

ENNAN RUSLAN

*National University “Odesa Law Academy”,
Associated Professor at the Department of Intellectual Property Law, PhD*

NEW DIGITAL RIGHTS IN THE DIGITAL ERA

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. 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.

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. 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*). Also in Italy the right to disconnect was introduced in labor law and in Germany the employment ministry banned managers from contacting staff outside working hours. 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.

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’, 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. 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, 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. This can result in insomnia, concentration problems and fatigue. Compulsive and excessive use of social media that is difficult to control can cause considerable problems with regard to well-being and health. In some countries even bootcamps ('digital detox') exist for people addicted to social media. 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.

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.

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. 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. A right to internet access can contribute to freedom of speech and to closing the digital divide, 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.

In most developed countries, large percentages of the population have internet access, so this may not be a big issue. However, it may be an issue for different groups in society⁴⁶ for different reasons. 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. 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.

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.

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.

For the opposite, a right not to know, 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 not know about this does not have to notify this (and therefore cannot notify this).

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.

A right to change your mind could perhaps be seen in the fundamental right to freedom of thought or the freedom of expression, 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. 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.

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, 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.

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. A right to be forgotten may be expected to entail much more than the right to have some data erased. 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.

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. 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.

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.

Ключові слова: цифрові права, цифрові технології, цифрова ера, право бути в автономному режимі, право на доступ до Інтернету, право не знати, право змінити своє рішення, цінність особистих даних.

Key words: digital rights, digital technology, digital era, 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.

КИРИЛЮК АЛЛА ВОЛОДИМИРІВНА

*Національний університет «Одеська юридична академія»,
доцент кафедри права інтелектуальної власності та патентної юстиції,
кандидат юридичних наук, доцент*

ТЕОРЕТИЧНІ ПОЛОЖЕННЯ ЗАХИСТУ АВТОРСЬКИХ ПРАВ У МЕРЕЖІ ІНТЕРНЕТ

Сьогодні Інтернет можна назвати найзручнішим постачальником свіжої інформації з будь-якої точки планети, у тому числі й зображень, текстів, творів літератури, музики, образотворчого мистецтва, кіно та інших, що охороняються авторським правом. Звідси, на наш погляд, випливають дві найактуальніші проблеми.

По-перше. Розміщення матеріалів в мережі Інтернет та надання відкритого доступу до них без дозволу правоволодільця. Багато хто вважає,