7 Non-use of the Internet as human rights enabler?

The curious cases of the right to privacy and the right to health

Władysław Józwicki and Łukasz Szoszkiewicz

7.1 Introduction

The diffusion of the Internet has revolutionised how we communicate, access information and receive public services. However, this technological innovation has also brought forth challenges that raise critical questions about its inherent features and their impact on the enjoyment of human rights. The excessive collection and commodification of personal data remain beyond the control of an individual. Paradoxically, countermeasures such as obligatory informed consent for personal data processing (i.e., cookies) have led to "privacy fatigue", a phenomenon when individuals "disclose personal information despite their privacy concerns" (Choi *et al.* 2018). Massive collection of personal data implies exposure of sensitive information to data breaches, for instance in healthcare (Seh *et al.* 2020). Network effects magnify these issues by enabling misinformation to spread rapidly and creating echo chambers where individuals are insulated from diverse perspectives. While the Internet serves as a powerful tool for social mobilisation, its network-based dynamics of information flow and content filtering algorithms can also facilitate polarisation (Peralta *et al.* 2021). Furthermore, algorithmic manipulation poses a distinct challenge to informational self-determination. By creating micro-profiles of individuals based on their online behaviour, these algorithms enable personalised targeting that can be harnessed for political campaigning (Martino *et al.* 2020).

For this reason, we will analyse whether non-access to the Internet can be seen as a human rights enabler and what consequences that brings to the realisation of particular human rights as well as to the proportionality analysis in a case of conflict of rights. We argue that the non-use of the Internet should be taken seriously when assessing all the requirements of proportionality in the large sense, as well as when applying the principle of progressive realisation of economic, social and cultural (ESC) rights. This is due to the fact that by choosing not to be online, individuals can protect themselves from the trade-offs inherent in the digital environment and exercise their rights in ways that are not achievable online. Also, the states and monitoring bodies should not forget about the threats to human rights, which are inherent in the nature of being online when Internet technologies are being used as a means to enable human rights. We will analyse these paradoxes through the lens

DOI: 10.4324/9781003528401-9

of two human rights – privacy and health – to demonstrate how informed choices regarding Internet non-use can influence their enjoyment and how that needs to be reflected in human rights policies and their review. In this analysis, we will primarily rely on the United Nations (UN) international human rights framework and, if necessary, integrate regional and national developments that relate to the non-use of the Internet.

7.2 Non-use of the Internet as an enabler of the right to privacy

The Internet is a technology based on the transmission of data over a network of computers and other devices, such as servers or mobile devices. Any data transmission is carried out through infrastructure maintained by intermediary entities (e.g., Internet service providers or operators of cloud-based services), which inevitably involves the possibility of third-party access. Even the most advanced data encryption methods (Stoykova 2023) and other privacy-enhancing tools (e.g., Virtual Private Networks, Tor network) do not provide complete protection against unauthorised access to data on online behaviour. The sense of privacy and anonymity relies on the assumption that the financial and organisational burden of identifying a given person will be too excessive for third parties. Nevertheless, any sharing of personal data means a potential loss of control over it. Even if reidentifying a person were not currently possible, advancements in technology could make it feasible in the (near) future. By not participating in the digital environment, individuals avoid the traps of data exploitation and maintain a degree of autonomy over their personal data that is increasingly difficult – or impossible – to achieve online.

However, non-use of the Internet is not about the complete rejection of technology but about making informed choices concerning when and how to engage with the digital environment to maintain control over one's personal data. It can be driven by the desire to protect one's private life, avoid personal data collection or minimise exposure to unwanted online digital tracking by corporations and public authorities for various purposes ranging from mass surveillance to targeted advertising.[1] An example of non-use in this context could be choosing not to use Internet-based health services to protect sensitive health data from digital collection and potential misuse or data breaches. It is estimated that between 2005 and 2019 the total number of individuals affected by data breaches in healthcare systems was nearly 250 million worldwide, with most of them affected in the last five years.[2] In the future, we will likely observe leakages of neural data, which is increasingly collected by business actors, and which can be decoded to reveal one's most intimate features (Yuste & De La Quadra-Salcedo 2023).

In this sense, the decision not to use the Internet can be seen as a form of exercising the right to informational self-determination, which was coined in the 1980s and, since then, penetrated regional and national human rights frameworks.[3] It has been invoked *expressis verbis* in the jurisprudence of the European Court of Human Rights (ECtHR 2023), Inter-American Court of Human Rights (IACtHR 2024), and selected Asian countries[4] as one of the fundamental components of the

right to privacy. Invoked, for the first time, by the German Constitutional Court in the *Census* case of 1983, the right to informational self-determination "confers upon the individual the authority to, in principle, decide themselves on the disclosure and use of their personal data" (BVerfG 1983). The Court has also emphasised that the lack of "sufficient certainty" over the kind and scope of personal data known to third parties "impede[s] freedom to make self-determined plans or decisions" (BVerfG 1983, para. 146).

As with other human rights, the right to informational self-determination is not absolute and can be restricted. It can, therefore, be subjected to a proportionality analysis, which requires all the proportionality tests to be conducted and passed in order to allow a limitation of a particular right or freedom. In this text, we adhere to a broad understanding of the proportionality analysis. Limitations in the enjoyment of rights and freedoms, in order to be legitimate and proportionate *sensu largo*, must cumulatively meet six requirements. First, they need to be determined/prescribed by law, which also contains legislative quality requirements. Second, they need to realise a legitimate aim, which in the context we are analysing is predominantly the rights and freedoms of others (the ones provided with the use of online methods). Third, they need to be suitable/appropriate to achieve the above aim. Hence, they must lead to genuine progress in the realisation of the right in question. Fourth, they need to be necessary to do that, meaning that there is no other less restrictive to the limited right method to achieve progress in the concurring right. Fifth, the limitation needs to be proportionate *sensu stricto*, meaning "[t]he harm (cost, burden, sacrifice) caused by the limitation must be 'proportional in a strict sense' to the benefit (gains, good) it contributes to produce" (Tremblay 2014, 865). Lastly, sixth, while introducing limitations in the enjoyment of rights and freedoms, we have to bear in mind that the essence of the limited right or freedom must always remain intact so the right may not become annihilated or drained out of its content.

Given the nature of the Internet, any transition to the digital environment will inherently involve limitations in the enjoyment of the right to informational self-determination. In other words, every digital solution perceived as an enabler of individual rights (e.g., personalised medicine as an enabler of the right to health) will require an assessment of proportionality that involves the right to informational self-determination. As we will show, the non-use of the Internet (and implications for the right to informational self-determination) is frequently overlooked in that context. However, if we take rights and freedoms seriously, we need to apply all the above-mentioned proportionality analysis elements.

First, the limitations need to be determined/prescribed by law. This means that the courts must determine whether the collection, retention, processing and authorisation of access to personal data are "in accordance with the law". Therefore, the legal basis must meet certain qualitative requirements (i.e., the "quality of the law"), which implies accessibility for the individual and predictability of its application (ECtHR 2015, para. 236). The law must also provide adequate and effective safeguards against arbitrariness and the risk of abuse (ECtHR 2015, para. 302). The German Federal Constitutional Court, in assessing a case on predictive

policing, ruled that "the severity of interference with the right to informational self-determination primarily depends on the type, scope and possible uses of the data, as well as the risks of abuse" (BVerfG 2023). For this reason, an individual should have sufficient certainty over the further use of one's personal data, in particular requirements under which data can be used for purposes other than initially collected. For example, under what requirements data taken as part of healthcare can be made available to law enforcement authorities for the purpose of crime prevention. In recent years, international and national legal instruments and case law has provided cases that involved "repurposing" of personal data processing, which implies the possibility of changing the legitimate aim for which the data was originally collected. For instance, the EU's proposal for establishing the European Health Data Space aims to introduce the secondary use of electronic health data for, *inter alia*, healthcare, scientific research, education and training of AI-based systems.[5] Hence, the technical and legal possibility of changing the purpose of processing should already be clearly determined by the law allowing the collection of data.

Second, limitations need to realise a legitimate aim. Sometimes, a collection of digital data is justified with the protection of national security or public order, particularly in countries where law enforcement agencies have extensive powers to search computer systems. Other commonly invoked legitimate aims include the protection of the rights and freedoms of others (in particular, an increasing accessibility and quality of a given social right) or public health (e.g., preventing the spread of COVID-19). The invocation of these values can lead to various actions in the digital environment. An analysis of the recommendations formulated under the Universal Periodic Review shows that in some countries, the Internet is primarily a tool to strengthen the protection of the right to freedom of expression or the right to assembly. Therefore, such countries are recommended to refrain from restricting and shutting down the Internet (UPR – Uganda 2022; Gabon 2023; Morocco 2023). At the same time, another group of states is recommended to ensure the right to privacy and freedom from censorship on the Internet, which suggests that they leverage digital connectivity for surveillance (UPR – the Netherlands 2022; Nauru 2021).

Although the Internet – like any technology – is described in terms of both risks and opportunities for human rights, some authors suggest that "preventive repression [will] increase as technology continues to develop in the future" (Dragu & Lupu 2021). In some states, digitalisation has become a tool that facilitates governmental control, such as in China or Egypt.[6] The preventive repression includes primarily non-violent forms of repression leading to chilling effect. In this context, the non-use of the Internet becomes not only an enabler of the right to privacy but the last stronghold of individual autonomy.

The broad powers of law enforcement agencies are also used in countries with strong protection of individual rights. This is demonstrated by the EncroChat case, in which the Dutch and French services, Europol as well as Eurojust successfully infiltrated the EncroChat network, which was facilitating communication (mainly) between organised crime groups. A series of cases before courts across Europe has

revealed the lack of binding digital forensics standards in criminal proceedings which would be compliant with the right to a fair trial (Stoykova 2023).

Third, limitations need to be suitable/appropriate to achieve the legitimate aim. Interventions involving the collection of personal data (and consequently limiting the right to informational self-determination) are usually motivated either by the protection of national security or the progressive realisation of other rights, in particular social rights such as the right to health or the right to education. However, to be considered appropriate, digital services should genuinely facilitate legitimate aims. For instance, despite their limitations, tracing apps have proven beneficial in preventing the spread of COVID-19. The deployment of smartphone applications enabled near real-time data collection and analysis, whereas traditional surveillance methods are typically delayed by one to three weeks (as seen in the United States) (Pandit *et al.* 2022). Timing is crucial in preventing the spread of the virus, whose incubation period is typically less than 14 days (O'Connell *et al.* 2021). While the collection of personal data interferes with privacy, it serves dual purposes: forecasting the transmission of the virus (thus protecting public health) and assessing an individual's likelihood of exposure when moving through various spaces or interacting with others (thus facilitating the right to health).

Fourth, limitations need to be necessary, which indicates that any limitation of an individual right should be the least restrictive means to achieve a legitimate aim. In the context of digital public services, the legitimate aim often hinges on their increasing quality (e.g., due to the better allocation of financial and organisational resources) and enhanced accessibility, which leads to the progressive realisation of ESC rights, such as the right to health. However, this rise in quality and accessibility cannot be justified by a proportional – or even exponential – enabling of the realisation of a given right if it leads to a restriction of another right. According to the requirement of necessity, any restriction of rights should be made only when there is no other way to achieve the legitimate aim, and to the narrowest possible extent for the realisation of a specific legitimate aim. This means that if it is possible to strengthen the realisation of a given right by allowing it to be exercised online while at the same time maintaining the possibility of offline exercise, public authorities should ensure both forms of realisation of the right. Both the Human Rights Committee (HRC 2014, para. 37) and the Committee on Economic, Social and Cultural Rights (CESCR 2000, para. 47) highlighted in various contexts that rights include "core obligations" which cannot be conditioned on the availability of resources and the same should apply to the right to informational self-determination.

Fifth, the limitation needs to be proportionate *sensu stricto*. Due to the "indivisibility, interdependence and interrelatedness"[7] of human rights, strengthening the realisation of one right often impacts the realisation of another. Assessment of proportionality *sensu stricto* then requires consideration of the proportion of an interference. The transfer of public services to the digital environment, in many cases, will involve strengthening the realisation of various rights, such as the right to participation in public life (e.g., voting online) or the right to health (e.g., telemedicine). At the same time – due to the specific features of the Internet described in the introduction – it will always interfere with the right to privacy, particularly

informational self-determination. As long as the infringing upon privacy remains proportional to strengthening the realisation of another right, it could be justified. Proportionality will become increasingly difficult to justify as privacy protection becomes more burdensome, e.g., when a significant reduction in the grid of polling places accompanies the introduction of an optional form of online voting. When the difference between the possibility of exercising a given right online and offline reaches such great differences that exercising it in the latter form will be extremely burdensome, such an action should be considered disproportionate. One can claim that it was possible for public authorities to act in such a way as to make it possible to organise online voting without unduly restricting the right to informational self-determination.

Estonia's Internet voting system exemplifies a careful balance between protecting privacy and promoting the right to public participation. Introduced in 2005, this system enhances participation by making voting more accessible to those who cannot or do not like to visit polling stations in person. However, despite its convenience, Internet voting poses privacy concerns, such as potential cyberattacks that could compromise ballot secrecy. The Supreme Court upheld that the individual, once properly informed of the risks related to Internet voting, should decide whether or not to cast his or her vote online (Madise & Vinkel 2011, 8). Therefore, Estonia maintains traditional paper ballots as an alternative, allowing individuals who prioritise privacy over digital convenience to vote in a traditional way.

Last but not least, limitations cannot infringe upon the essence of the right to informational self-determination. In this context of digital-only public services, it will be necessary to analyse the nature and scope of the data acquired, the retention period (which should be as short as possible), the authority processing the data, as well as the permissibility of changing the purposes of the processing. The degree of datafication of the society may also play a role in the assessment – the higher it is, the more likely it is that public authorities can create an accurate digital profile of an individual, which, in our opinion, could lead to the infringement of the essence of the right to informational self-determination.[8] It seems reasonable to claim that selected data, e.g., on the content of the vote cast in an election, should never be processed for different purposes than initially collected. However, most of the data protection regulations allow for further processing of personal data (even so called sensitive data) if certain conditions are met (e.g., for research and statistical purposes, when data is properly anonymised,[9] for the protection of equally important public interest).

7.3 Non-use of the Internet as an enabler of the right to health

One of the rights often associated with the benefits the Internet can provide to its realisation is the right to health. The Internet may enhance especially the accessibility and availability of the right to health. Regarding physical accessibility, the Internet opens the possibility of providing medical services, in cases not requiring in-person contact, *via* long-distance care (Pawelczyk 2018, 620). Regarding economic accessibility (affordability), online medical care does not require costly

and time-consuming travel to specialists unavailable in the neighbourhood. Also, the costs of consultations may be reduced. Internet access may alleviate health inequality (Yu & Meng 2022), thus serving non-discrimination in the enjoyment of the right to health. That applies especially when it comes to underprivileged groups, which are particularly economically vulnerable, as Internet access mitigates the negative impact of income inequality on healthcare access (Yu & Meng 2022). Internet access may also improve healthcare quality due to increased access to scientific knowledge for medical personnel, for instance, through databases of medical literature or Large Language Models, which are increasingly trained on medical papers (Clusmann *et al*. 2023). Finally, being online can significantly increase information accessibility. The latter should not, however, be considered as a possible replacement for professional medical care but as a supplement to it.

Recently, the COVID-19 pandemic revealed some health-beneficial force of the Internet and access to information. Regardless of community type, mortality rates were generally higher during the pandemic in places with limited Internet access (Lin *et al*. 2022). Moreover, being online may lead to increased demand for medical services. Searching for health information significantly affects an individual's demand for healthcare (Suziedelyte 2012). All in all, Internet access generally improves the average health condition (Yu & Meng 2022). As the UN Committee on the Rights of the Child (CRC) underlined regarding the relatively better digitally included group, which are young people:

> the Internet provides opportunities for gaining access to online health information, protective support and sources of advice and counselling and can be utilised by States as a means of communicating and engaging with adolescents. The ability to access relevant information can have a significant positive impact on equality.
>
> (CRC 2016, para. 47)

Being online in different ways serves as, and potentially increasingly so, an enabler of the right to health. This needs to be considered while undertaking the proportionality analysis with other rights and freedoms endangered by being online, such as the right to privacy, which was analysed in more detail in the previous section, but also other rights which can be negatively affected through (algorithmic) bias and discrimination or function creep, which often accompanies Internet-based healthcare services (Sun *et al*. 2020, 23). In all such cases, a method to be applied is the proportionality analysis of whether the advance in the realisation of one right is proportional to the detriment of another.

The situation when it comes to the right to health is, however, more complex than that. While being online provides certain benefits for the right to health, it also poses certain threats to this right. This is the case regarding both the very same aspects of the right that it may enhance but also regarding other ones. Digital health technologies can contribute to health inequity by deepening the consequences stemming from the "digital divide" between those who can and cannot access such interventions, some of which may be mitigated with different means like review

and accountability mechanisms (Sun *et al*. 2020, 23, 25, 29). Some, however, may not. Some threats to the right to health may not be prevented by legal mechanisms or technological solutions but are inherent to the nature of being online. All the benefits from the online right to health enablers may be enjoyed only by those who also enjoy Internet access (ca. two-third of the population worldwide). The issue is that some vulnerable groups are overrepresented in offline groups (e.g., indigenous peoples). That may be eliminated by the increase in Internet access availability and digital literacy promotion. Before that becomes universal, the divide and the most basic stemming from it right-to-health-related consequences remain, however, inevitable.

When it comes to equality, the health-related information gathered and available for the development of diagnosing, results analysis and research on the sources of and treatment methods of different diseases represents only those who actually are connected, which reflects the imbalance of the spread of connectivity, and privileges particular regions or particular groups. The so-called "health data poverty" disables individuals, certain groups or even whole populations from benefiting from discovery or innovation due to a scarcity of representative data. That may prevent some (groups of) people from the benefits of data-driven digital health technologies or even lead to them being harmed by such technologies (Ibrahim *et al.* 2021, 260–261). That, again, may, to some extent, be mitigated by different means, which, however, cannot be immediate. Also, an extended history of data availability may create something of a kind of "connectivity capital", resulting in more accurate and effective data-driven digital health technologies applications for certain groups. In 2021, 86.3% of genomics studies including genome-wide association studies have been conducted in individuals of European descent. This proportion has increased from 81% in 2016 at the cost of the underrepresented populations (Fatumo *et al*. 2022), which shows that both the current situation and tendency are counter-egalitarian.

Another significant issue is the access to health-related information. Generally, the Internet threatens with disinformation or information overload as well as shallowness or superficiality of the information offered (Kloza 2024). These threats become particularly hazardous when it comes to health-related information. The information may quickly turn out to be incomplete, imprecise or even represent misinformation, and thus be useless or even harmful in the hands of a recipient. An unprecedented and increasing majority of parents and guardians are using the Internet for information concerning their children's health. They are, however, not necessarily using reliable and safe sources of information (Pehora *et al*. 2015). Reliance on non-traditional health sources, amplified by network effects and algorithmically designed echo chambers, led, already before the COVID-19 pandemic, to increasing vaccine hesitancy (Getman *et al*. 2018). The COVID-19 pandemic may, however, serve as a particularly telling example of the potential scale of health misinformation, which arose to an extreme example of an "Infodemic" (Borges do Nascimento *et al*. 2022).

There are methods to minimise that kind of threats. It is undoubtedly advisable that "health care providers should begin to focus on improving access to safe,

accurate, and reliable information through various modalities including education, designing for multiplatform, and better search engine optimization" (Pehora *et al*. 2015). This and other means can also be implemented on policy-making and legal grounds. None of them may, however, be fully implemented together with connectivity. Access to the Internet or health-related information may not be made in any way conditional upon meeting certain requirements by the receivers. Also, a full or limited selection of available Internet information does not rest in any single state or international organisation's capacities. Therefore, it is imminent that misinformation, misinterpretation or misapplication of information on the web might lead to health-threatening choices by the receivers. A new challenge has been created by the development of the Large Language Models, which, admittedly, may have some potential to democratise medical knowledge and facilitate access to healthcare but – due to their design – are also prone to "distribute misinformation and exacerbate scientific misconduct due to a lack of accountability and transparency" (Clusmann *et al*. 2023). The balance between benefits and damages stemming from an almost unlimited flow of information on the Internet and access to it by anybody is, in many aspects, extremely shaky.

The CRC already in 2013 expressed concern

> by the increase in mental ill-health among adolescents, including developmental and behavioural disorders; depression; eating disorders; anxiety; psychological trauma resulting from abuse, neglect, violence or exploitation; alcohol, tobacco and drug use; obsessive behaviour, such as excessive use of and addiction to the Internet and other technologies; and self-harm and suicide.
>
> (CRC 2013a, para. 38, see as well: CRC, 2013b, para. 46)

Being online is one of the factors increasingly endangering mental health. Children represent a particularly vulnerable group in that regard, but not the only one. The most apparent threats seem to be addictions and the so-called FOMO ("fear of missing out") (Kloza 2024), but the constant connectivity can impair people's well-being in many ways and is related to the most severe clinical phenomena like depression but also anxiety, loneliness and other mental health outcomes related to subjective well-being (Cai *et al*. 2023). "Digital detox" or simply a choice of limiting connectivity may be one of the means to challenge this threat (Radtke *et al*. 2022).

However, that has become more and more difficult also due to the increased supply of online services. For those who do not have Internet access, "especially on a 'smart' device, life has become unduly burdensome and, at times, even impossible" (Kloza 2024). That applies also to the digital services provided in order to facilitate certain human rights availability. Therefore, the related to being online mental health threats become accompanied also by the accumulated enablement of other rights *via* online means, which increases the scale of the problem and thus of the risks that excessive use of the Internet brings to people's health. That calls for an in-depth proportionality analysis of the increased demand for connectivity required by enabling other human rights by the online services and resulting

from that adverse effects on the right to health, which have to be considered as limitations of the latter and allowing the increase in the services available online only if all the proportionality requirements in limiting the right to health are met. Their offline availability becomes thus yet another parameter to be considered under the proportionality test while introducing their online equivalents at the cost of other rights, like the right to health. That is yet another example of the first of the general conclusions that stem from our analysis.

However, while being a threat, online solutions may also be effectively used to solve at least some of the mental health issues. The earlier arguments regarding healthcare improvement through the possibilities the Internet provides also apply to mental health issues (Reglitz & Rudnick 2020). That is yet another example of the second of the general conclusions that stem from our analysis. Enabling the right to health *via* the Internet requires an in-depth analysis of the being online effects on the health of people under the framework of progressive realisation of the right to health in both the mental and physical dimensions and increasing the services available online only if the overall result is positive, especially in the light of "strong presumption that retrogressive measures taken in relation to the right to health are not permissible" (CESCR 2000, para. 32). Enabling the right to health *via* the Internet also requires the guarantee that the right will be exercised without discrimination of any kind, which is an immediate obligation of the states (CESCR 2000, para. 30), not a progressive one (Saul *et al*. 2014, 133–213). In light of what has been shown, the latter seems especially challenging in the context of the "digital divide" and other threats to equality connected to online enablers of the right to health.

7.4 Concluding remarks

Being online indisputably enhances the enjoyment of different human rights. At the same time, it brings some trade-offs to some of them, like the right to privacy or, to some extent, the right to health. Some of the challenges may be avoided or mitigated by adjusting policies or legal solutions to be implemented on the state or international level. Nevertheless, certain trade-offs remain inherent in the very nature of being online, and it is not possible to eliminate them.

Inevitably, an increasing number of services, be they public or private, become available *via* the Internet (Kloza 2024). When it comes to enabling human rights and endangering other human rights by those services, it becomes an issue of proportionality analysis. It must become increasingly applied at policy-making, judicial review or other monitoring levels. That applies equally, irrespective of whether we recognise online services as enablers of human rights or as a self-standing right of access to the Internet, which, not being absolute, also is a subject of proportionality (Dror-Shpoliansky & Shany 2021, 1274). Similarly, it applies irrespective of whether we consider non-access to the Internet as a choice driven by the realisation of human rights and hence their enabler (as we do in this text) or whether we opt for the recognition of a new, standalone human right not to use the Internet, which neither is absolute and is thus subject of proportionality (Kloza 2024).

The competent bodies should carefully take all the stemming from being online consequences for the enjoyment of human rights under consideration. That means that they should consider the benefits to human rights available through online means, but also the threats stemming therein. They should remember that progress in one right achieved *via* online means may adversely affect other human rights, but also that online realisation of a particular right may, in one aspect, enhance its enjoyment while, in another, deteriorate it. The proportionality methodology should be applied with all the tests it requires and with particular sensitivity to the being-online-related consequences for both rights at stake – the one that benefits and the one enjoyment of which is being limited. That concerns the proportionality analysis and the tests it requires. As a result, the enthusiasm for connectivity should not lead to disregarding the offline availability of rights and freedoms. Another issue is the cost-benefit analysis within the scope of one particular right that its online realisation might bring about. That applies especially to ESC rights like the right to health. In the ESC rights realm, the critical issue becomes the principle of progressive realisation of those rights so that the progress achieved by online services outweighs the detriments caused by it and is not discriminatory.

Perhaps the concept that "[t]he same rights that people have offline must also be protected online", which has dominated the recent international discourse about human rights in cyberspace (Dror-Shpoliansky & Shany 2021, 1253–1256), should become supplemented with two caveats. As the first caveat, we propose: While enabling human rights online, we may not resign from providing them offline if the protection of other rights requires that. That may seem somewhat self-evident. However, not necessarily so, as the recent pandemic crisis revealed, for example, when travellers' obligation to complete the passenger location form upon arrival in Belgium could be fulfilled only through the Internet (Kloza 2024). As the second caveat we propose: While enabling human rights online, we may do that only as far as it leads to genuine and non-discriminatory progress in the realisation of the particular right. However, this kind of in-depth analysis seems so far to be absent in the policy-making process or in the activity of human rights monitoring bodies.

Notes

1 It should be noted, however, that companies are able to create profiles of offline people they know exist and supplement the information with information coming in from various sources, such as friends who are online. See: Dunbar *et al.* (2015).
2 The number of data breaches in healthcare has been on the rise since 2005. See: Seh *et al.* (2020).
3 Nevertheless, it has not been recognised *expressis verbis* in the universal human rights framework. The General Comment no 16 on the right to privacy does not mention the concept, nor the individual communications of the Human Rights Committee (for more: Vaitkunaite 2023). The Universal Human Rights Index, the most comprehensive database of human rights recommendations adopted by the UN Treaty Bodies, Human Rights Council special procedures and within the Universal Periodic Review, discloses only one mention of this concept made by the Independent Expert on the enjoyment of all human rights by older persons. See: IE Older persons (2020, para. 115).

4 For instance, in India. See: Writ Petition (Civil) No 494 of 2012. Although Indian Supreme Court uses the phrasing "informational privacy", it draws parallels with the German Census case of 1983 and the concept of "informational self-determination" (see paras. 207, 241).
5 European Union, Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM/2022/197 final, Article 34.
6 In the Arab Spring countries, social media initially empowered activists but quickly became a tool for repression. Government and military forces transformed platforms like Facebook and Twitter into arenas of harassment and danger for dissidents, leading to arrests and forced exiles. See: Tufekci (2019).
7 World Conference on Human Rights in Vienna, Vienna Declaration and Programme of Action, 25 June 1993.
8 Federal Constitutional Court of Germany, when adjudicating on the permissibility of AI-based software for law enforcement agencies noted that their use

> can also come close to developing a full profile. This is because the software can open up new possibilities of filling in the available information on a person by factoring in data and algorithmic assumptions about relationships and connections surrounding the person concerned.
>
> See: BVerfG (2023)

9 Although anonymised data is no longer considered "personal data", it could potentially be reidentified and linked back to an individual in the future. This likelihood increases with ongoing advancements in datafication of society and increasing computational power.

Bibliography

Books and articles

Borges do Nascimento, I. J., A. B. Pizarro, J. M. Almeida, N. Azzopardi-Muscat, M. A. Gonçalves, M. Björklund, & D. Novillo-Ortiz (2022), Infodemics and Health Misinformation: A Systematic Review of Reviews, *Bulletin of the World Health Organization*, 100(9), 544–561.

Cai, Z., P. Mao, Z. Wang, D. Wang, J. He, & X. Fan (2023), Associations Between Problematic Internet Use and Mental Health Outcomes of Students: A Meta-analytic Review, *Adolescent Research Review*, 8, 45–62.

Choi, H., J. Park, & Y. Jung (2018), The Role of Privacy Fatigue in Online Privacy Behavior, *Computers in Human Behavior*, 81, 42–51.

Clusmann, J., F. R. Kolbinger, H. S. Muti, Z. I. Carrero, J-N. Eckardt, N. Ghaffari Laleh, C. M. L. Löffler, S-C. Schwarzkopf, M. Unger, G. P. Veldhuizen, S. J. Wagner, & J. N. Kather (2023), The Future Landscape of Large Language Models in Medicine, *Communications Medicine*, 3. www.nature.com/articles/s43856-023-00370-1

Dragu, T., & Y. Lupu (2021), Digital Authoritarianism and the Future of Human Rights, *International Organization*, 75(4), 991–1017.

Dror-Shpoliansky, D., & Y. Shany (2021), It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights – A Proposed Typology, *The European Journal of International Law*, 32(4), 1249–1282.

Dunbar, R., V. Arnaboldi, M. Conti, & A. Passarella (2015), The Structure of Online Social Networks Mirrors Those in the Offline World, *Social Networks*, 43, 39–47.

Fatumo, S., T. Chikowore, A. Choudhury, M. Ayub, A. R. Martin, & K. Kuchenbäcker (2022), Diversity in Genomic Studies: A Roadmap to Address the Imbalance. Available at: www.ncbi.nlm.nih.gov/pmc/articles/PMC7614889/, Accessed on 16 May 2024 (published in final edited form as: A roadmap to increase diversity in genomic studies, *Nature Medicine,* 2022; 28(2)).

Getman, R., M. Helmi, H. Roberts, A. Yansane, D. Cutler, & B. Seymour (2018), Vaccine Hesitancy and Online Information: The Influence of Digital Networks, *Health Education & Behavior*, 45(4), 599–606.

Ibrahim, H., X. Liu, N. Zariffa, A. D. Morris, & A. K. Denniston (2021), Health Data Poverty: An Assailable Barrier to Equitable Digital Health Care, *The Lancet. Digital Health*, 3(4), 260–265.

Kloza, D. (2024), The Right Not to Use the Internet, *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 52. https://doi.org/10.1016/j.clsr.2023.105907

Lin, Q., S. Paykin, D. Halpern, A. Martinez-Cardoso, & M. Kolak (2022), Assessment of Structural Barriers and Racial Group Disparities of COVID-19 Mortality With Spatial Analysis, *JAMA Network Open*, 5(3). https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2789619

Madise, Ü., & P. Vinkel (2011), Constitutionality of Remote Internet Voting: The Estonian Perspective, *Juridica International Law Review*, VIII, 8.

Martino, G. D. S., S. Cresci, A. Barrón-Cedeño, S. Yu, R. Di Pietro, & P. Nakov (2020), A Survey on Computational Propaganda Detection, *arXiv preprint arXiv:2007.08024*.

O'Connell, J., M. Abbas, S. Beecham, J. Buckley, M. Chochlov, B. Fitzgerald, L. Glynn, K. Johnson, J. Laffey, B. McNicholas, B. Nuseibeh, M. O'Callaghan, I. O'Keeffe, A. Razzaq, K. Rekanar, I. Richardson, A. Simpkin, C. Storni, D. Tsvyatkova, J. Walsh, T. Welsh, D. O'Keeffe (2021), Best Practice Guidance for Digital Contact Tracing Apps: A Cross-disciplinary Review of the Literature, *JMIR Mhealth Uhealth*, 9(6), e27753. https://doi.org/10.2196/27753. PMID: 34003764; PMCID: PMC8189288.

Pandit, J. A., J. M. Radin, G. Quer, et al. (2022), Smartphone Apps in the COVID-19 Pandemic, *Nature Biotechnology*, 40, 1013–1022.

Pawelczyk, B. (2018), Art. 12. Prawo do ochrony zdrowia, in: Z. Kędzia & A. Hernandez-Połczyńska (eds), *Międzynarodowy Pakt Praw Gospodarczych, Socjalnych i Kulturalnych*. Komentarz, C.H. Beck, Warszawa.

Pehora, C., N. Gajaria, M. Stoute, S. Fracassa, R. Serebale-O'Sullivan, C. T. Matava (2015), Are Parents Getting it Right? A Survey of Parents' Internet Use for Children's Health Care Information, *Interactive Journal of Medical Research*, 4(2). https://pubmed.ncbi.nlm.nih.gov/26099207/

Peralta, A. F., M. Neri, J. Kertész, & G. Iñiguez (2021), Effect of Algorithmic Bias and Network Structure on Coexistence, Consensus, and Polarization of Opinions, *Physical Review E*, 104(4), 044312.

Radtke, T., T. Apel, K. Schenkel, J. Keller, & E. von Lindern (2022), Digital Detox: An Effective Solution in the Smartphone Era? A Systematic Literature Review, *Mobile Media & Communication*, 10(2), 190–215 (Special Issue: Digital Wellbeing in an Age of Mobile Connectivity).

Reglitz, M., & A. Rudnick (2020), Internet Access as a Right for Realizing the Human Right to Adequate Mental (and other) Health Care, *International Journal of Mental Health*, 49(1), 97–103.

Saul, B., D. Kinley, & J. Mowbray (2014), *The International Covenant on Economic, Social and Cultural Rights: Commentary, Cases, Materials*. Oxford University Press, Oxford.

Seh, A. H., M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal, R. Kumar, & R. A. Khan (2020), Healthcare Data Breaches: Insights and Implications. *Healthcare (Basel, Switzerland)*, 8(2), 133.

Stoykova, R. (2023), Encrochat: The Hacker with a Warrant and Fair Trials? *Forensic Science International: Digital Investigation*, 46, 301602.

Sun, N., K. Esom, M. Dhaliwal, & J. J. Amon (2020), Human Rights and Digital Health Technologies, *Health and Human Rights Journal*, 22(2), 21–32.

Suziedelyte, A. (2012), How Does Searching for Health Information on the Internet Affect Individuals' Demand for Health Care Services?, *Social Science & Medicine*, 75(10), 1828–1835.

Tremblay, L. B. (2014), An Egalitarian Defense of Proportionality-based Balancing, *International Journal of Constitutional Law*, 12(4), 864–890.

Tufekci, Z. A. (2019), Response to Johanne Kübler's A Review of Zeynep Tufekci – Twitter and Tear Gas: The Power and Fragility of Networked Protest (2017, New Haven: Yale University Press). *International Journal of Politics, Culture, and Society*, 32, 365–369.

Vaitkunaite, I. (2023), *Reinventing the Right to Privacy Towards Full-Fledged Informational Self-Determination A doctrinal study of the evolutive interpretation of Article 17 of ICCPR*, MA Thesis, Lund University.

Yu, J., & S. Meng (2022), Impacts of the Internet on Health Inequality and Healthcare Access: A Cross-Country Study, *Frontiers in Public Health*, 10. www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2022.935608/full

Yuste, R., & T. De La Quadra-Salcedo (2023), Neuro-Rights and New Charts of Digital Rights: A Dialogue Beyond the Limits of the Law, *Indiana Journal of Global Legal Studies*, *30*(1), 15–37. https://doi.org/10.2979/gls.2023.a886161

Documents

BVerfG, Judgment of the First Senate of 16 February 2023 – 1 BvR 1547/19.

BVerfG, Order of 15 December 1983 – 1 BvR 209/83.

CESCR, General Comment No 14 (2000), The right to the highest attainable standard of health (article 12 of the International Covenant on Economic, Social and Cultural Rights), E/C.12/2000/4, from 11 August 2000.

CRC, General Comment No 15 (2013a) on the right of the child to the enjoyment of the highest attainable standard of health (art. 24), CRC/C/GC/15, from 17 April 2013.

CRC, General Comment No 17 (2013b) on the right of the child to rest, leisure, play, recreational activities, cultural life and the arts (art. 31), CRC/C/GC/17, from 17 April 2013.

CRC, General Comment No 20 (2016) on the implementation of the rights of the child during adolescence, CRC/C/GC/20, from 6 December 2016.

ECtHR (2015), *Zakharov v. Russia*, 47143/06, 4 December 2015.

ECtHR (2023), *L.B. v. Hungary*, 36345/16, 9 March 2023.

European Union, Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM/2022/197 final.

HRC, General Comment No 35 (2014) on ICCPR article 9 on liberty and security of person.

IE Older persons, Report of the Independent Expert on the enjoyment of all human rights by older persons: Visit to New Zealand, A/HRC/45/14/ADD.2, 13 July 2020.

Inter-American Court of Human Rights, Members of the Corporation Lawyers Collective "José Alvear Restrepo" (CAJAR) Vs. Colombia, 18 March 2024.

UPR (Universal Periodic Review), 2021-2023. Recommendations toward Uganda (from Canada). A/HRC/50/11, 2022, para. 123.132; Recommendation toward Gabon (from Estonia), A/HRC/53/6, 2023, para. 136.83. Recommendation toward Morocco (from Greece), A/HRC/52/7, 2023, para. 57.109; Recommendations toward the Netherlands (from Cuba), A/HRC/52/16, 2022, para. 147.121. Recommendation toward Nauru (from France), A/HRC/47/17, 2021, para. 99.94.

World Conference on Human Rights in Vienna, Vienna Declaration and Programme of Action, 25 June 1993.