), https://edri.org/our-work/technological-testing-grounds-border-tech-is-experimenting-with-peoples-lives/, accessed 03 April 2023.

37 Fundamental Rights Agency (2022) Establishing national independent mechanisms to monitor fundamental rights compliance at EU external borders, https://fra.europa.eu/en/publication/2022/border-rights-monitoring, accessed 03 April 2023.

Article 20

1 Frantz Fanon, Black Skin, White Masks (Grove Press 2008 [1952]) 90.

2 A fuller account of her experiences can be found in her TEDxBeaconStreet Talk: Joy Buolamwini, Code4Rights, Code4All (2016).

3 Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', Proceedings of Machine Learning Research 81 (2018) 77-91.

4 Simone Browne, Dark Matters. On the Surveillance of Blackness (Duke University Press 2015) 8.

5 For overviews and examples, besides the works cited in the other footnotes see e.g. Cathy O'Neil, Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy (Crown 2016); Virginia Eubanks, Automating Inequality: How High-tech Tools Profile, Police, and Punish the Poor (St. Martin's Press 2018); Catherine D'Ignazio and Lauren F. Klein, Data Feminism (MIT Press 2020); Jens T. Theilen and others, 'Feminist Data Protection: An Introduction', Internet Policy Review 10 (2021) doi:10.14763/2021.4.1609.

6 For discussion of this in the context of digital technologies, see

Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism (Oxford University Press 2019) 239; Tendayi E. Achiume, Racial discrimination and emerging digital technologies: a human rights analysis (2020), UN Doc. A/HRC/44/57.

7 See Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the new Frontier of Power (Public Affairs 2019).

8 E.g. ECJ, Case C-414/16 – Egenberger, para 76.

9 For a critique of the 'current dominant single-axis framework within EU equality law' as well as possible ways forward, see Nozizwe Dube, 'Not Just Another Islamic Headscarf Case', European Law Blog, 19 January 2023.

10 For an overview of debates on intersectionality, see Patricia Hill Collins and Sirma Bilge, Intersectionality (2. edn, Polity 2020), especially at 127-138 on social media and digital violence; in the context of anti-discrimination law, see Kimberlé Crenshaw, 'Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics', University of Chicago Legal Forum (1989) 139; Shreya Atrey, Intersectional Discrimination (Oxford University Press 2019); Anna Lauren Hoffmann, 'Where Fairness Fails: Data, Algorithms, and the Limits of Antidiscrimination Discourse', Communication & Society 22 (2019) 900.

11 Safiya Umoja Noble, Algorithms of Oppression. How Search Engines Reinforce Racism (New York University Press 2018).

12 Center for Intersectional Justice, Intersectional Discrimination in Europe: Relevance, Challenges and Ways Forward (2019), at 20; a step in the right direction is provided by the European Parliament, Resolution of 6 July 2022 on intersectional discrimination in the European Union (P9_TA(2022)0289).

13 Aisha P.L. Kadiri, 'Data and Afrofuturism: An Emancipated Subject?', Internet Policy Review 10(4) (2021) doi:10.14763/2021.4.1597.

14 Os Keyes, 'The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition', Proceedings of the ACM on Human-Computer Interaction 2 (2018) 88; Foad Hamidi, Morgan Klaus Scheuerman and Stacy M. Branham, 'Gender Recognition or Gender Reductionism? The Social Implications of Automatic Gender Recognition Systems', CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems 1 (2018) 8.

15 See also Morgan Klaus Scheuerman, Madeleine Pape and Alex Hanna, 'Auto-essentialization: Gender in Automated Facial Analysis as Extended Colonial Project', Big Data & Society 8(2) (2021) doi:10.1177/20539517211053712.

16 Mar Hicks, 'Sexism is a Feature, Not a Bug' in Thomas S. Mullaney and others (eds), Your Computer is on Fire (MIT Press 2021); see also their chapter 'When Did the Fire Start?' in the same volume.

17 Ruha Benjamin, Race After Technology. Abolitionist Tools for the New Jim Code (Polity 2019) 44.

18 P. Khalil Saucier and Tryon P. Woods, 'Ex Aqua: The Mediterranean Basin, Africans on the Move and the Politics of Policing', Theoria 61 (2014) 55-75.

19 Dean Spade, 'Intersectional Resistance and Law Reform', Signs 38 (2013) 1031-1055.

20 bell hooks, 'The Oppositional Gaze. Black Female Spectators', Black Looks: Race and Representation (South End Press 1992) 116.

21 Marika Cifor et al., Feminist Data Manifest-No (2019), principle 21.

Article 21

1 Influential works include Safiya Umoja Noble, Algorithms of oppression: How search engines reinforce racism (New York University Press 2018); Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', Conference on Fairness, Accountability, and Transparency, Proceedings of Machine Learning Research 81 (2018) 77-91; Ruha Benjamin, Race after technology: Abolitionist tools for the new Jim code (Oxford University Press 2020).

2 C-617/10 Åklagaren v Hans Åkerberg Fransson EU:C:2013:105, para. 26.

3 The scope of protection is uneven across protected grounds: the area of work is for instance covered across the entire spectrum, whereas access to goods and services is only covered in relation to gender and race equality.

4 C-414/16 Vera Egenberger v Evangelisches Werk für Diakonie und Entwicklung e.V. EU:C:2018:257, para. 81.

5 Ibid, paras. 76-79.

6 See e.g. C-406/15 Petya Milkova v Izpalnitelen direktor na Agentsiata za privatizatsia i sledprivatizatsionen kontrol EU:C:2017:198 and C-528/13 Geoffrey Léger v Ministre des Affaires sociales, de la Santé et des Droits des femmes and Etablissement français du sang EU:C:2015:288.

7 See Claire Kilpatrick, 'Article 21: Non-Discrimination' in S. Peers, T. Hervey, J. Kenner and A. Ward, The EU Charter of Fundamental Rights. A Commentary (Hart Publishing, 2014); Emmanuelle Bribosia et al., 'Article 21: Non Discrimination' in F. Picod, S. van Drooghenbroeck and C. Rizcallah, Charte des droits fondamentaux de l'Union européenne: Commentaire article par article (Bruylant, 2017).

8 Regulation 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 2 119/1.

9 See J. Buolamwini and T. Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', Proceedings of Machine Learning Research 81 (2018) 77-91; and H. F. Menezes, A. S. C. Ferreira, E. T. Pereira and H. M. Gomes, 'Bias and Fairness in Face Detection', 34th SIBGRAPI Conference on Graphics, Patterns and Images (SIBGRAPI), 2021, pp. 247-254.

10 EU law only sets minimum requirements for the protection against discrimination and national law can grant more extensive protection as long as it remains compliant with the EU treaties. However, considerations of national law fall outside the scope of this essay.

11 Article 3(1)(g) of Directive 2000/43/EC.

12 C-414/16 Egenberger EU:C:2018:257.

13 See College voor de Rechten van de Mens, Judgment 2022-146 (7 December 2022) available at https://oordelen.mensenrechten.nl/oordeel/2022-146.

14 To do so, it relied on the CJEU's finding that an applicant can 'substantiate a prima facie case of discrimination by relying on general statistical data […] where the person concerned cannot be expected to produce more precise data regarding the relevant group of workers, such data being difficult to access or unavailable'. See C-274/18 Minoo Schuch-Ghannadan v Medizinische Universität Wien EU:C:2019:828, para. 56.

15 The Institute referred to the decision of the European Court of Human Rights in Basu v Germany App no 215/19 (ECtHR, 18 October 2022).

16 See Janneke Gerards and Frederik Borgesius, 'Protected Grounds and the System of Non-discrimination Law in the Context of Algorithmic Decision-making and Artificial Intelligence', Colorado Technology Law Journal 20(1) (2022):1-55 (2022).

17 See C-354/13 Fag og Arbejde (FOA) v Kommunernes Landsforening (KL) EU:C:2014:2463, paras. 36 and 39.

18 See Raphaële Xenidis, Beyond the 'Master's Tools': Putting Intersectionality to Work in European Non-Discrimination Law (2020) European University Institute.

19 Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', Conference on Fairness, Accountability, and Transparency, Proceedings of Machine Learning Research 81 (2018) 1–15.

20 C-443/15 David L. Parris v Trinity College Dublin and Others EU:C:2016:897.

21 Direct and indirect discrimination trigger the application of different justification regimes. As mentioned above, indirect discrimination can be justified upon satisfying the three criteria if the proportionality test. By contrast, derogations to direct discrimination are limited to a few exceptions explicitly foreseen in the EU Directives.

22 See Raphaële Xenidis, 'Algorithmic Neutrality vs Neutralising Discriminatory Algorithms: For a Paradigm Shift in EU Anti-Discrimination Law', Lavoro e Diritto 4 (2022) 765-771 and Raphaële Xenidis, 'When computers say no: Towards a legal response to algorithmic discrimination in Europe' in Bartosz Brożek, Olia Kanevskaia & Przemysław Pałka (eds.), Research Handbook on Law and Technology (Edward Elgar, forthcoming).

23 See Raphaële Xenidis, 'The Polysemy of Anti-discrimination Law: The Interpretation Architecture of the Framework Employment Directive at the Court of Justice', Common Market Law Review 58(6) (2021) 1649-1696.

24 A potential counter-argument for the defendant could be that the system aims to ensure fairness and merit in exams, which are key dimensions of the fundamental right to education protected in Article 14 of the Charter.

25 Difficulties also arise regarding the assessment of system providers' choice of adequate fairness metrics and interventions.

Article 7

1 Bits of freedom, We want more than "symbolic" gestures in response to discriminatory algorithms, 10 February 2021, https://edri.org/our-work/we-want-more-than-symbolic-gestures-in-response-to-discriminatory-algorithms/

2 BNNVARA, Veel meer kinderen van toeslagenschandaal-ouders uit huis geplaatst dan tot nu toe bekend was, 30 November 2022, https://www.bnnvara.nl/joop/artikelen/veel-meer-kinderen-van-toeslagenschandaal-ouders-uit-huis-geplaatst-dan-tot-nu-toe-bekend-was

3 Belastingdienst/Toeslagen, De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag, Onderzoeksrapport | z2018-22445, https://autoriteitpersoonsgegevens.nl/uploads/imported/onderzoek_belastingdienst_kinderopvangtoeslag.pdf

4 Amnesty International, Toeslagenschandaal is mensenrechtenschending, zegt Amnesty International, 25 October 2021, https://www.amnesty.nl/actueel/toeslagenaffaire-is-mensenrechtenschending-zegt-amnesty-international

5 Bits of freedom, De Belastingdienst laat internationaal goed zien hoe het dus niet moet, 28 October 2021, https://www.bitsoffreedom.nl/2021/10/28/de-belastindienst-laat-internationaal-goed-zien-hoe-het-dus-niet-moet/

6 Controlealtdelete, Etnisch en religieus geladen risicoprofielen bij Belastingdienst, https://controlealtdelete.nl/articles/etnisch-en-religieus-geladen-risicoprofielen-bij-belastingdienst

7 K.W. Crenshaw (2017), On Intersectionality: Essential Writings, The New York Press, https://scholarship.law.columbia.edu/books/255/

8 Rechtbank Den Haag, ECLI:NL:RBDHA:2020:865, https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBDHA:2020:1878

9 NOS, Ouders zwartgelakte dossiers: 'Ik weet nog steeds niet wat ik fout heb gedaan', 11 December 2019, https://nos.nl/artikel/2314288-ouders-zwartgelakte-dossiers-ik-weet-nog-steeds-niet-wat-ik-fout-heb-gedaan

10 deRechtspraak, Reflectie bestuursrechters rechtbanken op toeslagenaffaire gepubliceerd, Toeslagenaffaire: 'Belang rechtsbescherming individu moet zwaarder wegen dan vaste lijn jurisprudentie', 8 October 2021, https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Raad-voor-de-rechtspraak/Nieuws/Paginas/Toeslagenaffaire-Belang-rechtsbescherming-individu-moet-zwaarder-wegen-dan-vaste-lijn-jurisprudentie.aspx

Article 8

1 Joined Cases C203/15 and C698/15 Tele2 Sverige AB v Post- och telestyrelsen, para 129.

2 Case C131/12 Google Spain SL v AEPD.

3 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) [2016] OJ L 119.

4 Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119.

5 See, for example, supra 2, art 4(1) and 4(2).

6 Case C-73/07 Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, paras 36-37.

7 Case C434/16 Nowak v DPC, para 34.

8 Case C-582/14 Breyer v Bundesrepublik Deutschland, para 44.

9 See Case C291/12 Schwarz v Stadt Bochum, para 28.

10 Supra 1.

11 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201, art 1(3).

12 Supra 1, paras 67-81.

13 Case C623/17 Privacy International v SSFCA.

14 Ibid, paras 40-41.

15 See, inter alia, Joined Cases C92/09 and C93/09 Schecke v Land Hessen [2010] ECR I-11063.

16 See, for example, Joined Cases C293/12 and C594/12 Digital Rights Ireland v Minister for Communications, Marine and Natural Resources, para 36.

17 Christopher Docksey, 'Four fundamental rights: finding the balance' (2016) 6 International Data Privacy Law 195.

18 Supra 15, para 52

19 See FRA/ECtHR/EDPS, Handbook on European data protection law (Publications Office of the European Union, 2018) 20.

20 R (Bridges) v CCSWP [2019] EWHC 2341 (Admin).

21 Herke Kranenborg, 'Article 8' in Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds.), The EU Charter of Fundamental Rights: A Commentary (Hart 2021) 242.

22 Supra 16, paras 39-40.

23 Ibid, para 40.

24 Maja Brkan, 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning' (2019) German Law Journal 20 864, 878.

25 Case C73/16 Puškár v Finančné riaditeľstvo Slovenskej republiky, para 64.

26 Case C205/21 V.S., paras 125-128.

27 Joined Cases C511/18, C512/18 and C520/18 La Quadrature du Net v Premier minister, paras 136-137.

28 Supra 2, para 81.

29 Joined Cases C37/20 and C601/20 WM v Luxembourg Business Registers, paras 83-86.

Article 41

1 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOC_1988_180_R_0007_01&from=EN

2 https://curia.europa.eu/juris/document/document.jsf;jsessionid=1A4F9052F6441373B59362B8770E246D?text=&docid=130241&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1552373

3 https://curia.europa.eu/juris/document/document.jsf?text=&docid=234205&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1553564

4 Ibid

5 https://curia.europa.eu/juris/showPdf.jsf;jsessionid=7DA478E8C73B02CCE9126CEC38D3B3C8?text=&docid=97440&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=124762

6 https://curia.europa.eu/juris/document/document.jsf?text=&docid=110209&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=129508

7 https://verfassungsblog.de/frontex-and-algorithmic-discretion-part-i/

8 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32021R1152

9 https://raley.english.ucsb.edu/wp-content/Engl800/Pasquale-blackbox.pdf

10 https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf

11 https://scholarlypublications.universiteitleiden.nl/handle/1887/3439725

12 https://arxiv.org/pdf/1606.08813.pdf

13 S. Wachter, B. Mittelstadt, L. Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, International Data Privacy Law, 7(2):76–99, https://doi.org/10.1093/idpl/ipx005

14 https://curia.europa.eu/juris/showPdf.jsf?text=&docid=45418&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2109541

15 https://curia.europa.eu/juris/showPdf.jsf?text=&docid=99241&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=14505857

16 https://curia.europa.eu/juris/document/document.jsf?text=&docid=65303&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=14505723

17 https://www.cambridge.org/core/services/aop-cambridge-core/content/view/01B90DB4D042204EED7C4EEF6EEBE7EA/S2752613522000479a.pdf/reclaiming-transparency-contesting-the-logics-of-secrecy-within-the-ai-act.pdf

Article 47

1 Chisnall, M. (2020). Digital slavery, time for abolition?. Policy Studies, 41(5), 488-506.

2 See for instance: Regulation 2016/679/EU 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 [2016]

3 Van Dalen, S. Gilder, A. Hooydonk, E. Ponsen, E. (2016) System Risk Indication An Assessment of the Dutch Anti-Fraud System in the Context of Data Protection and Profiling https://pilpnjcm.nl/wp-content/uploads/2016/06/memorandum_1_-_system_risk_indication_an_assessment_of_the_dutch_anti-fraud_system_in_the_context_of_data_protection_and_profiling-1.pdf

4 Rachovitsa, A., & Johann, N. (2022). The human rights implications of the use of AI in the digital welfare state: Lessons learned from the Dutch SyRI case. Human Rights Law Review, 22(2), ngac010.

5 Ibid

6 SUWI Act, Art. 65(1).

7 Brief by the United Nations Special Rapporteur on extreme poverty and human rights as Amicus Curiae in the case of NJCM c.s./De Staat der Nederlanden (SyRI) before the District Court of the Hague (case number. C/09/550982/ HA ZA 18/388).

8 Ibid

9 Ibid

10 Lenaerts, K. (2012). Exploring the limits of the EU charter of fundamental rights. European Constitutional Law Review, 8(3), 375-403.

11 Ibid

12 Klamert, M. (2018). The implementation and application of the Charter of Fundamental Rights of the EU in Austria. Acta Universitatis Carolinae Iuridica, 64(4), 89-99.

13 Pech, Laurent, and Sébastien Platon. "Judicial independence under threat: the Court of Justice to the rescue in the ASJP case." Common Market L. Rev. 55 (2018): 1827.

14 Mulders, S. (2023). The relationship between the principle of effectiveness under Art. 47 CFR and the concept of damages under Art. 82 GDPR. International Data Privacy Law, 2023, Vol. 00, No. 0.

15 In Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, the Court declared the EU directive requiring Internet Service Providers (ISPs) invalid under Articles 7 and 8 CFR. In Tele2/Watson, the CJEU decided that national legislation enabling the indiscriminate retention of data from electronic devices for the purpose of fighting crime violates the rights enshrined in articles 7 and 8 CFR. Also, Google v. Spain in 2014 and the Schrems cases (2015 and 2020) dealt with issues related to having the right to have your data deleted from platforms and the rules regarding the sharing of personal data with third countries. See, Cameron, I. (2017). Balancing data protection and law enforcement needs: Tele2 Sverige and Watson. Common Market L. Rev., 54, 1467 and Voss, W. G. (2016). European union data privacy law reform: General data protection regulation, privacy shield, and the right to delisting. The Business Lawyer, 72(1), 221-234.

Article 34

1 UNGA, 'Report of the Special Rapporteur on Extreme Poverty and Human Rights', A/74/493, (October 11 2019).

2 Virginia Eubanks, 'Automating Inequality: How High Tech Tools Surveil, Profile and Punish the Poor', (St. Martin's Press, Inc., 2018)

3 Johns, F. (2019), From Planning to Prototypes: New Ways of Seeing Like a State. The Modern Law Review, 82: 833-863. https://doi.org/10.1111/1468-2230.12442

4 Scott JC, Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed (Yale University Press 1998)

5 Algorithm Watch and Bertelsmann Stiftung. 'Automating society report 2020.' (2020); Marta Choroszewicz and Beata Mäihäniemi, 'Developing a Digital Welfare State: Data Protection and the Use of Automated Decision-Making in the Public Sector across Six EU Countries', Global Perspectives 1(1) (2020) 12910.

6 Agneta Ranerup and Helle Zinner Henriksen, 'Digital Discretion: Unpacking Human and Technological Agency in Automated Decision Making in Sweden's Social Services', Social Science Computer Review 40(2) (2022) 445-461.

7 See Algorithm Watch (n2).

8 Naomi Appelman, Ronan Ó Fathaigh and Joris van Hoboken, 'Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands', Journal of Intellectual Property, Information Technology & E-Commerce Law 12(4) (2021) 257.

9 'The Algorithm Addiction' (Lighthouse Reports), https://www.lighthousereports.nl/investigation/the-algorithm-addiction.

10 See Choroszewicz (n2); Human Rights Watch, 'How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net: Questions and Answers', https://www.hrw.org/news/2021/11/10/how-eus-flawed-artificial-intelligence-regulation-endangers-social-safety-net.

11 Mike Ananny and Kate Crawford, 'Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability', New Media & Society 20 (2018) 973.

12 Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Why Fairness Cannot Be Automated: Bridging the Gap between EU Non-Discrimination Law and AI', Computer Law & Security Review 41 (2021) 105567.

13 'Austria's Employment Agency Rolls out Discriminatory Algorithm, Sees No Problem' (AlgorithmWatch), https://algorithmwatch.org/en/austrias-employment-agency-ams-rolls-out-discriminatory-algorithm/ (accessed 27 February 2023).

14 Ada Lovelace Institute, AI Now Institute and Open Government Partnership (2021), 'Algorithmic accountability for the public sector', https://www.opengovpartnership.org/wp-content/uploads/2021/08/algorithmic-accountability-public-sector.pdf

15 EU Fundamental Rights Agency, 'Getting the Future Right Artificial Intelligence and Fundamental Rights', (Publications Office of the European Union 2020), https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights.

16 Frans Pennings, 'Does the EU Charter of Fundamental Rights Have Added Value for Social Security?' European Journal of Social Security 24 (2022) 117.

17 Jaan Paju, 'The Charter and Social Security Rights: Time to Stand and Deliver?' (2022) 24 European Journal of Social Security 21. Ane Aranguiz, 'Bringing the EU up to Speed in the Protection of Living Standards through Fundamental Social Rights: Drawing Positive Lessons from the Experience of the Council of Europe' Maastricht Journal of European and Comparative Law 28 (2021) 601.

18 General Comment No 19: The right to social security, adopted on 23 November 2007, UN doc. E/C.12/GC/19.

Article 28

1 https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/98373/117044/F1671923749/IRL98373.pdf

2 https://www.tuc.org.uk/research-analysis/reports/section-tucs-first-victories

3 Indeed Article 11 (2) of the European Convention on Human Rights is highly conditional in this regard: "No restrictions shall be placed on the exercise of these rights other than such as are prescribed by law and are necessary in a democratic society in the interests of national security or public safety, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others."

4 https://www.legislation.gov.uk/ukpga/2022/32/contents/enacted

5 https://www.theguardian.com/business/2018/nov/22/gmb-union-drops-support-for-dpd-courier-walkout-after-legal-threat

6 https://www.elpuntavui.cat/societat/article/5-societat/2254689-l-acco-planteja-una-sancio-de-mes-de-122-000-euros-a-elite-taxi-per-boicotejar-uber.html

7 https://www.thetimes.co.uk/article/uber-gives-police-private-data-on-drivers-and-passengers-dm7l3gsxv

8 https://www.wired.co.uk/article/dominic-cummings-coronavirus-big-tech

9 https://files.mutualcdn.com/ituc/files/2022-ITUC-Rights-Index-Exec-Summ-EN.pdf

10 https://www.gmb.org.uk/news/uber-and-gmb-strike-historic-union-deal-70000-uk-drivers

11 https://www.gmb.org.uk/news/gmb-and-deliveroo-sign-historic-recognition-deal

12 In their submission to the European Parliament Committee for Employment and Social Affairs the government wrote: "the Riksdag is strongly opposed to more binding directives that destroy functioning labour market models. In recent years, the Riksdag has seen a number of initiatives from the European Commission that pose a direct threat to the Swedish labour market model, under which the social partners deal with matters through collective agreements. The Riksdag sees this very clearly in the current proposal for a directive, in particular in Article 4, where the presumption of an employment relationship invalidates the Swedish concept of an employee. The entire proposal is based on that presumption of an employment relationship and is, essentially, ill-conceived. Furthermore, there is a risk that the directive will have repercussions for both the tax system and the social insurance system, which is unacceptable. If the proposal for the directive is adopted, it will have far-reaching consequences for existing platform firms and for the entire gig economy. The proposal undermines the autonomy of the social partners and poses a threat to the Swedish labour market model. The Riksdag notes the strong concern of the referral bodies regarding the consequences of the proposal for the Swedish labour market model, in particular as regards Article 4 and its impact on the Swedish concept of an employee."

13 https://www.convert.com/eu-gdpr/recital-68-gdpr/

14 https://5b88ae42-7f11-4060-85ff-4724bbfed648.usrfiles.com/ugd/5b88ae_de414334d89844bea61deaaebedfbbfe.pdf

Article 37

1 Patrick Williams and Eric Kind (2019) Data-driven Policing: The hardwiring of discriminatory policing practices across Europe. Project Report. European Network Against Racism (ENAR); EDRi (2023). Decolonising digital rights. https://edri.org/what-we-do/decolonising-digital-rights/

2 Metcalfe, P., & Dencik, L. (2019). The politics of big borders: Data (in) justice and the governance of refugees. First Monday; Andreea Belu (2020). Surveillance on the seas: Europe's new Migration Pact. EDRi https://edri.org/news/surveillance-on-the-seas-europes-new-migration-pact/

3 European Union, 'Charter of Fundamental Rights of the European Union'. Official Journal of the European Union C326/391 http://data.europa.eu/eli/treaty/char_2012/oj.

4 Michelle Thorne, 'Funders Convening on Climate Justice and Digital Rights' (2022) <https://michellethorne.cc/2022/04/funders-convening-on-climate-justice-and-digital-rights/>

5 Fieke Jansen, 'Framing the climate crisis as a digital rights issue' (2022) Green Web Foundation <https://www.thegreenwebfoundation.org/news/framing-the-climate-crisis-as-a-digital-rights-issue/>

6 Michael Brennan, 'Intersections of Digital Rights and Environmental and Climate Justice' (2022) <https://www.fordfoundation.org/work/learning/learning-reflections/intersections-of-digital-rights-and-environmental-and-climate-justice/>

7 Becky Kazansky, Shayna Finnegan, & Maja Romano, 'Solidarity not solutionism: Wayfinding just paths for digital infrastructure that serves the planet' (2023) <https://www.apc.org/en/node/38497/>

8 Shayna Robinson, Remy Hellstern, & Mariana Dia, 'Sea Change: Prioritizing the Environment in Internet Architecture' (2022). For IAB workshop on Environmental Impact of Internet Applications and Systems 2022. <https://github.com/intarchboard/e-impact-workshop-public/blob/main/papers/Robinson_Sea-Change-Prioritizing-the-Environment-in-Internet-Architecture.pdf>

9 Robinson, et al, 'Sea Change'

10 Leslie Hook & Dave Lee, 'How tech went big on green energy' (2021) Financial Times. <https://www.ft.com/content/0c69d4a4-2626-418d-813c-7337b8d5110d>

11 Sebastian Moss, 'Los Lunas locals question Facebook's data center expansion, worry about water use' (2021) Data Center Dynmics. <https://www.datacenterdynamics.com/en/news/los-lunas-locals-question-facebooks-data-center-expansion-worry-about-water-use/>

12 Merijn Renger and Carola Houtekamer, 'Datacentra Zeewolde vragen twee keer zoveel stroom als Amsterdam' (2020) NRC. <https://www.nrc.nl/nieuws/2020/06/21/zeewolde-speelt-straks-champions-league-met-stroomverbruik-a4003548>

13 Merijn Renger & Carola Houtekamer, 'Gebroken beloftes: hoe de Wieringermeerpolder dichtslibde met windturbines en datacentra' (2020) NRC. <https://www.nrc.nl/nieuws/2020/06/05/gebroken-beloftes-hoe-de-wieringermeerpolder-dichtslibde-met-windturbines-en-datacentra-a4001882>

14 Renger et al. 'Gebroken beloftes'.

15 Moss, 'Los Lunas locals question'.

16 Association for Progressive Communication 'Extractivism, mining, and technology in the Global South: Towards a common agenda for action'. In: At the interstice of digital rights and environmental justice: Four issue briefs to inform funding (2022).

17 Niels ten Oever, 'Wired Norms: Inscription, resistance, and subversion in the governance of the Internet infrastructure' (2020) PhD thesis University of Amsterdam. <https://nielstenoever.net/wp-content/uploads/2020/09/WiredNorms-NielstenOever.pdf>

18 Association for Progressive Communication 'Extractivism, mining'

19 Thierry Breton, 'Critical Raw Materials Act: securing the new gas & oil at the heart of our economy I Blog of Commissioner Thierry Breton'. (2022) European Commission. <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_5523>

20 Internal Market, Industry, Entrepreneurship and SMEs, 'Critical raw materials. European Commission' (2023). <https://single-market-economy.ec.europa.eu/sectors/raw-materials/areas-specific-interest/critical-raw-materials_en>

21 European Commission, 'White Paper on Artificial Intelligence: a European approach to excellence and trust' (2020) 19.2.2020 COM(2020) 65 final.

22 European Union, 'Charter of Fundamental Rights'

23 Max Liboiron, 'Pollution is colonialism' (2021) Duke University Press.

24 Shanon Dosemagen, Emelia Williams, Katie Hoeberling & Evelin Heidel, 'Environmental justice, climate justice, and the space of digital rights' (2022) Open Environmental Data Project and Open Climate.

25 Association for Progressive Communication 'Extractivism, mining'

26 Fieke Jansen, 'Presenting new research climate justice x digital rights' (2022) Green Web Foundation. <https://www.thegreenwebfoundation.org/news/presenting-new-research-climate-justice-x-digital-rights/>

Article 38

1 Art.169 TFEU reads as follows "in order to promote the interests of consumers and to ensure a high level of consumer protection, the Union shall contribute to protecting the health, safety and economic interests of consumers, as well as to promoting their right to information, education and to organise themselves in order to safeguard their interests (...)".

2 Commission Communication on the Charter of Fundamental Rights of the European Union (Brussels, 13 September 2000) (see pt 22).

3 CHARTE 4422/00, CONVENT 45 of 28 July 2000.

4 e.g., amendment by Lord Goldsmith QC proposing to remove the article because 'it is so vague as to provide no sensible restriction on the Institutions or any assistance to individuals in informing them of their rights (...)".

5 e.g., amendment by Ieke van den Burg proposing to redraft the article as follows: "everyone has the right to be protected as a consumer against health and safety risks, and has the right to defend his/her interests individually and collectively".

6 I. Benöhr, EU consumer law and human rights, Oxford Studies in European Law, 2014, 272 p.

7 COM(2018) 184 final 2018/0089(COD), 11 April 2018.

8 COM(2018) 185 final 2018/0090 (COD), 11 April 2018

9 BEUC, Regulating AI to protect the consumer, BEUC-X-2021-088, 7 October 2021

10 I. Benöhr, EU consumer law and human rights, Oxford Studies in European Law, 2014, 272 p.

11 European Union Agency for Fundamental Rights, Ten years on: unlocking the Charter's full potential, 2020, p.14 (http://fra.europa.eu/en/publication/2020/ten-years-unlocking-charters-full-potential).

12 CJEU, case C-12/11 Mc Donagh v Ryanair, 31 January 2013, ECLI:EU:C:2013:43.

13 supra note 8, pt.63

14 CJEU, Case C-28/20 Airhelp, 23 March 2021, ECLI:EU:C:2021:226

15 Czechia / Constitutional Court / II. ÚS 78/19 (http://fra.europa.eu/en/caselaw-reference/czechia-constitutional-court-ii-us-7819).

16 Slovakia / Regional Court Prešov / 10Co/51/2017 (http://fra.europa.eu/en/caselaw-reference/slovakia-regional-court-presov-10co512017#deeplink2).

17 I. Benöhr, EU consumer law and human rights, Oxford Studies in European Law, 2014, 272 p.

Credits

Editor

Alexandra Giannopoulou

with the contribution of Nikita Kekana and César Manso-Sayao

Authors

Anna Mazgal, *Wikimedia Europe*

Alexandre Biard, *BEUC - The European Consumer Organisation*

Divij Joshi, *University College London*

Fieke Jansen, *Critical Infrastructure Lab, University of Amsterdam/Green Screen coalition Climate Justice and Digital Rights*

Giulia Gentile, *LSE Law School*

Ioannis Kouvakas, *Privacy International / Vrije Universiteit Brussels (VUB)*

James Farrar, *Worker Info Exchange*

Jens Theilen, *Helmut-Schmidt-University Hamburg*

Melanie Fink, *Leiden Law School*

Nadia Benaissa, *Bits of freedom*

Nawal Mustafa, *Public Interest Litigation Project (PILP)*

Romain Lanneau, *Statewatch*

Raphaële Xenidis, *SciencesPo Law School*

Art direction

DFF & Justina Leston

Visual identity

Nicole Snaiderman

Artwork of front and back cover

Nicole Snaiderman

Essay illustrations

Yorgos Konstantinou

Graphic design

Justina Leston

Communications

Barbara Okeyo

Ekaterina Balueva

Learn more about the digiRISE project here

Funded by the
European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the CERV Programme. Neither the European Union nor the granting authority can be held responsible for them.


DFF
Digital
Freedom Fund
digiRiSE