DEBATES AND
DOCUMENTS COLLECTION,
OCTOBER 2024

37

EMERGING TECHNOLOGIES

SOCIETAL AND DEMOCRATIC CHALLENGES

LUCIE DU PASQUIER (ED.)

FONDATION
JEAN MONNET
POUR L'EUROPE

Table of Contents

Information Intermediaries and IT Service Providers Shall Be Made Liable

Sylvain Métille
Professor of data protection and IT criminal law at the University of Lausanne
Member of the Bar (HDC)
August 2024

Online services have changed considerably since Tim Berners-Lee invented the Internet in 1989.[129] We are a long way from the initial ideals of freedom and knowledge sharing. Today there is a huge volume of information on the web, often of uneven quality, and users can see only what information intermediaries – search engines, social media platforms, multimedia platforms, microblogging and instant messaging services, and other hybrid services – choose and select to display.

These intermediaries facilitate the access to information, and in that sense play a positive role, including by enabling people to form opinions – essential for the proper functioning of any democratic space. For instance, information intermediaries make it possible for local newspapers to reach a broader audience at no additional cost or let an individual publish content even if they do not have any IT infrastructure at all.

Contrary to the first hosting providers in the early days of the Web, who did nothing more than giving customers a virtual space for posting content, today's information intermediaries, have a much broader range of capabilities, especially when it comes to the content posted on their platforms. They can decide what content should be seen by whom, what content is worth promoting and what content will be lost among thousands of others.

For example, a search engine does not simply give access to content supplied by a third party. It also suggests ways to reword the search, uses extracts from other websites directly on its home page to answer the question without leaving the search engine's site or will recommend specific websites because they are deemed most relevant or because those companies have paid the most for advertising.

A far cry from the early days of the Web, when these intermediaries were simply passive, neutral conduits for information, they have become veritable gateways to information.[130] They play a fundamental role in our society but are subject to little oversight, particularly in terms of how they control information. Yet the slippage is well known, as the consequences of the spread of harmful anti-Rohingya content in Myanmar, amplified by Facebook's algorithms, sadly showed back in 2017.[131]

The transparency some intermediaries lack, most notably with regard to the rules they use for deciding when to keep or delete content or a user's account, is also quite alarming. X (formerly Twitter) demonstrated this when it closed and then reopened Donald Trump's account or when it placed only a small team in charge of content moderation.[132]

EU regulators have passed a "digital services package" in response to the dominant position held by information intermediaries and to the proliferation of some content that seriously harm the public sphere, such as disinformation or hate speech. The package includes the Digital Services Act (DSA) and the Digital Markets Act (DMA), which are designed to establish greater accountability among these intermediaries.

To better combat the proliferation of illicit content, the DSA now sets a number of transparency obligations for large online platforms that also strengthen users' rights. As for the DMA, it introduces requirements for companies considered to be gatekeepers, in regard to their economic power, in order to prevent market abuse. So far, six companies have been designated by the European Commission as gatekeepers: Alphabet (Google's parent company), Amazon, Apple, ByteDance (TikTok's parent company), Meta (Facebook's parent company) and Microsoft.[133]

Accountability for technology companies is a broader issue that concerns the entire digital space. It gave rise to some debate about ten years ago, with plans for a 'personality' for robots, which would allow the designers of these machines to be exempt from liability in exchange for taking out civil liability insurance.[134] These proposals came to nothing because so few robots are used by the general public, but also because of the fear that designers would be completely immune.

The issue of accountability will undoubtedly come up again in the light of recent technological developments and the increasingly widespread use of artificial intelligence (AI) – a technology we are just beginning to understand.

Although the Swiss legislator has not yet decided how it wishes to regulate the use of AI,[135] the Federal Act on Data Protection (FADP) already imposes obligations of transparency and human control in the case of automated decision (see Article 21). There is also little doubt that anyone using an AI driven tool is responsible for it.

The European Parliament introduced the Artificial Intelligence Act in March 2024, which classifies AI systems into four categories based on their level of risk. Those with an unacceptable degree of risk are prohibited. Those classified as high risk must comply with numerous requirements, while moderate risk systems must meet mainly transparency obligations. Those considered to have only minor risks are not subject to any particular requirements.

Currently, the IT world has become accustomed to operating with very little liability, even massive exclusions of any sense of responsibility – something that would be unthinkable in any other sector. For example, whereas goods purchased from a vendor often come with a mandatory three-year warranty (see Article 197 of the Swiss Code of Obligations), it is standard for software to be delivered with a warranty of only a few days, even if it is expensive and tailor-made. Users must purchase a separate maintenance agreement in which suppliers undertake to fix any errors in return for the payment of fees. Furthermore, these maintenance agreements typically contain an obligation of means (or best efforts) rather than an obligation of result.

At the same time, Internet users have become accustomed to consuming content quickly and, especially, for free. However, this costlessness is only apparent. Users pay for it by agreeing to watch advertisements, share their personal data, or test or train programs that are still in a preliminary stage. Also, content services are generally provided on an as-is basis – not backed by a warranty or liability, or with very limited liability (sometimes just a few Swiss francs). But all this seems acceptable, since the service is free. Who would dare demand warranties for something they receive at no cost? And even when they pay for a licence, the conditions are very unfavourable and cases of liability remain very limited.

Yet, that could change. The European Commission, for example, wants to impose common cybersecurity obligations for all connected devices through the Cyber Resilience Act[136] and adapt the Product Liability Directive to the digital age.[137] In the same vein, the Biden-Harris administration has announced its intention to propose legislation that would make companies that sell software without sufficient cyber security liable.[138]

While these examples concern foreign jurisdictions, we are likely to see this new approach to regulation reflected in Swiss law. Not only has the Swiss legislator often passed provisions similar to those in other countries, but the broad extraterritorial scope of foreign laws could also affect entities

129 To learn more about the origins of the web, see: https://home.cern/science/computing/birth-web.

130 Riordan, Jaani. *The Liability of Internet Intermediaries*, thesis, Oxford 2016, p. 8.

131 See:https://www.amnesty.org/en/latest/news/2022/09/myanmar-facebooks-systems-promoted-violence-against-rohingya-meta-owes-reparations-new-report/.

132 The European Commission opened formal proceedings against X to assess potential breaches in the areas of transparency, content moderation and more. See the European Commission press release (18 December 2023): https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709.

133 See the European Commission press release (6 September 2023): https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328.

134 Set forth in Article 59c of the European Parliament resolution of 16 February 2017. The Resolution is available here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017IP0051.

135 The Federal Council instructed DETEC to examine possible approaches for regulating AI and issue a report by the end of 2024. See the Federal Council press release (22 November 2023): https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-98791.html.

136 Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM(2022) 454 final).

137 Proposal for a Directive of the European Parliament and of the Council on liability for defective products (COM(2022) 495 final).

138 The Biden-Harris administration announced a national cybersecurity strategy in March 2023; see: https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

located in Switzerland.[139] Finally, as we have seen, the Swiss legislator is not totally indifferent to these issues, and it will be particularly important to monitor developments relating to draft regulations on major communication platforms[140] and AI.[141]

The protection of personal data and the fundamental rights of Internet users are fairly well taken into account by recent data protection laws.

Switzerland's FADP went into effect on 1 September 2023, while the General Data Protection Regulation has been protected European Economic Area residents since 2018.

As for the Swiss Criminal Code (SCC), it has long contained provisions against offences committed online, including offences against personal honour (Article 173 *et seq.*), various kinds of fraud (Article 146), data theft and hacking (Article 143 *et seq.*) and pornography (Article 197). The government recently added identity theft (Article 179decies) and pornodisclosure (Article 197a),[142] thus further enhancing the protection of injured parties.

That said, some laws have proven to be inefficient. For example, the distribution of pornographic content to minors is a criminal offence punishable by up to three years in prison,[143] yet this provision is regularly broken without any major reaction. Of course, it's not easy to set up monitoring systems that don't also infringe on users' privacy, but we could still require that the websites offering such content take appropriate measures to comply with the law and protect the youth.

All in all, the substantive law appears to be fairly satisfactory, and it is the application of the law that needs to be improved. Although data protection laws guarantee the rights of data subjects, the application of these laws sometimes remains theoretical, and data subjects must act alone to ensure that their rights are respected.

Greater action by the supervisory authorities would be welcome. Greater action by the supervisory authorities would be welcome.

The criminal prosecution authorities (justice and police) have to deal with an ever-increasing number of offences committed in cyberspace, even though their resources have hardly been adapted. The essentially decentralised nature of the Internet and information intermediaries means that international investigations are required, as well as cooperation with states that are sometimes far away or whose concerns may differ fundamentally from our own.[144]

139 Sury, Ursula. Digital Services Act (DSA), *Informatik Spektrum* 45 2022, p. 266.

140 See the Federal Council press release (5 April 2023): https://www.bakom.admin.ch/bakom/en/homepage/ofcom/ofcom-s-information/press-releases-nsb.msg-id-94116.html.

141 See the Federal Council press release (22 November 2023): https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-98791.html.

142 Went into effect on 1 July 2024.

143 Article 197.1 of the SCC.

144 The Federal Council brought up this issue as it pertains to online hate speech in a report published on 15 November 2023 (*Discours de haine. La loi présente-t-elle des lacunes?*, p. 12).

Bibliography

AMNESTY INTERNATIONAL. *Myanmar: Facebook's systems promoted violence against Rohingya; Meta owes reparations*, 29 September 2022. Available at: https://www.amnesty.org/en/latest/news/2022/09/myanmar-facebooks-systems-promoted-violence-against-rohingya-meta-owes-reparations-new-report/

CERN. *The birth of the Web*. Available at: https://home.cern/science/computing/birth-web

Civil Law Rules on Robotics. "European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robots (2015/2103(INL))" in. *Official Journal of the European Union*, 18 July 2018, 19 pp. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017IP0051

Federal Council. *Report supports proposed measures to counter the spread of illegal hate speech*. 14 November 2023. Available (only in French, German and Italian) at: https://www.bakom.admin.ch/bakom/en/homepage/electronic-media/media-policy/news-and-background/hate_speech.html

Press Release of the European Commission. *Commission opens formal proceedings against X under the Digital Services Act*, Brussels, 18 December 2023. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709

Press Release of the European Commission. *Digital Markets Act: Commission designates six gatekeepers*, Brussels, 6 September 2023. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328

Press release of the Federal Council. *Federal Council examining regulatory approaches to AI*, 22 November 2023. Available at: https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-98791.html

Press release of the Federal Council. *Federal Council seeks to regulate large communication platforms*, 5 April 2023. Available at: https://www.bakom.admin.ch/bakom/en/homepage/ofcom/ofcom-s-information/press-releases-nsb.msg-id-94116.html

RIORDAN, Jaani. *The Liability of Internet Intermediaries,* Oxford University Press (Thesis), 2016, 696 pp.

SURY, Ursula. "Digital Services Act (DSA)" in. *Informatik Spektrum,* vol. 45, n°4, 2022, pp. 265-266

The White House. *National Cybersecurity Strategy,* mars 2023, Washington, 39 pp. Available at: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf