cife POLICY PAPER
NOTE DE RECHERCHE
N° 148

Katharina Sigwald - 12 June 2023

Extremism in Digital Spheres: Can European Union Directives curb it?

Introduction

The Internet is a place of sheer wonder and light-speed innovation. It offers unlimited knowledge, connections to every corner of the world, and plays a crucial role in our day-to-day communication. Beyond its unique positive capabilities, and perhaps even because of those features, it also possesses negative characteristics. From a holistic standpoint: little research has been made on the psychological effects of the overwhelming amount of information exposed to users every day. There have been efforts though, to regulate and understand other challenges, such as secluded 'filter bubbles', which furnish and profit from disinformation and may lead to extremist ideologies.

In light of increasing violent extremist attacks in the European Union (EU), the European Council updated its 2020 conclusion on external actions in the field of counter-terrorism (CT) and the prevention of radicalisation leading to violent extremism (P/CVE). An interesting new aspect proposed by the 2020 conclusion is that violent extremism continues to evolve, increasingly with the help of online activities (URL 1).

Starting in 2016, the EU introduced different regulations for the Internet. But regulations go as far back as the adoption of the 2000 e-Commerce Directive, aiming to harmonise preexisting rules on electronic trade, including the "liability of service providers" (Giugni & de Santis 2021: 6). Non-neutral entities were obliged to flag or take down illegal content. The e-Commerce Directive is considered obsolete today, as it has been outpaced by the fleet-footed development of the Internet.

In 2016 the EU introduced the General Data Protection Regulation (short GDPR), which remains a significant step forward in the regulation of sensible data on the Internet. It may only have a limited impact on the prevention of extremism, but it has laid the ground for further regulatory incentives and the EU's dominant position in global internet regulations. In 2020 the European Commission proposed the Digital Services Act (DSA) and the Digital Markets Act (DMA). The conclusion came into force in 2022 and must be implemented by 2024.

Parallel to the introduction of the DSA/DMA, a new research centre, with the beginning of 2023, the European Centre for Algorithmic Transparency (ECAT), seeks to contribute to a safer World-Wide-Web (www) by scientific and technical expertise (URL 2).

Extremism by proxy

Extremism describes a religiously or politically motivated ideology or worldview. Extremist ideologies can lead to radicalism and, in turn, to violent extremism. In their 2022 Situation and Trend Report, Europol identifies the following extremist groups which have attempted or successfully carried out attacks: Right Wing Extremism, Left Wing & Anarchist Extremism, Jihadist Extremism, Ethno-Nationalist, and Separatist Extremism (URL 3). A defining feature of extremist groups is that social networks are vital for a group to stay connected and to exchange their views. The Internet has proven to be a practical sphere to enhance these features, as algorithms might create 'echo-chambers' in which individuals mutually affirm their inherent beliefs without being questioned or criticized (URL 4).

In order to understand extremism reproduced on the www, one must look at algorithms, which are at the core of creating 'filter-bubbles'. Algorithms are, of course, not the sole factor for easily propagating extremist views. In fact, one of the Internet's most cherished and loathed characteristics, namely 'virality', allows messages, correct or un/intentionally incorrect, to travel quickly and far, reaching a large audience (Nardon & Rust 2021: 28).

Strictly speaking, the Oxford Dictionary describes an Algorithm as a "a process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer" (Concise Oxford

* **Katharina Sigwald** *works as an Office and Project coordinator at the Austro-French Centre for Rapprochement in Europe. Ms. Sigwald has a bachelor's degree in Social and Cultural Anthropology and Transcultural Communications (working languages German, English, French) respectively.*

Dictionary 1999). Algorithms may have the task of filtering certain unwanted content on social media websites, but they also learn from human decision-making in order to reproduce them. In the case of extremism, an algorithm functioning as a recommender system may show further extremist content after little interaction with the initial content (Wagner 2016: 6). One may find oneself engulfed by similar videos, pictures, podcasts, reels, etc. after a few seconds of active viewing time. To a certain degree this process might resemble a 'rabbit-hole' in that one extremist video leads to another and another, falling deeper into a thematic tunnel, which leaves little room to question or criticise the proposed opinions.

It seems as though algorithmic decision-making is opaque and incomprehensible (Neyland 2019: 5). Another problem is that algorithmic biases are only visible on the larger scale, rather than the small scale. It is because of this, among other things, that experts are calling for algorithmic transparency, thus the disclosure of algorithmic patterns and output, to open and modify this 'black box' (Grimmelikhuijsen 2023).

Offline Interventions

The EU has decided on many policies to combat extremism offline. For example, the introduction of the Radicalisation Awareness Network (RAN), the EU's Security Union strategy 2020-2025, and the new Counter-Terrorism Agenda (URL 4). As well as RAN and EU conclusions in general, Europol plays a vital role in preventing extremist violent acts. RAN describes frontline practitioners, such as civil society representatives, social workers, youth workers, teachers, etc., working with people who are vulnerable to radicalisation or were already radicalised (URL 5). These groups represent a very important puzzle in combating radicalisation, both within and outside of the Internet (URL 1).

DSA/DMA

Since the General Data Protection Regulation (GDRP) the EU has been considered one of the leading practitioners of the regulatory force for digital services. In December 2020, the European Commission published a broad package of regulations for the European Parliament and the Council, encompassing the Digital Services Act (DSA) and, as a second part, the Digital Market Act (DMA). The Digital Services Act short DSA aims to better protect consumers and their fundamental rights online, to create transparency and accountability for online platforms, and to promote innovation, growth, and competitiveness in the single market (URL 8).

In October 2022 the proposals came into force and will be ratified in February 2024. The regulations are applicable throughout as well as outside the EU and do not require implementation by national law. In fact, they intentionally override certain national laws already in place so as to find a harmonised legal basis on which national laws can be built (such as in France, Germany, Denmark, Austria etc.; URL 7). However, each member state is called upon to entrust a Digital Services Coordinator or a ministry with the task of coordinating the implementation of the regulation (URL 7).

Different rules apply, depending on the role, size, and impact of a platform. Platforms are organized into four categories: intermediary services that offer network infrastructure, hosting services such as cloud and web hosting services, online platforms that introduce sellers and consumers (online marketplaces but also social media platforms), and very large online platforms, which pose a particular risk in distributing illegal content and thus will be subject to stricter requirements (URL 6).

In relation to extremism, the following concrete measures taken by the DSA are of most interest: mechanisms to flag illegal content by users in cooperation with the platforms; the possibility for users to challenge a platform's content moderation decisions; transparency of an assortment of issues, such as algorithmic decision making, content recommendation systems and targeting (URL 6).

ECAT

To scientifically enforce the DSA, the European Commission launched a new research programme within the framework of the Joint Research Centre (JRC) in 2022: the European Centre for Algorithmic Transparency (ECAT) with its seat in Seville, Spain. On 18 April 2023, experts at the Joint Research Centre, the European Commission, Universities, and political figures, as well as the team from ECAT, presented the centre to the public, paradoxically with a few technical issues (URL 2).

ECAT will function as a research centre for AI, Algorithms, and everything related to supporting the implementation of the DSA/DMA, as well as a facilitator to society. The presenters highlighted the need to research the black box of these systems for the good of humanity and global society. For this, talented minds should come together, not working in rivalry against private companies, but together, as with the European Organisation for Nuclear Research (CERN). The Presenters similarly hoped that the DSA/DMA might provoke another Brussels effect.

Conclusion

As the DSA is not fully employed yet, it is difficult to predict how it will play out. As important as these regulatory steps are, there are uncertainties regarding the staggering pace at which AI and Algorithms are evolving, uncertainties as to whether the regulation will be outdated by the time it comes into force. Simultaneously, experts question if the DSA & DMA can "remedy existing asymmetries of the digital space" (Obendiek 2021: 4). For one, EU regulations are often only voluntary or imposed with soft standards, in the case of the DSA legal uncertainties could be the outcome. Another mentioned persistent issue is the lack of adequate research funding of Algorithms and AI (Giugni & de Santis 2021).

Much has been decided in the last 20 years. Though only recently negative features of AI and Algorithms have been acknowledged as possibly dangerous, the EU has made a big impact in the international arena by flexing its regulatory muscles with the GDPR and the future implementation of the DSA/DMA. It remains to be seen how much impact the DSA/DMA might have and what steps still lay ahead to address the problem of extremism produced by the Internet. Whatever the outcome, the DSA/DMA is perceived as a step in the right direction which will probably leave its mark on a global scale.

Bibliography

URL 1: European Council website. Council Conclusion on EU External Action on Preventing and Countering Terrorism and Violent Extremism, 16 June 2020.
URL 2: European Commission website. European Centre for Algorithmic Transparency.
URL 3: Europol. Terrorism Situation and Trend Report 2022.
URL 4: European Parliament News. Radicalisation in the EU: what is it? How can it be prevented, 27 January 2021.
URL 5: European Commission website. About Radicalisation Awareness Network (RAN).
URL 6: European Commission website. The Digital Services Act: ensuring a safe and accountable online environment.
URL 7: Österreichisches Bundeministerium website. Digital Services Act.
Lilia Giugni & Chiara de Santis, Naming it, fighting it: a multi-level analysis of digital gender-based violence, 25 February 2021.
Laurence Nardon & Siméon Rust, États-Unis/Europe : sept enjeux du numérique, 7 July 2021.
Concise Oxford Dictionary. Oxford: Oxford University Press. 1999 (10th ed.).
Ben Wagner, Algorithmic regulation and the global default: Shifting norms in Internet technology, 22 March 2016.
Neyland, Daniel. The Everyday Life of an Algorithm. 2019. Cham: Springer International Publishing Imprint: Palgrave Pivot, 2019.
Grimmelikhuijsen, Stephan. "Explaining Why the Computer Says No: Algorithmic Transparency Affects the Perceived Trustworthiness of Automated Decision- Making." Public Administration Review 83, no. 2 (2023).
Anke S. Obendiek. Take back control? Digitale Souveränität und Europas digitale Zukunft, 11 May 2021.

Rédaction: Laurent Baechler et Aline Palige
Policy Paper / Note de recherche est publiée par le Centre international de formation européenne, association dont le siège est 81, rue de France, F-06000-Nice.

www.cife.eu

Ce projet a été financé avec le soutien de la Commission européenne.
Cette publication (communication) n'engage que son auteur et la Commission n'est pas responsable de l'usage qui pourrait être fait des informations qui y sont contenues.

Avec le soutien du programme Erasmus+