eLaw
Working Paper Series

No 202ť/0ŤŤ - ELAW– 202ť

Zq¤,Pusu¡mx,^us t¡

U y msuzuzs,mppu¡u{ zmx,r¢zpm y qz¡mx,~us t¡ ,r{~,¡ tq, pusu¡mx,q~m

O¢ ¡q~ ,N:T:Y:,

Universiteit Leiden
eLaw

Discover the world at Leiden University

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

New digital rights: Imagining additional fundamental rights for the digital era

*Bart Custers**

Prof.mr. dr. ir. B.H.M. Custers is a full professor of Law and Data Science at eLaw, the center for law and digital technologies at Leiden University, Leiden University, Steenschuur 25, 2311 ES Leiden, Netherlands

ARTICLE INFO

Keywords:
Digital rights
The right to be offline
The right to internet access
The right not to know
The right to change your mind
Value of personal data
Clean digital environment
Safe online environment

ABSTRACT

The increasing use of digital technologies by governments and companies raises numerous questions regarding the regulation of these technologies, particularly regarding the rights and legal protections citizens are entitled to. The focus is mostly on the application and potential modification of existing (fundamental) rights. However, the debate and legal research in this area lacks a broader discussion on which new rights citizens should have in the digital era. Only now and then new concepts surface, such as the 'right to be forgotten'. This article deals with the question which new, additional rights could be imagined in the digital era if we were to draft them right now, from scratch, rather than being tied to a set of existing fundamental rights. In order to start a broader legal debate on this, various new rights for citizens in the digital area are proposed.

1. Introduction[1]

Law and digital technology, also referred to as IT law, is a functional area of law that has gotten a firm foothold between other legal disciplines over the past decades, both in legal practices and academia. New technological developments such as big data, the Internet of Things, quantum computing, blockchain technology and sophisticated algorithms raise questions regarding the regulation of such technologies, for instance, with regard to which rights and protection citizens have or should have. In essence, legal issues related to the rights of citizens can be categorized into three types of issues:

1 Violations of rights resulting from (the use of) new technologies
2 Conflicting rights resulting from (the use of) new technologies
3 New issues resulting from (the use of) new technologies, for which no rights exist yet

The first and second category are familiar problems for lawyers. Typical examples in the first category are questions regarding the extent to which sophisticated data analytics interfere with someone's privacy, or the extent to which the use of risk profiling is potentially discriminatory against particu-

* Corresponding author: Bart Custers, Leiden University, Steenschuur 25, 2311 ES Leiden, Netherlands.
E-mail address: b.h.m.custers@law.leidenuniv.nl

[1] An earlier version of this article was published in Dutch, see Custers B.H.M. (2019), Nieuwe digitale (grond)rechten, *Nederlands Juristenblad* 94(44): 3288-3295.

https://doi.org/10.1016/j.clsr.2021.105636

lar groups of people.[2] Typical examples in the second category are questions regarding the extent to which someone may be wiretapped (privacy interest) for the purpose of criminal investigation (security interest) or the extent to which someone may insult a religion (freedom of religion versus freedom of speech). On all such questions large amounts of literature and case law are available.[3]

The third category, however, is much less discussed in literature, legal practice and academic debates. A typical example in the third category is the 'right to be forgotten', sometimes referred to as the 'right to oblivion',[4] that is since 2018 incorporated in Article 17 of the EU General Data Protection Regulation (GDPR), or a (theoretical, non-existing) 'right to anonymity'.[5]

The fact that there exists little attention for new concepts may be partially due to the fact that many legal issues in legal practice and legal research have a legal-dogmatic nature, focused on the question whether and how existing legislation applies to new technology. Typical examples are questions whether Bitcoins and other cryptocurrencies qualify as money as defined in legislation for the financial sector or questions whether e-mail is covered by constitutional secrecy of letters. In all these examples, the starting point tends to be existing legislation and any potential interpretations, which allows limited leeway for new concepts.

More leeway for new concepts and conceptualizations may exist when dealing with regulatory issues of a more normative and explorative nature, for instance, focused on questions regarding whether and how particular technologies may need to be regulated. Typically, in such instances, the potential threats of such new technologies, such as cryptocurrencies, artificial intelligence, or drones, are the starting point for any discussion on which types of regulation may perhaps be needed. Also, underlying moral norms and values that are at stake (and which may not or not entirely or explicitly be covered by the legal rules) then come to the foreground.[6] The aim then often is to, on the one hand, facilitate as much as possible technological innovation and its societal and economic benefits and, on the other hand, minimize and mitigate any disadvantageous effects or harmful side effects as much as possible.

Although such normative and explorative research allows room for considering new concepts, this rarely takes place, because existing regulatory frameworks are usually the starting point. This is in a way problematic because it can entail a distorted perspective, since many rights that citizens have, particularly fundamental rights that determine the bigger picture, were drafted in an era in which the world looked completely different. Hence, what is lacking in the current debate and in legal research is a broader discussion on which new (fundamental and other) rights citizens should have in the digital era. That raises the question which (fundamental and other) rights one would come up with if we would have to draft them starting on a clean slate, rather than being tied to a set of existing fundamental rights. In this article, hoping to broaden the focus of the current debate and to somewhat disconnect it from current frameworks and lines of thought, several new digital rights for citizens are proposed.

This article is structured as follows. Section 2 further discusses the three types of legal issues related to the rights of citizens that were set out above. The aim is to clearly locate the question of new rights within a more extended discussion of the regulatory landscape of digital technologies and explain why focusing on only existing regulatory frameworks may be constraining in this respect. Section 3 provides a catalog of potential new digital rights, by way of out of the box suggestions. Although this catalog obviously is not exhaustive, it includes suggestions like a right to be offline, a right to internet access, a right not to know, a right to change your mind, a right to (re)start with clean (digital) slate, a right to have expiration dates for data, the right to know the value of your data, the right to a clean digital environment, and the right to a safe online environment. It is not argued that we should have all these rights in all jurisdictions, they are simply suggestions put on the table for (re)starting a (broader) debate. Section 4 provides conclusions on how to further investigate (the need for) new digital rights, broadening the debate on this, and further implementation of any new digital rights.

2. Three types of issues

In order to clearly locate the question of new rights in the more extended discussion of the regulatory landscape of digital technologies, the three types of legal issues related to the rights resulting from (the use of) new technologies of citizens are further discussed in this section. By providing a discussion of literature and approaches in this area, the status of the current regulatory landscape is examined. Also, it is argued why focusing only on existing regulatory frameworks may be constraining in this respect.

2.1. *Violations of rights*

The first type of legal issues is that of violations of rights resulting from (the use of) new technologies. Digital technologies can violate several fundamental rights (which can sometimes be hard to determine). This is the category of issues in which only one single (fundamental) right has to be taken into account for each issue. Although this may perhaps seem easier than issues in which several competing fundamental rights are involved, this does not mean that the issues in this category are easy and straightforward. For instance, the scope of protection offered by a fundamental right may not be clear, making it hard to assess whether a right is violated. A typical example, for instance, is whether privacy can be violated

[2] Barocas, S., and Selbst, A.D. (2016) Big Data's Disparate Impact (2016). 104 *California Law Review* 671.

[3] For references, see the footnotes in Section 2.

[4] Xanthoulis, N. (2012) Conceptualizing a Right to Oblivion in the Digital World: A Human Rights-Based Approach, https://ssrn.com/abstract=2064503

[5] Prins, J. E. J. (2000). Privacy, consument en het recht op anonimiteit: een oud fenomeen in een nieuw jasje. In K. Stuurman, R. Westerdijk, & C. Sander (Eds.), *De E-Consument* (pp. 123-140). Den Haag: Elsevier.

[6] La Fors, K., Custers, B.H.M., and Keymolen, E. (2019) Reassessing values for emerging big data technologies: integrating design-based and application-based approaches, Ethics and Information Technology, Volume 21, Number 3, p. 209-226. https://doi.org/10.1007/s10676-019-09503-4

in public places. Also, fundamental rights can be violated in different degrees. If a particular technology violates a fundamental right (for instance, wiretapping interfering with privacy), such a violation, severe in itself, can be considered even more severe under specific circumstances (for instance, wiretapping communication between a doctor and her patient or between a criminal suspect and his lawyer). In fact, as will be discussed in the next subsection, some violations can even be legitimate (for instance, the police wiretapping a suspect under a court warrant).

Matching digital technologies and fundamental rights one-on-one can be done starting from the technologies or from the fundamental rights and both have been done in literature.[7] In the former approach, a specific technology is under scrutiny and it is assessed whether and how this may interfere with one or more fundamental rights in existing catalogues (such as the European Convention on Human Rights, the EU Charter of fundamental rights or a national constitution). In the latter approach, a specific human right is under scrutiny and it is assessed to what extent one or more new technologies may interfere with these rights. In both approaches, the focus can be on the extent to which existing provisions can be applied in the context of new technologies and the extent to which they actually protect citizens.

The right to privacy is probably the first fundamental right ever to be discussed in relation to information technologies[8] and it arguably also is the most often discussed human right in the light of digital technologies. However, in recent years other fundamental rights have also received increasing attention in literature, most notable the right to equal treatment (non-discrimination).[9] Almost all fundamental rights may to some extent be affected by technological developments. For instance, the emergence of the use of technology in courts may raise issues regarding the right to a fair trial,[10] the rise of predictions by algorithms and neuro-implants may affect freedom of thought,[11] and the increasing exploitation of data even causes some authors to discuss (data) slavery.[12]

New technologies can interfere with fundamental rights, but also with rights provided in secondary legislation. Most notable in this respect are the rights provided in data protection law, such as the EU General Data Protection Directive (GDPR), which contains an extensive list of data subject rights. Typical rights under pressure are the right to data portability,[13] the right to erasure[14] mentioned earlier, and the right not to be subjected to automated decisions.[15] Also, some rights not explicitly included in legislation are subject of debate, such as an alleged right to explanation.[16]

2.2. *Conflicting rights*

The second type of legal issues is that of conflicting rights resulting from (the use of) new technologies. This can be any combination of fundamental rights, but usually there are two conflicting rights that need to be balanced.[17] Sometimes cate-

[7] Examples starting with a particular technology include: Mantelero, A. (2018) AI and Big Data: A blueprint for a human rights, social and ethical impact assessment, *Computer Law & Security Review*, Volume 34, Issue 4, 2018, p. 754-772, https://doi.org/10.1016/j.clsr.2018.05.017; Hughes, K. (2017) Blockchain, The Greater Good, and Human and Civil Rights, *Metaphilosophy*, Vol 48, Nr. 5, p. 654-665; Custers, B.H.M. (2016) Drones here, there and everywhere, in: B. Custers (ed.) The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives, Springer; Davis, S.L.M., and Williams, C. (2020) Enter the Cyborgs: Health and Human Rights in the Digital Age, *Health and Human Rights Journal*, 22(2), p. 1-6. Examples starting with a particular human right include: Holtzman, D.H. (2006) Privacy Lost: How Technology is Endangering Your Privacy, Jossey-Bass; Wittkower, D.E. (2018) Technology and Discrimination, ODU Digital Commons, Old Dominion University, https://digitalcommons.odu.edu/cgi/viewcontent.cgi?article=1036&context=philosophy_fac_pubs; Watson, R.A. (1971) Human dignity and technology, The Philosophy Forum, 9:3-4, p. 211-241; Marrani, D., (2019) Right to fair trial. Impacts of new technology and contemporary space of justice on the process and administration of justice. Universitat Autonoma de Barcelona, https://www.tdx.cat/bitstream/handle/10803/669451/dama1de1.pdf?sequence=1&isAllowed=y.

[8] Warren, S.D., and Brandeis, L.D. (1890) The right to privacy; the implicit made explicit, *Harvard Law Review*, p. 193-220. The earlier technologies of the industrial revolution (such as the steam engine) and discussions on human dignity related to it are not considered to be information technologies.

[9] Barocas, S. & Selbst, A. (2016) Big Data's Disparate Impact, 104 *California Law Review*, 671. Custers, B.H.M., Calders, T., Schermer, B., and Zarsky, T. (eds.) (2013) Discrimination and Privacy in the Information Society, Springer.

[10] Allsop, J. (2019) Technology and the Future of the Courts, 38 *University of Queensland Law Journal* 1; Dymitruk, M. (2019) The right to a fair trial in automated civil proceedings, *Masaryk University Journal of Law and Technology*, Vol. 13, Nr. 1, p. 27-44; Ulenaers, J. (2020) The Impact of Artificial Intelligence on the Right to a Fair Trial: Towards a Robot Judge? *Asian Journal of Law and Economics*, *11*(2).

[11] McCarthy-Jones, S. (2019) The Autonomous Mind: The Right to Freedom of Thought in the Twenty-First Century, 2 *Frontiers in Artificial Intelligence* 19; Lavazza A (2018) Freedom of Thought and Mental Integrity: The Moral Requirements for Any Neural Prosthesis, 12 *Frontiers in Neuroscience* 82.

[12] Hildebrandt, M. (2013) Slaves to Big Data. Or Are We? 17 *IPD Revista de Internet, Derecho y Politica*, p. 7-44; Damanhouri, D. (2017) Data Slavery: You're Actually Selling Your Information For Free, *Medium.com*, 3 November 2017; Pirkowski, M. (2018) Data Slavery and Decentralized Emancipation: Facebook, Google and the Future of Data Ownership, *Medium.com*, 21 June 2018.

[13] Ursic, H. (2018) Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control, *SCRIPTed*, Vol. 15, Issue 1, August 2018. Swire, P., and Lagos, Y. (2013) Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique, 72 *Maryland Law Review* 335; Graef, I., Verschakelen, J., and Valcke, P. (2013) Putting the Right to Data Portability into a Competition Law Perspective, Journal of Higher School Economics Annual Review, 53, 63.

[14] Fosch-Villaronga E., Kieseberg P. & Li T. (2018) Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten, *Computer Law and Security Review* 34(2): 304-313.

[15] Sancho, D. (2020) Automated Decision-Making under Article 22 GDPR: Towards a More Substantial Regime for Solely Automated Decision-Making. In M. Ebers & S. Navas (Eds.), *Algorithms and Law*, p. 136-156. Cambridge: Cambridge University Press.

[16] Wachter, S., Mittelstadt, B., and Floridi. L. (2017) 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.

[17] Rosas, A. (2014) Balancing Fundamental Rights in EU Law. In: Cambridge Yearbook of European Legal Studies, 16, p. 347-360.

gories of competing rights are balanced, such as fundamental rights and economic rights.[18] Obviously, such balancing of two or more rights is not possible for *absolute* fundamental rights, i.e., rights that cannot be lawfully interfered with, no matter how important competing interests are. Typical examples of such absolute rights in the ECHR are the prohibition of torture, the prohibition of slavery and forced labor, and freedom of thought.

In contrast, *relative* fundamental rights (i.e., rights that can be legitimately interfered with in specific situations under particular circumstances) can be subject to such balancing in case of competing rights. Typical examples of such relative rights in the ECHR are the right to life (for instance, when absolutely necessary for defending a person from unlawful violence or when quelling an insurrection), the right to privacy (for instance, when necessary for public safety or national security), and freedom of expression (for instance, when this interferes with rights and freedoms of others, such as in the case of hate speech).

A typical example of a right that is often present in these balancing exercises is freedom of expression. A question that often pops up is to what extent freedom of expression is not interfering with the rights and freedoms of other, particularly when the content is insulting, threatening or hateful.[19] Typically, technologies like social media and deepfakes may contribute to freedom of expression, but can also facilitate fake news and hate speech. Another thorny issue is that of privacy versus security, discussing the extent to which law enforcement can interfere with private lives of citizens.[20] Typically, technologies like wiretapping, forensic DNA research, and camera surveillance can contribute to security, but may have a strong impact on privacy. Both academic literature and litigation flesh out all kinds of specific circumstances in the gray areas between these rights.[21] Depending on the specific nature and circumstances of a case, one right may be prioritized over another or vice versa. Similar to the previous category of issues, also when dealing with conflicting rights there can be significant legal uncertainty in how existing rights should be applied.

Many of the first and second type of legal issues are dealt with within the national and international legal frameworks for human rights. At an international level, the EU Charter for fundamental rights and the European Convention for Human Rights are the legal instruments to deal with this, supplemented by secondary legislation and case law, both at a national and international level. These points are still being resolved, but in this article, we will focus beyond this, to investigate whether more is needed to offer people sufficient protection in the digital era.

2.3. *A need for new rights*

The regulatory landscape of digital technologies focuses on addressing any undesirable aspects of such technologies and, to a lesser extent, on further facilitating innovation and technology development. However, both in the case of violations of rights and in the case of conflicting rights, there is significant legal uncertainty in how the existing (general) law applies. Also, there has been very little litigation to date on many of these issues. Technology often seems to develop faster than the body of case law. As a result of this legal uncertainty, the extent to which citizens are protected is not clear.

This raises the bigger question whether citizens are sufficiently protected by the rights provided by the current legal framework. Apart from the legal uncertainty, both categories of legal issues discussed above have in common that they take existing fundamental rights as the starting point. Most of these fundamental rights were drafted in an era in which the world looked completely different. For instance, the ECHR was ratified in 1950, before any computers, databases or the internet existed. Admittedly, most fundamental rights are drafted in general phrases, aligned with core ethical and societal values, rather than tailored to specific situations and circumstances. The advantage of these broad phrasings is that these rights provide room for interpretation and can easily be applied to very different situations in very different contexts. This aspect most certainly has helped most fundamental rights to stand the test of time and to remain fundamental.

However, this does not mean that the values underlying these fundamental rights have not changed over time. For instance, perceptions of the right to privacy have changed over the decades. With the rise of social media, people increasingly disclose information about themselves. This may be an indication that people attach less value to their privacy. Or perhaps they now have to make different types of decisions than a few decades ago, balancing privacy risks with fostering their online reputation. Research in this area is inconclusive: many people express concern about their privacy online, but do not act in ways that confirm to these concerns – the so-called privacy paradox.[22]

Another example can be found in non-discrimination law: the increased use of personalized pricing means that people can be selected on a plethora of characteristics beyond those that are traditionally considered sensitive and discriminatory. Some online food ordering and delivery platforms charge 50% higher prices for customers in wealthy neighborhoods.[23] Taxi platform Uber charges higher prices for customers whose phone batteries are almost empty.[24] Whereas in the past discrimination focused on characteristics like gender, ethnicity, religion and other sensitive characteristics, now also zip codes

[18] Vries, S.A. de (2013) Balancing Fundamental Rights with Economic Freedoms According to the European Court of Justice, *Utrecht Law Review*, 9(1), p.169–192.

[19] Massaro, T.M. (1991) Equality and Freedom of Expression: The Hate Speech Dilemma, 32 *William & Mary Law Review*, p. 211-265.

[20] Stalla-Bourdillon, S., Phillips, J., and Ryan, M.D. (2014) Privacy vs. Security. Springer.

[21] Cf. Teeuw, W.B., Vedder, A.H., et al. (2008) Security Applications for Converging Technologies. The Hague: WODC.

[22] Norberg, P.A., Horne, D.R., and Horne, D.A. (2007) The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors, *Journal of Consumer Affairs*, Vol. 41, No.1, p. 100-126.

[23] Maxwell, S. & Garbarino, E. (2010) The identification of social norms of price discrimination on the internet. *Journal of Product & Brand Management*, 19(3), p. 218-224.

[24] Dakers, M. (2016) Uber knows customers with dying batteries are more likely to accept surge pricing. *The Telegraph*, October 30, 2017.

and empty phone batteries can be criteria for in automated decision-making. While public opinions on and perceptions of this are being investigated, this raises the question whether current norms and values are still fully reflected in these fundamental rights. A case in point is the relatively new fundamental right to data protection incorporated in the EU Charter on fundamental rights. Before, a right to data protection was considered an aspect of the right to privacy. The elevation of personal data protection to the category of a stand-alone EU fundamental right is a strong signal of how important the legislator considers this right to be (and the values it is supposed to protect).[25]

Arguably, the gaps in the protection that existing fundamental rights offer citizens in the digital era may not be that large and the existing fundamental rights certainly are not redundant. Nevertheless, there may be situations in which additional fundamental rights may be needed. Focusing only on existing legal frameworks of fundamental rights can be constraining in this respect, as these frameworks, even though they perhaps indicate what is missing, may not fully reflect what is needed.

It may be argued that the best way to identify gaps in existing regulatory frameworks is to assess how they apply in practice. Although that makes sense, it is likely to result in further stretching interpretations of the existing legal framework. This is perhaps possible for some time, but after a while it may yield untenable distortions, drifting away from the original goals of the legal frameworks. This may result in legal frameworks that, apart from lacking legal elegance, may also increasingly lack legal certainty.

For these reasons (i.e., potential gaps in protection and shifting values over time), it may be useful to perform a thought experiment: 'which new, additional fundamental rights are necessary in the digital era?', as it sets aside for a moment the already existing (fundamental and other) rights that people have and freshly considers what may be needed rather than how we can apply what we already have. This is where the third category of legal issues comes in, i.e., new issues resulting from (the use of) new technologies, for which no rights exist yet.

Only a few concrete examples are available here, such as the EU (fundamental) right to data protection and, in the GDPR, newly introduced rights such as the right to be forgotten and the right to data portability.

3. New rights

The catalog of proposed rights in this section is intended as a list of out of the box suggestions, collected from, derived from or inspired by existing literature on this topic. Some suggestions have received significant attention in literature and in practice, but others have not been mentioned thus far or only briefly touched upon. The references provided for each new right roughly indicate the level of attention for it in existing literature. On this point, each source we were able to identify on this topic focuses on one new right only – we have not identified literature discussing two or more new rights in one source, in the way we do in this article. This section starts with a few disclaimers (Section 3.1), then puts forward several new digital rights (Section 3.2) and concludes with an overview (Section 3.3).

3.1. *Disclaimers*

Before discussing the suggestions for new digital rights, here are some disclaimers. Firstly, we would like to stress that we are not beforehand advocates of codifying each of these rights. We would like to put them on the table, but do not defend each of them piece by piece. We merely try to argue why considering and discussing them could make sense, which is not necessarily the same as accepting them. Obviously, each of these proposed rights entail various pros and cons. For each right, we bring in some discussion of the opposition and critiques, but we stress that further research will be needed to assess how desirable and viable each of these rights is.

Secondly, these rights are not elaborated in high levels of detail. A detailed elaboration would merit at least a separate journal article for each of these rights. Hence, no concrete phrasing for the suggested rights is proposed and neither is discussed whether these rights should be incorporated at the level of fundamental rights or elsewhere, in secondary legislation. Such suggestions may distract the focus from a more conceptual level to a legislative, legalistic or even political discussion. In order to have these discussions on the implementation, it is important to first determine what is needed, i.e., which direction we are heading for with this. Hence, the question whether, where and how these rights should be codified, should be subject of debate.

Thirdly, it is important not to perceive the catalog of suggestions provided here as exhaustive. It is explicitly intended as a first step. In fact, there does not exist any systematic methodology to create a complete list of rights that should be included in the debate.[26] However, we hope that the suggestions below incite others to add to this list more rights that they may find missing.

Fourthly, we stress that by saying the rights below are 'new' rather than building on existing (fundamental) rights, this does not mean they all have never been mentioned before and certainly not that we invented all these rights ourselves. Here, 'new' means that these rights have not yet been incorporated in legislation widely in different jurisdictions or, in case non-digital equivalents exist for some rights, that they are new in the digital context. We neither want to claim novelty for these rights nor do we claim being the first to think of this. Rather, the novelty here is in providing a broader overview of the developments in this area.

[25] Note though that some have argued that the right to data protection enshrined in the Charter does not meet the criteria for fundamental rights and should be considered as an ordinary consumer right. See Sloot, B. van der (2017) Legal fundamentalism: is data protection really a fundamental right? in: R. Leenes, R. van Brakel, S. Gutwirth, P. de Hert (eds.) *Data Protection and Privacy: (In)visibilities and Infrastructures*. Heidelberg: Springer.

[26] Also note, for the same reason, that the list below has no specific order or prioritization.

3.2. *Proposed new rights*

3.2.1. *The right to be offline*

Since 2017, French employees have a new form of protection for their workspace: companies with fifty employees or more have to make agreements with their personnel regarding the hours at which they can be contacted by their employer.[27] Outside these hours, they cannot be contacted, not in person, nor by phone or e-mail. In other words, they have a right to be offline, at least from the work perspective. The French call this the right to disconnect (droit à la déconnexion).[28] Also in Italy the right to disconnect was introduced in labor law[29] and in Germany the employment ministry banned managers from contacting staff outside working hours.[30] In December 2020, also the European Parliament called for an EU-wide 'right to disconnect', at least partially framed within the perspective of the coronavirus pandemic, during which ever more people work from home.[31]

The discussion on the right to disconnect is increasing, but a more general right to be offline (including all aspects of life, rather than only a work context) has received less attention thus far. Although a right to disconnect or to be offline resembles a right to privacy (note the similarity with privacy as the 'right to be let alone',[32] this is essentially different. Such a right does not deal with the collecting and processing of personal data like the right to data protection, nor does it deal with observing various aspects of private and family life covered by the right to privacy.[33] For instance, the right to data protection focuses on personal data and would not be violated if people are completely anonymous when online. A right to privacy would not be violated if a person is communicating online via confidential channels. But even if personal data and private communications are completely secured, being online all the time can be strenuous. Expectations of others may also put pressure on this. A right to be offline focuses on the potential nuisance that always being online can cause and the freedom to choose whether to be online or offline.

Always being online (i.e., 24/7), particularly on social media, can be exhausting and problematic for people and the people around them. In this context, addiction or aspects of addiction are often mentioned,[34] although it is not entirely clear how to define internet addiction. For instance, this can be related to online gaming, pornography, shopping or gambling. Internet addiction therefore often coincides with other disorders. The 'Fear Of Missing Out' (FOMO) is a psychological phenomenon describing anxiety caused by a desire not wanting to miss out on anything, which can cause people to continuously stay online.[35] This can result in insomnia, concentration problems and fatigue.[36] Compulsive and excessive use of social media that is difficult to control can cause considerable problems with regard to well-being and health.[37] In some countries even bootcamps ('digital detox') exist for people addicted to social media.[38] These programs vary from boy scouts type of camps to military style rehab programs and are focused on improving communication and team spirit among participants. A right to be offline could be invoked by people as an escape from these kinds of pressure. A right to be offline would be a strong signal in setting standards and expectations, preventing addictions and helping people find better balances in life. Such a signal would also be directed at social media companies, underlining the importance of healthy, rather than addicted users, and the role these companies may have in taking responsibility in this. At the same time, there are indications that such rights may be hard to implement in current cultures.[39]

Also for people who do not use the internet in addicted, obsessive ways, the question is how to find a good balance between living online and offline, a line that is increasingly blurred. Internet addiction may be at one extreme end of the spectrum, a life completely without internet (sometimes referred to as 'off the grid', referring to autarkic societies not connected to the power grid), may be at the other extreme end of the spectrum. Internet addiction may not be anyone's choice, but a life completely without internet access also may not be realistic in our society. If people have limited internet access (which is discussed next), this is usually related to the known drivers of the digital divide, such as the costs involved

[27] Migliorato, L. (2017) Culturing Boundaries: The Right to be Offline, *The Technosceptic*, 22nd March 2017. https://thetechnoskeptic.com/culturing-boundaries/

[28] Article 55 under Chapter II "Adapting the Labour Law to the Digital Age" (*Adaptation du droit du travail à l'ère du numérique*) included a provision to amend the French Labour Code to include the right to disconnect (*le droit de la déconnexion*).

[29] Article 19.1 of Senate Act n0 2233-B.

[30] Vasagar, J. (2013) Out of office working banned by German labour ministry, *The Telegraph*, 30 August 2013.

[31] https://www.europarl.europa.eu/news/en/press-room/20201126IPR92512/meps-call-for-an-eu-wide-right-to-disconnect.

[32] Warren, S.D., and Brandeis, L.D. (1890) The right to privacy; the implicit made explicit, *Harvard Law Review*, p. 193-220. See also Custers B.H.M. & Ursic H. (2018) Worker Privacy in a Digitalized World under European Law, *Comparative Labor Law & Policy Journal* 39(2): 323-344.

[33] Cf. Article 8 of the European Convention on Human Rights.

[34] Tsitsika, A., Janikian, M., Schoenmakers, T. M., Tzavela, E. C., Olafsson, K., Wo´jcik, S., . . . Richardson, C. (2014). Internet addictive behavior in adolescence: A cross-sectional study in seven European countries. *CyberPsychology, Behavior, and Social Networking*, 17, 528–535; Blackwell, D., Leaman, C., Tramposch, R., Osborne, C., Liss, M. (2017) Extraversion, neuroticism, attachment style and fear of missing out as predictors of social media use and addiction, Personality and Individual Differences, Vol. 116, p. 69-72.

[35] Alt, D., Boniel-Nissim, M. (2018) Parent–Adolescent Communication and Problematic Internet Use: The Mediating Role of Fear of Missing Out (FoMO), *Journal of Family Issues*. 39 (13): 3391–3409.

[36] Przybylski, A.K., Murayama, K., DeHaan, C.R., Gladwell, V. (2013) Motivational, emotional, and behavioral correlates of fear of missing out. Computers in Human Behavior. 29 (4): 1841–1848.

[37] Valkenburg, P. (2014) *Schermgaande jeugd*, Prometheus/Bert Bakker.

[38] Rudd, M. (2019) Parents are spending $5,000 to send their children to digital detox bootcamps run by veterans, *Daily Mail Australia*, 2nd July 2019.

[39] For instance, the right to disconnect in France faced many obstacles deeply rooted in the current French work culture, see Pansu, L. (2018) Evaluation of 'Right to Disconnect' Legislation and Its Impact on Employee's Productivity, *International Journal of Management and Applied Research*, Vol. 5, No. 3, p. 99-119.

or the cognitive skills required. Solutions suggested for closing the digital divide usually focus on these drivers (i.e., removing cost barriers and improving digital skills), but the right to be offline could be relevant as the other side of closing the digital divide, as not everything always has to be done online.[40]

In other words, few people will voluntarily renounce the benefits the internet has to offer, but the question is how and to which extent the intrusive and ubiquitous internet (most notably the Internet of Things) can and perhaps should be pushed back. For instance, banks in many countries nowadays expect (as a default) that all clients use online banking and charge extra fees for those who cannot or will not use online banking. Tax authorities in many countries prefer online completion of tax return forms. Many shops are no longer brick-and-mortar shops in city centers, but have been replaced by online shops and this will likely increase over the next years. A right to be offline could address and fence off the pressure of a ubiquitous internet and the technologies related to it, for those who may need it.

3.2.2. *The right to internet access*

The other way around, it could also be argued that everyone should have a right to get online, i.e., a right to have internet access, which has been discussed extensively in literature.[41] Sometimes products and services are only offered online or are (much) more expensive if purchased offline. In such cases, citizens who have no or limited internet access can be disadvantaged. Particularly for government services this can be problematic. For instance, if tax authorities only allow online tax return forms, citizens are essentially required to have internet access. Also for private issues, such as applying for a job, internet access is more or less mandatory these days. For such reasons, the UN already in 2016 suggested in a resolution that there should be a fundamental right to internet access, although this resolution was non-binding and focused on condemning intentional disruption of internet access by governments, rather than guaranteeing internet access for everyone.[42] A right to internet access can contribute to freedom of speech and to closing the digital divide,[43] but at the same time it may be hard to qualify such access (as discussed below) and it may need to be balanced with other rights and competing interests such as privacy and intellectual property protection.[44]

In most developed countries, large percentages of the population have internet access, so this may not be a big issue.[45] However, it may be an issue for different groups in society[46] for different reasons.[47] Furthermore, the discussion regarding net neutrality shows that some are in favor of a layered internet, on which users who pay more can have faster or higher quality connections. Net neutrality is the principle that internet providers treat all data packages on the internet the same, regardless of user, content or equipment.[48] Many countries have codified this in their (telecommunications) legislation. As of 2015 this is harmonized via EU legislation.[49]

Each new generation of communication and network technology increases the amounts of data that can be transferred via the internet and the speed of these data transfers.[50] These developments can result in higher costs for users, who may need to purchase new versions and updates of technology and they may require higher levers of knowledges and skills of users regarding digital technologies.[51] If these increased costs or levels of knowledge and skills are barriers for particular groups of users to keep pace with these technological developments, this can result in social polarization and manipulation. If some groups have access to a (fast and functional) internet and others have not, this can lead social segregations (i.e., haves and have-nots). If some groups of people have difficulties to keep up with these technological developments, they can easily be manipulated, both in terms of content or information (e.g., filtering fake news) and in terms of communication channels (e.g., where to find relevant and reliable information).[52] A right to internet access could guarantee that

[40] Another critique on the right to disconnect is that this is not a free choice for people who are not connected (i.e., no dysconnectivity without connectivity) and therefore cannot be regarded separately from the right to internet access below. See Hesselberth, P. (2018) Discourses on dysconnectivity and the right to disconnect, *New Media & Society*, Vol. 20(5), p. 1994-2010.

[41] Mathiesen, K. (2012) "The Human Right to Internet Access: A Philosophical Defense", *The International Review of Information Ethics*. Edmonton, Canada, 18, pp. 9–22; Hartmann, I.A. (2013) A right to free internet? On internet access and social rights,13 *Journal of High Tech Law* 297; Skepys, B. (2012) Is There a Human Right to the Internet? *Journal of Politics and Law*, Vol. 5, No. 4, p. 15-29; Reglitz, M. (2019) The Human Right to Free Internet Access, *Journal of Applied Philosophy*, Vol. 37, No. 2, p. 314-331.

[42] UN Resolution A/HRC/32/L.20 of 27 June 2016, see https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement

[43] Warschauer, M. (2004) *Technology and social inclusion: Rethinking the digital divide*. Cambridge: MIT press.

[44] Tully, S. (2014) A Human Right to Access the Internet? Problems and Prospects, *Human Rights Law Review*, Vol. 14, Nr. 2, June 2014, p. 175–195.

[45] For instance, according to Eurostat, across the EU the share of households with internet access has risen to 90% in 2019 (from 64% in 2009). See https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals.

[46] For instance, for disable people, see Scholz, F. , Yalcin, B., & Priestley, M. (2017). Internet access for disabled people: Understanding socio-relational factors in Europe. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 11(1), article 4.

[47] Van Deursen, A. J., & Van Dijk, J. A. (2014) The digital divide shifts to differences in usage. *New Media & Society*, 16, p. 507-526.

[48] Cf. Wu, T. (2003) Network neutrality, broadband discrimination, *Journal on Telecommunications and High Tech Law*, Vol. 2, p. 141-176.

[49] Directive 1015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union.

[50] Schaller, R.R. (1997) Moore's Law: Past, Present and Future, *Spectrum*, IEEE, Volume 34, June 1997, pp. 52-59.

[51] Custers B.H.M. (2008) The Exclusivity of Ultrafast Communication Networks, *Journal of International Commercial Law and Technology* 3(4): 247-253.

[52] Vedder, A. (2005) Expert knowledge for non-experts: Inherent and contextual risks of misinformation. ICES, Journal of Information, *Communication and Ethics in Society* (2005) Volume 3, p. 113–119.

costs of technology and digital skills and knowledge are not insurmountable barriers. Some countries already introduced such a right. For instance, Finland made broadband internet a legal right in 2010, guaranteeing 1 Mbit/s connections for every citizen[53] (updated to 100 Mbit/s in 2015), and in France the constitutional council ruled in 2009 that internet access is a human right.[54] Other countries, like Greece[55] and Spain[56] created a duty of care for the government regarding internet access.

Building on a right to internet access, as a conditio sine qua non, also a right to digitization education is something to reflect on. Such a right, a further specification of a right to education, could address the digital divide and digital illiteracy.[57]

3.2.3. *The right not to know*

Current legislation in the EU and its member states contains lots of disclosure provisions. For instance, Freedom of Information Acts contain obligations for government agencies to provide all kinds of government information to citizens upon request. The EU General Data Protection Regulation (GDPR) contains several data controller obligations regarding transparency, such as the obligation to inform data subjects (on their request) about which information about them is collected and processed, for which purposes and in which ways. In short, the right to information (a right to be informed, a right to know) can be clearly identified in many pieces of legislation, even though it usually has to be invoked actively by citizens and the scope and conditions may not always be clear. For instance, questions regarding inferred data, such as credit scores, life expectancies and health or other risks remain unanswered.[58]

For the opposite, a right not to know,[59] nothing is codified in legislation. Suppose a citizen does not want to know his or her individualized life expectancy, simply because he or she wants to live a life without an explicit 'due date'. In our society, such a person can nevertheless be confronted with such information, for instance, when applying for life insurance. Someone from a family with a hereditary disease can experience severe difficulties when applying for such a life insurance, as it may result in denying access to insurance or yield considerably higher premiums. In many cases, someone applying for life insurance is obliged to notify a hereditary disease on the forms (and disadvantage himself or herself), whereas someone who does no know about this does not have to notify this (and therefore cannot notify this).

With the help of big data, it is relatively easy to predict many sensitive characteristics of people. Apart from life expectancies, also risks for divorce, substance abuse, cardiovascular diseases and particular types of cancer can be predicted.[60] Some people may want to know the probability of suffering a cardiac arrest within five years, but others may not want to know this, as they may not want to live with such a 'Sword of Damocles' pending over their lives. This may particularly be the case for odds that cannot be influenced, for instance by adopting a different lifestyle, and diseases for which no cure or therapy exists.

Furthermore, it can be argued that some of these predictions have a high level of predestination or self-fulfilling prophecy. For instance, if it is predicted that someone will likely vote for a specific political party, such a prediction, if shared with the data subject, can influence an initially free choice. If it is predicted that a couple that is getting married will probably get a divorce after five years, it may perhaps make them wonder whether this is a good idea. If these are general statistics, the couple may be optimistic and think they can beat the odds, but if this is a personalized prediction, things may be different. Knowing the final result, they can decide to go for a few happy years anyway. Also, it could be argued they have right to make their own mistakes and learn from it, for instance, by better understanding what their ideal partner looks like after a failed marriage. If it can be predicted for a five-year old child whether it is straight or gay, it may be undesirable to actually make such predictions, because perhaps a person should find out for himself who he or she is, without life being mapped out in advance.

A right not to know, i.e., not being obliged to take notice of or being confronted with particular information, particularly information about yourself, could contribute to people's well-being. There is a plethora of literature on the right not to know, but mostly in a medical context,[61] not in a broader perspective. It is sometimes argued that withholding information from people is paternalistic and interferes with people's autonomy, but at the same time it can also have a positive effect on autonomy, for instance with regard to a right to make mistakes and the right to change your mind (see below). A further analysis would require making a distinction between not

[53] West, D.M. (2010) *An International Look at High-Speed Broadband*, Washington DC: The Brookings Institution. See also https://www.bbc.com/news/10461048.

[54] Sparks, I. (2009) Internet access is a fundamental human right, rules French court, *Daily Mail*, 12 June 2009. https://www.dailymail.co.uk/news/article-1192359/Internet-access-fundamental-human-right-rules-French-court.html.

[55] Article 5A of the Greek Constitution.

[56] In Spain, this was arranged via public procurement, see Reuters (2009) Spain govt to guarantee legal right to broadband, *Reuters*, 17 November 2009. https://www.reuters.com/article/idUSLH61554320091117.

[57] Blau, A (2002) Access isn't enough: Merely connecting people and computers won't close the digital divide. *American Libraries*. 33 (6): 50–52.

[58] Wachter, S., Mittelstadt, B., and Floridi. L. (2017) 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.

[59] Chadwick, R., Levitt, M., and Shickle, D. (1997) *The right to know and the right not to know*, Aldershot, U.K.: Avebury Ashgate Publishing Ltd.

[60] Kosinski, M., Stillwell, D. & Graepel, T. (2012) Private traits and attributes are predictable from digital records of human behaviour, *Proceedings of the National Academy of Sciences* (PNAS), www.pnas.org/content/early/2013/03/06/1218772110.

[61] Harris, J. (2020) Is there a right not to know? Journal of Medical Ethics 46, p. 414-415; Davies, B., Savolescy, J. (2020) The Right Not to Know: some Steps towards a Compromise, Ethical Theory and Moral Practice, https://doi.org/10.1007/s10677-020-10133-9; Vakharia, K. (2020) The right to know: ethical implications of antibody testing for healthcare workers and overlooked societal implications, *Journal of Medical Ethics*, 0, p. 1-3.

being informed about the use of predictive analytics[62] or the predictions resulting from it. Both scenarios do not necessarily involve a prohibition of predictive analytics in certain areas. However, allowing predictive analytics while at the same time giving people a right not to know can be complicated, for instance when the information is subsequently used to categorize people (such as credit scores) and make decisions that can influence their lives (such as restrictions in loans or mortgages).

3.2.4. *The right to change your mind*

When people disclose their preferences via their online behavior, for instance, when searching for particular information, all kinds of algorithms will try to offer information, including products and services, personalized on the bases of these preferences. For instance, if someone appears to be interested (inferred from clicking on particular links online) in sports and the economy, he or she will be fed more information on these topics than on other topics, like politics or music. As a consequence, people may end up in filter bubbles, with one-sided information provision.[63]

Sometimes, information is fed back in contents and formats that invariably confirm people in their perceptions and convictions. Online platforms in which this happens are referred to as echo chambers. In psychology it is commonly known that, in general, people prefer receiving information that confirms what they already thought above information that criticizes or contradicts this, a phenomenon known as cognitive dissonance.[64] Because of mechanisms like these, people can get stuck in feedback loops of information.

But what if people change their mind? Suppose someone who has always been interested in soccer wants to know more about tennis or that someone who was fully into politics now wants to learn more about arts. In a free society, it should obviously be possible that someone's interests or perspectives change. However, the ways in which information is supplied via the internet complicates this. People can become stuck in filter bubbles and echo chambers on the basis of interests and preferences from the past. If they change their minds, the current mechanisms for finding and retrieving information are not helpful, they may actually hinder or even prevent this.

A right to change your mind could perhaps be seen in the fundamental right to freedom of thought[65] or the freedom of expression,[66] but maybe the current technological developments required a renewed and strengthened right to change your mind. Literature on a right to change your mind is virtually absent, the only sources available in this area focus on contract law.[67] Particularly in contract law it is obvious that if people change their minds all the time this has significant legal complications. However, in a broader perspective, in the digital era, a new right to change your mind (if not too often) might put more weight on values like personal development, autonomy, informed consent and online freedoms. It may be invoked by people who end up in filter bubbles or are dealing with fake news and it may emphasize the role companies (particularly social media platforms and big tech companies) may have in taking responsibility in this.

3.2.5. *The right to start over with a clean (digital) slate*

The mechanisms of algorithms and risk profiling can be self-reinforcing processes. This may entail the risk that biases and inaccuracies can become further entrenched via positive feedback loops. Small deviations, such as incorrect or incomplete data, can then lead to larger perturbations and errors in conclusions that are drawn. Imagine that police surveillance is typically focused on specific neighborhoods that are known to be 'problematic'. As a consequence, police databases will become filled with data on citizens of these neighborhoods over time. When algorithms and risk profiling tools are then used to derive risk profiles from these police databases,[68] the results may show that the police should focus surveillance on these problematic neighborhoods. Obviously, this is circular reasoning, in which it is overlooked that the input data already contained bias.

In this example, the citizens of the 'problematic' neighborhoods, even those who do not show any criminal behavior at all, will be subjected to increasing surveillance and checks by law enforcement. More police surveillance can lead to stigmatization of these neighborhoods, causing decrease of the value of real estate in these neighborhoods. Such subsequent developments may make it harder for citizens to shake off these profiles and stereotypes, for instance, because they may not be able to move to another neighborhood even if they wanted so. In fact, these data may be connected to people for the rest of their lives.

A right to start over with a clean (digital) slate may strongly resemble the 'right to be forgotten', codified as the right to erasure in Article 17 of the EU General Data Protection Regulation (GDPR), a right figuring prominently in literature.[69] However, the right to erasure in the GDPR is not really a right to

[62] Note this would be in tension with Article 13-15 of the GDPR. These provisions state that people have a right to know about the existence of automated decision-making. Obviously, people can choose not to invoke these rights if they do not want to know, but they may be confronted with it anyway in the privacy policies provided by companies.

[63] Pariser, E. (May 2011) *The Filter Bubble: What the Internet Is Hiding from You*. New York: Penguin Press. p. 17.

[64] Festinger, L. (1962) Cognitive dissonance, *Scientific American*. 207 (4): 93–107.

[65] Cf. Article 18 of the UN Universal Declaration of Human Rights and Article 9 of the ECHR.

[66] Cf. Article 19 of the UN Universal Declaration of Human Rights and Article 10 of the ECHR.

[67] Smits, J.M. (2011) The right to change your mind? Rethinking the usefulness of mandatory rights of withdrawal in consumer contract law, *Penn State International Law Review*, Vol. 29, p. 671-684.

[68] Calders T. & Custers B.H.M. (2013), What is data mining and how does it work?. In: Custers B.H.M., Calders T., Schermer B., Zarsky T. (eds.) *Discrimination and Privacy in the Information Society*. Heidelberg: Springer.

[69] Fosch Villaronga, E., Kieseberg, P., Li, T. (2018) Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten, *Computer Law & Security Review*, Vol. 34, No. 2, p. 304-313,; Ausloos, J. (2012) The "Right to Be Forgotten" — Worth Remembering? 28 *Computer Law and Security Review*, 143, 152; Graux, H., Ausloos, J., and Valcke, P. (2012) The Right to Be Forgotten in the Internet Era, 11 ICRI Research Paper; Werro (2009) The Right to Inform v the Right to be Forgotten: A Transatlantic Clash, in A.C. Ciacchi, C. Godt, P. Rott, and L.J. Smith (eds.) Haftungsbereich im dritten Millennium/Liability in the Third Millennium (Nomos, Baden- Baden

be forgotten, it is merely a right to have some personal data erased in particular situations, if specific conditions have been met. In fact, Article 17 of the GDPR carefully balances the interests of data controllers and data subjects. It is in no respect a fundamental right, firstly because it is mentioned only in secondary rather than primary legislation, and secondly, because it is not phrased as an (almost) absolute right to which few or none exceptions apply.

A right to be forgotten may be expected to entail much more than the right to have some data erased. The right to erasure is very limited and data controllers do not always have to cooperate with requests from data subjects.[70] A right to start over with a clean digital slate would be much more comprehensive and would have to allow people to start over with a completely new (digital) identity.

In order to further explain this, compare this with someone who has finished serving time in prison. Ideally, after returning to society, this person should be able to start life with a clean slate. Criminal law assumes that the time in prison was the right and sufficient sanction. In practice, however, finding a job may be hard for someone who has been in prison for some time. The CV will contain an unexplained gap or, if someone is honest about this, prospective employers may be hesitant. Even though it is prohibited in several jurisdictions to refuse someone for a job because that person has a criminal record,[71] in reality reintegration can be hard for ex-convicts. It is for this reason that some states in the US, like New York State, introduced legislation prohibiting Criminal Record-Based Employment Discrimination (CBED).[72]

In this example, anti-discrimination law may also be sufficient, but a right to a clean digital slate (not discussed in existing literature) would cover a much wider range of issues that cannot all be addressed via anti-discrimination law. Examples of this could be debauchery and extravagance when being a student or diseases that a person overcame. When particular information becomes less attributable, for instance information on someone's youth, a right to a clean slate should perhaps be stronger. Particularly for children and adolescents, who are still developing their personality and personal and cognitive skills, a right to a clean digital slate may be useful, as some learning can only be done by trial and error. At the same it is clear that starting over with a clean digital slate would entail practical problems, but at a minimum it could be regulated that someone who really needs it, under certain conditions, is no longer linked to particular data from the past.

3.2.6. *The right to expiry dates for data*

The aspect of time is relevant when looking at changing interests and preferences, as discussed above, but also for the fact that data can become outdated over time. Addresses change when a person moves, names can change when people get married, and hobbies may change over the years. Just like milk, bread and other products, also data can expire. Therefore, it might be good to label data with expiry dates, just like any other consumable. Such expiry dates are obviously metadata and from a technological perspective they can easily be added to data. Or, at a minimum, the limited validity can be qualified. When doing this, it may also be considered adding confidence intervals to the data, indicating accuracy and reliability.[73] These things could be covered by a right to expiry dates for data, something that is not discussed in current literature, despite the fact that accuracy and reliability are important topics in technological, ethical and legal literature.

In practice, it may be hard to assign expiry dates to particular data in advance. In such cases, a date of origin (i.e., a date indicating when the data was generated) or a time limit that can be extended can be attached to the data. Someone may not know in advance whether he or she will move to a new address within five years from now, but an address dating from 1985 may very well be outdated. For hobbies or preferences, an extendable time limit of say three or five years could be used. Within this time limit, it may be assumed the data are still correct, whereas after that time limit has expired, it must be assumed the data are incorrect, unless their correctness is reconfirmed.

The same can be applied to informed consent for the collecting and processing of personal data.[74] Usually, such informed consent is asked for and provided when registering for a particular online service (like social media) or website (like when shopping online). However, after that initial moment of registration, the consent is only rarely reconfirmed or updated. Instead of consent forever, consent with an expiry data of three or five years might be more appropriate.[75]

3.2.7. *The right to know the value of your data*

Many online products and services, such as search engines and social media are for free. In essence this usually means that no subscription fee (i.e., a number of euros, dollar, or other currency) needs to be paid, but that a person 'pays with his or her data'. The companies offering the products and services are then allowed to collect and process these data and in some occasion can even trade, sell or lease the data. Although many people know that 'for free' is not really for free and that their data are being processed, it rarely is transparent which data are actually processed and how that is done. From a financial or economic perspective, it often is unclear what kind of transaction someone engages in.

2009) 291; Koops, B.J. (2011) Forgetting Footprints, Shunning Shadows 8 *SCRIPTed* 3, 5.

[70] Fazlioglu, M. (2013) Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet, *International Data Privacy Law*, Volume 3, Issue 3, p. 149–157.

[71] Article 10 of the GDPR regulates the processing of personal data relating to criminal convictions and offences. Such data can only be carried out under the control of official authority or when authorized by Union or Member State law. In short, this means private actors, like companies hiring employees are not allowed to process these data.

[72] https://dhr.ny.gov/protections-people-arrest-and-conviction-records

[73] Custers B.H.M. (2003) Effects of Unreliable Group Profiling by Means of Data Mining. In: Grieser G, Tanaka Y, Yamamoto A (red.) *Lecture Notes in Artificial Intelligence*. Heidelberg, New York: Springer Verlag. 290-295.

[74] Kleinig, J. (2010) The nature of consent. In: The ethics of consent: Theory and practice (Miller & Wertheim, ed.), New York: Oxford University Press.

[75] Custers B.H.M. (2016) Click here to consent forever: Expiry dates for informed consent, *Big Data & Society* : 1-6.

When a person purchases a washing machine, a car or a kitchen table, regardless of whether that is offline or online, such a product has a clear price tag indicating the amount of money that needs to be paid when buying it. However, for most of the free online services, like social media and search engines, it is entirely unclear what the value is that needs to be paid. True, in euros, dollars, or any other currency, the amount is zero, but in terms of data this is not clear, simply because consumers do not know what their personal data is worth for these companies. For a fair transaction, it could be argued, consumers should have the right to know the value of their data.[76]

Although there is plenty of literature on the value of personal data,[77] hardly any literature touches upon the right to know this value. Obviously a right to know the value of personal data requires determining the value first. There is no commonly accepted method for estimating the value of personal data.[78] Also, the value may be in the eye of the beholder. An important aspect here is that an individual's data on its own may not have significant value, but when combined with other data and processed, it may be very valuable.[79] Although it may be argued that data subjects are entitled to the value represented by their own personal data, this may be different when companies start adding value to the personal data via combining and analyzing it.

Hence, for this right there may exist several practical issues, such as regarding which pricing models need to be used for this, who should determine the value of data and how to enforce all this. Furthermore, there may be moral issues, since privacy is a fundamental right rather than a commodity that can be sold or traded and social segregation and ex ante discrimination may result from the fact that the personal data of some people is worth more than that of others.[80] On top of this, there may be cognitive issues related to this: research shows people do not read and understand privacy policies, terms & conditions, and other information provided, which makes it unlikely that they will take notice of these types of pricing information. There may also exist social pressure on people to sell their data, quickly capitalizing its value. Nevertheless, despite all these issues, it would enable a consumer to better assess how much a 'free' service actually costs (or should cost) in terms of disclosing personal data and granting rights to process these data for various purposes.

3.2.8. *The right to a clean digital environment*

Environmental law is a response to technological developments.[81] The right to a clean environment is included in various ways in catalogues of human rights, mostly as an obligation for governments to strive for a clean environment. It has been included in the constitution of more than one hundred countries across the planet.[82] A typical example can be found in Article 37 of the EU Charter of fundamental rights, stating that the government should protect a high level of environmental protection. Via national laws and case law, this is no longer merely a duty of care of governments, but has also become an individual right in many countries.[83]

Building on this, it could be argued that data is the pollution issue of the information age.[84] We all leave digital traces everywhere, consciously and unconsciously, intentionally and unintentionally. In analogy with the environment, it can be argued that all this digital exhaust can cause considerable pollution to the online ecosystem. Digital pollution can result in noise and bias if sucked into aggregation of data or analyses in combination with other data. Furthermore, digital pollution may be a barrier to the retrievability of other, more relevant data, like a kind of smog, obfuscating the (over)view.

In the area of environmental law, several instruments have been developed, such as energy labels, emission quota, and trade of emission rights. It could prove to be a useful exercise to assess to which extent such instruments are also applicable and useful to realize a clean digital environment. For a proper assessment, it is important to first investigate to which extent digital pollution is actually harmful for people, both in the short term and the long term. When a right to a clean digital environment is elaborated, it is also important, comparable to regular environmental law, to investigate whether this should be mostly or solely a duty of care for governments or also an individual right for citizens. Enforcement of such rights is also something to consider: given its international nature, there may be similar enforcement issues as in regular environmental law.

A right to a clean digital environment is not discussed in literature on environmental law, such literature only focuses on the offline environment. Also in IT law, this does not seem to be a topic of debate. However, these fields may be more closely related than perhaps expected. For instance, the use of

[76] Malgieri G. & Custers B.H.M. (2018), Pricing privacy – the right to know the value of your personal data, *Computer Law and Security Review* 34(2): 289-303.

[77] Ng, I. (2013) Value and worth: creating markets in the digital economy, Innovorsa, Cambridge; World Economic Fund (FEM), 2013, Unlocking the Value of Personal Data: From Collection to Usage, World Economic Forum, Geneva; Liem, C., & Petropoulos, G. (2016) The economic value of personal data for online platforms, firms and consumers, *The London School of Economics and Political Science*.

[78] OECD (2013) Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, Organization For Economic Cooperation And Development OECD Publishing.

[79] Stelmaszak, M., and Parry, G. (2021) Data are in the Eye of the Beholder: Co-creating the Value of Personal Data, Proceedings of the 54th Hawaii International Conference on System Sciences.

[80] Typically, data on people facing a big life event, such as having a baby or getting married are worth more, because companies know people will be spending large(r) amounts of money.

[81] Rhoen, M. (2017) Rear View Mirror, Crystal Ball: Predictions for the Future of Data Protection Law Based on the History of Environmental Protection Law, 33 *Computer Law & Security Review,* 603.

[82] https://www.unenvironment.org/explore-topics/environmental-rights-and-governance/what-we-do/advancing-environmental-rights/what-0

[83] Verschuren, J. (1993) The constitutional right to environmental protection, see https://pure.uvt.nl/ws/portalfiles/portal/364753/envartcult.html#N_1_; Atapattu, S. (2002)The right to a healthy life or the right to die polluted? The emergence of a human right to a healthy environment under international law, *Tulane Environmental Law Journal*, Vol. 16, p. 65-126.

[84] Schneier, B. (2013) The Battle for Power on the Internet, *Internet and Security* 19. https://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/

blockchain technology may use very large amounts of energy and generating this energy may put pressure on the environment.[85] Another example is the current rush for lithium and other rare earth elements, which are a critical ingredient for all batteries around the world.[86] Hence, a right to a clean digital environment may be directly related to the right to a clean (offline) environment, since a clean digital environment may require less energy and natural resources or at least will use these more effectively.

3.2.9. *The right to a safe digital environment*

When dealing with (human) rights in the digital era, it is perhaps not very practical to use the traditional distinction between classic human rights versus social human rights – in the digital era these may all have a somewhat classic nature. Nevertheless, the underlying distinction (a government needs to restrain itself and refrain from interfering with the lives of citizens in various aspects versus a government has a duty of care) may be useful. A duty of care is a useful starting point for several of the abovementioned rights, such as the right to digitization education and a right to a clean digital environment. This may also apply to a right to safety, more particularly a right to a safe online environment.[87]

Safety can be under pressure when people are not very careful (do not pay attention), when systems are designed in flawed ways, or when other people have bad intentions. The third category mostly focuses on security issues.[88] One hundred percent safety (and security) usually cannot be guaranteed in most contexts, neither online nor offline. However, that does not mean that the government and private actors should not strive for safety and security. Governments can try to improve online safety via specific regulation in this domain, such as criminalizing types of excessive online behavior and creating private law liabilities if actors do not implement adequate safety measures. Many countries have codified that the government has a duty of caring for a safe and secure society, but it is not clear whether this extends to the online environment. In some ways it does, for instance, when people threaten each other online, but in some ways it is unclear, for instance, in case of hate speech or misinformation. It could prove to be helpful to have explicit norms for minimum levels of online safety and confirmation that a right to a safe and secure environment (whether that is a duty of care for the government or an individual right) also extends to the online environment. There exists a lot of literature on cybersecurity,[89] but a fundamental right to a safe digital environment is rarely discussed.

Table 1 – Status overview of the new digital rights suggested.

New right	Status
The right to be offline	Introduced in some countries
The right to internet access	Introduced in some countries
The right not to know	Novel concept, only in literature
The right to change your mind	Novel concept, only in literature
The right to start over with a clean (digital) slate	First, limited attempt in the GDPR' right to erasure
The right to expiry dates for data	Novel concept, only in literature
The right to know the value of your data	Novel concept, only in literature
The right to a clean digital environment	Extension of existing (non-digital) right
The right to a safe digital environment	Extension of existing (non-digital) right
The right to digital education	Extension of existing (non-digital) right

3.3. *Status overview*

Apart from a few exceptions and attempts, the new digital rights put forward in Section 3.2 are not yet implemented in practice. The right to be offline exists to some extent in France, Italy, and Germany. The right to internet access exists to some extent in Finland, France, Greece, and Spain. Furthermore, the right to erasure (sometimes referred to as 'the right to be forgotten' although that is not entirely the same) in Article 17 of the EU General Data Protection Regulation (GDPR) could be considered as an attempt to introduce a right to start over with a clean (digital) slate

Some of the new digital rights put forward in this article are not really novel, but mostly extensions of already existing rights. A right to digitization education arguably is an extension or elaboration of the right to education, the right to a clean digital environment is an extension of the right to a clean environment, and the right to a safe online environment is an extension of the right to a safe environment or a right to security. In other words, implementing these rights could be relatively uncomplicated – in most jurisdictions it would require rephrasing or interpreting the non-digital right in a digital context.

At the other end of the spectrum, however, are the new digital rights that currently only exist as concepts in literature. Typically, the right not to know, the right to change your mind, the right to expiry dates for data, and the right to know the value of your data are all rights that have not been implemented in any jurisdiction. Implementation of these rights is complicated, as further debate on the exact phrasing and scoping would be required as well as further research on the consequences of introducing any of these rights.

Whether a new right is an extension of an existing right or a completely novel concept obviously affects the feasibility of implementing such a right. Table 1 provides an overview of

[85] De Vries, A. (2018) Bitcoin's Growing Energy Problem, *Joule*, Volume 2, Issue 5, p. 801-805; Dittmar, L., Praktiknjo, A. (2019) Could Bitcoin emissions push global warming above 2 °C? *Nature Climate Change*, 9, p. 656–657.

[86] Haxel, G. B.; Hedrick, J. B.; Orris, G. J., (2002) Rare Earth Elements - Critical Resources for High Technology. In Department of the Interior, U.S.G.S., p 4. http://pubs.usgs.gov/fs/2002/fs087-02/.

[87] Cf. Van Kempen, P.H. (2013) Four Concepts of Security – A Human Rights Perspective. *Human Rights Law Review*, Vol. 13(1), p. 1-23.

[88] Burns, A., McDermid, J., Dobson, J. (1992) On the Meaning of Safety and Security, *The Computer Journal*, Volume 35, Issue 1, p. 3–15.

[89] Tikk, E., and Kerttunen (2020) Routledge Handbook of International Cybersecurity, New York: Routledge; Moallem, A. (2018) Human-Computer Interaction and Cybersecurity Handbook, Taylor & Francis.

the current status of the rights put forward in this article, to further clarify these differences.

4. Conclusion

In this article, several new (fundamental) rights for citizens in the digital era were suggested. As indicated, this is not an exhaustive enumeration, these are merely some suggestions to revive and broaden the debate on this topic.

Although the thought experiment ('which new, additional fundamental rights are necessary in the digital era?') is useful to set aside for a moment the already existing (fundamental and other) rights that people have, it may be clear that we should not abandon these existing fundamental rights. Admittedly, the rights suggested in this article are not always that much out of the box: some of these rights are mostly a digital extension of an already existing (non-digital) right. At the same time, some other rights are novel concepts that only exist in academic literature and may be a long way from actual implementation, requiring further research and extensive political and societal debate. Despite these differences, implying differences in feasibility, they were put forward here, because they are all new, some of them new in all aspects, some of them new only in a digital context. For all rights, even those that are perhaps more feasible to implement, it can be said that the current debate does not really focus much on these topics. It often seems hard enough to deal with the challenges and issues in an offline context. As a result of this, there is perhaps limited time, energy and budget left to focus on additional issues in an online context. However, it may be clear that not focusing on these issues does not imply they will automatically disappear themselves.

Most of the debates in this area focus on a limited number of (fundamental) rights that may need to be updated, such as the right to freedom of expression and the right to privacy. Hence, even when discussing the need for updating existing rights, the debate can be broadened to a number of other rights that are hardly in scope. The scope and workings (including the level of protection they offer) of almost all current fundamental rights may be different in an online context. For instance, the right to fair trial and access to courts, which are fundamental in democratic societies, can be viewed from a completely new perspective in the light of developments in artificial intelligence that is tailored for the judiciary. If artificial intelligence can accurately predict court outcomes,[90] the need for going to courts may change. If these litigating parties can benefit from very expensive tools, the access to justice and the equality of arms during litigating may get under pressure. Some even argue that artificial intelligence might take over court decisions in the long term, being more objective judges than human beings.[91] Such developments obviously may cause concerns related to procedural and material justice.

The rights suggested in this article are specifically tailored to the digital era, but existing fundamental rights relating to, among others, equal treatment, freedom of religion, freedom of expression, freedom of thought, privacy, access to courts and fair trial are all relevant in the digital era in which personal data are collected and processed on a massive scale to take decisions on people. This means that the current catalogues of fundamental rights (e.g., the ECHR, the EU Charter of fundamental rights and national constitutions) are as relevant as they have always been.

However, on the one hand these catalogues of fundamental rights may need some maintenance and updating by now and on the other hand these catalogues may need a thorough review on how complete they are in this digital era. There does not seem to be an on-going debate on this in most countries or at the EU level.

The suggestions in this article cannot be regulated by slightly modifying existing fundamental rights. Firstly, it is necessary to do further research on these and other potential new (fundamental) rights, particularly on what kind of protection they can offer. Ideally, in such research developments in several front-running countries are compared. Secondly, on the basis of this information societal and political debates have to take place, discussing which rights are considered necessary. Thirdly, after having a clearer understanding of what is needed, further research needs to be done on how these new (fundamental and other) rights can be implemented, for instance, focusing on the exact phrasing, the level of (primary or secondary) legislation and the precise scope. In this way, the legal protection for citizens can be made future-proof for the longer term.

Declaration of Competing Interest

For this paper, there are no conflicts of interests to report.

Data Availability

1. No data was used for the research described in the article.

[90] D Katz, M Bommarito, and J Blackman, "Predicting the Behavior of the Supreme Court of the United States: A General Approach", *PLoS ONE,* Vol. 12, nr. 4., e0174698, 2014; N Aletras, D Tsarapatsanis, D Preoţiuc-Pietro and V Lampos, "Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective". *PeerJ Computer Science* 2:e93, 2016. See https://doi.org/10.7717/peerj-cs.93.

[91] Nakad-Weststrate H.W.R., Herik H.J. van den, Jongbloed A.W.T. & Salem A.B.M. (2015) The Rise of the Robotic Judge in Modern Court Proceedings, *International Journal for Digital Society* 6(4), p. 1102-1112.