Chapter VI

Disinformation in the Regulations of Selected Countries

KATARZYNA CHAŁUBIŃSKA-JENTKIEWICZ

Abstract Modern democratic legal and political systems, within which public space should serve the free exchange of opinions, are much less able to fulfil their social function as a result of the technological revolution of the 21st century. Media systems have evolved considerably, in which the recipients of messages, who are now also active participants in the social universe of communication, play a fundamental role. The multitude of issues concerning the new sphere of social discourse mobilises legislators at national and regional level to take reasonable care of the legal basis for countering the numerous threats. The main factors disrupting communication are the manipulation and disinformation of messages, deliberately and intentionally formatted for the interests of external actors and by participants introduced at the initiative of external actors. The main research challenge of this article is to analyse the legal arrangements for disinformation in the world. In the light of the current legal solutions, the research objective of the paper should be considered valuable not only from a theoretical, scientific point of view, but also in terms of increasing in practice the possibilities of systemic solutions in the area of threats concerning the security of the individual-citizen in the digital world. The article is based on materials from the author's book entitled 'Legal Limits of Disinformation in Social Media. Between Freedom and Security' (Publisher: Adam Marszałek: Toruń 2023).

Keywords: • cyber attacks • disinformation • freedom of expression • media

CORRESPONDENCE ADDRESS: Katarzyna Chałubińska-Jentkiewicz, Ph.D., Associate Professor, Kozminski University, College of Law, ul. Jagiellonska 57/59, 03-301 Warszawa, Poland, e-mail: kasiachalubinska@gmail.com, ORCID: 0000-0003-0188-5704.

https://doi.org/10.4335/2024.2.6 ISBN 978-961-7124-25-5 (PDF)
Available online at http://www.lex-localis.press.

1 General comments

Disinformation messages are a global problem. Countries are trying to implement their legal and technical solutions to tackle disinformation. As a result – based on different rationales depending on the political system, the nature of governments, and the specificity of the problems related to information disseminated on the Internet – attempts are made to introduce legal regulations regarding responsibility for disinformation activities and mechanisms to influence this type of content and to possibly counteract the dissemination of and access to content deemed to be untrue or to violate certain standards or third-party rights. The selected legal systems presented in the article show the diversity of approaches and the lack of a uniform system of legal solutions, which stems from evident geopolitical, cultural or national differences. However, common and unidirectional regulatory trends can also be observed – especially those that touch on such sensitive elements as fighting against disinformation activities in political advertising and during the election period. Undoubtedly, the events during the elections in the USA and France, and during the referendum in the United Kingdom, indicated the need to move in a regulatory direction – not only in the systems of the countries affected by this type of disinformation, and regardless of the legal culture and administrative and organisational system existing in a given country. It should, therefore, be assumed that the shape of the adopted regulations usually also reflects the specificity of the legal systems and political systems of the jurisdictions in which they were introduced, hence the different regulations of similar problems and the limited transferability of solutions between significantly different jurisdictions (Chałubińska-Jentkiewicz, 2023: 425–425).

2 Australia

The spread of disinformation via the Internet, especially via social media platforms, is recognised as a severe problem in Australia. A global survey conducted in early 2018 showed that trust in the media in the country was at a record low of just 31%, and consumers said they struggled to tell the difference between fake news and facts. Over the past two years, the Australian Government and Parliament have taken several actions relating to protecting democratic systems from interference, including cyber attacks and the spread of disinformation via the Internet. Legislative actions have included strengthening the requirements for authorisation statements for campaign advertisements under election law, with the requirements specifically extended to social media pages and posts. New criminal offences were introduced that concern acts of foreign interference that affect the political or governmental process, the exercise of democratic political rights or duties, or undermine national security. In addition, a new Foreign Influence Transparency Registry has been created, and persons engaging in communications activity in Australia on behalf of a foreign principal, to exert political or governmental influence, must make a statement, also available on social media. Legislation passed in April 2019, following the attacks in Christchurch, New Zealand, requires social media entities to promptly remove abhorrent violent material. Liability for the offence applies to individuals and companies responsible for hosting online content.

Over the past two years, legislative reforms that may affect social media platforms and users have sought to increase the transparency of political advertising, to introduce new offences relating to foreign interference and the sharing of information affecting national security, to establish a registration system and disclosure requirements where communication is made on behalf of a foreign principal, and to impose a new requirement on online companies to remove "abhorrent violent material". The Australian Government introduced the Electoral and Other Legislation Amendment Bill in March 2017. The Bill was enacted in September 2017, and the amendments came into force in March 2018. The Bill aligns election authorisation requirements with modern communication channels, requires all paid election advertising (involving distribution or production) to be authorised, regardless of the source, and ensures that the duty to authorise election and referendum matters rests primarily with those responsible for the decision to provide them, and replaces the current criminal non-compliance regime with a civil penalty regime to be administered by the Australian Electoral Commission. The requirements for the authorisation of political advertising in Australia are contained in XXA Commonwealth Electoral Act 1918 (Cth) (https:/erma. cG753-PB; JSCEM, The 2016 Federal Election: Interim Report on the Authorisation of Voter Communication (Dec. 2016)25).

In April 2019, the Australian Parliament passed legislation establishing new offences in the Criminal Code that require Internet, hosting or content service providers (including social media platforms) to ensure the "prompt removal" of "abhorrent violent material that can be accessed in Australia" and to provide details of such material that was found in Australia to the Australian Federal Police. "Abhorrent violent material" is defined as material that records or transmits abhorrent violent behaviour and is material that "reasonable persons would regard as being, in all circumstances, offensive". It must also be produced by a person who has engaged in violent conduct or who has "aided, abetted, counselled or procured or in any way knowingly participated in abhorrent violent conduct". The offence of failing to remove abhorrent violent material is punishable by imprisonment for up to three years or a fine of up to AU$2.1 million (approximately US$1.47 million) in the case of an individual or a fine of up to AU$10.5 million (approximately US$7.32 million) or 10 per cent of annual turnover, whichever is greater if the offender is a legal entity (Criminal Code Amendment https://perma.cc/UV8K-FHD [accessed on: 21/08/2022]).

3 People's Republic of China

Although the Constitution of the People's Republic of China (PRC or China) declares that citizens enjoy freedom of speech and freedom of the press, these freedoms are not institutionally protected in practice. Freedom House, in its "Freedom in the World 2019" report, states that China is "home to one of the world's most restrictive media environments and its most sophisticated system of censorship, particularly online" (Freedom House, Freedom in the World China Country Report). In November, the

National Radio and Television Administration released new regulations for the country's massive live-streaming industry, which features around 560 million users. The regulations include requirements that platforms notify authorities ahead of celebrity and foreigner appearances, and that they promote accounts embodying core socialist values. The administration also said it would enforce the new regulations during a clean-up campaign in December, during which it would shut down platforms that do not comply (Chiu, 2020). Censors increasingly target "self-media", i.e., the category including independent writers, bloggers, and social media celebrities. Overall, tens of thousands of these accounts have been shut down, delivering a major blow to one of the few remaining avenues for independent and critical news and analysis. The authorities apply pressure on Chinese Internet companies to tightly enforce censorship regulations or risk suspensions, fines, blacklisting, closure, or even criminal prosecution of relevant personnel. Such pressure has intensified under the Cybersecurity Law, which came into force in 2017. (PRC Cybersecurity Law adopted by the Standing Committee of the National People's Congress on 7 November 2016, effective from 1 June 2017. https://perma.cc/3HAP-D6M [accessed on: 21/08/2022]).

From 10 to 17 June 2020, the Cyberspace Administration of China (CAC) suspended the trending topics list for the popular Sina Weibo micro-blogging service, saying messages on the platform had been "disrupting online communication order" and "spreading illegal information". In March 2021, the CAC reportedly ordered Microsoft's LinkedIn to suspend new sign-ups for 30 days and undergo a self-evaluation for not censoring enough content. The company issued a statement on 9 March that it was "working to ensure we remain in compliance with local law".

Despite strict media regulation, disinformation – or what Chinese law often refers to as "gossip" – still seems to permeate the Internet and social media. Internet regulators are said to have received 6.7 million reports of illegal and false information in a single month in July 2018, with many cases coming from Chinese social media platforms Weibo and WeChat. Pursuant to the 1997 State Council Regulation on Computer Information Network and Internet Security, Protection, and Management, it is prohibited to use the Internet to create, repeat, transmit and broadcast information that threatens the implementation of the constitution, laws and administrative regulations inciting to overthrow the government or socialist system, divide the country or threaten national unification, spreading hatred or discrimination against ethnic groups or threatening their unity, spreading rumours or false information, promoting feudalism, obscene material, pornography, gambling, violence, murder, terrorism or supporting criminal activities, violating personal rights, defaming state organisations, as well as any other activity against the constitution, laws and administrative regulations. In contrast, under the 2000 State Council Regulation, websites in China are not permitted to link to foreign news sites or disseminate news from such sites without separate authorisation. In 2016, in the Cybersecurity Law, China criminalised the creation and dissemination of online rumours that threaten economic and social order. In 2017, the Act on the Administration of Internet News Information Service made it mandatory for online news providers to report news

delivered by government-approved news agencies and present it without tampering with or undermining its content. This is to prevent the introduction of messages on social media platforms that do not come from official sources.

In 2018, it was announced that a regulation would be introduced requiring micro-blogging service providers to establish mechanisms to prevent the spread of rumours. On 15 December 2019, the previous scattered regulations were replaced by a new regulation, the Provisions on Governance of the Network Information Content Ecology, issued by the State Internet Information Office, which came into force on 1 March 2020. The addressees of the new regulation are content creators, platforms and Internet users, and it defines prohibited content as illegal, restricted content as harmful and actively promoted content. The actively promoted content should publicise Xi Jinping's thoughts on socialism with Chinese characteristics for the new era, promote the main policies and political thought of the Chinese Communist Party, as well as core socialist values, enhance the international influence of Chinese culture, respond to social needs, teach taste, style and responsibility, proclaim truth, goodness and beauty, and promote unity and stability. Any content that threatens the national unity and national religious policy or gossip that threatens social or economic order, national honour and interests are recognised as illegal content. Online content creators are obliged to take measures to prevent the creation, repetition or publication of negative information, including the use of exaggerated titles, gossip, inappropriate comments about natural disasters, major accidents or other catastrophes, sexual innuendo, sexually related content, fear-inducing content, and things that would push minors into dangerous behaviour or violate social mores. According to the provisions, online platforms are responsible for overseeing all these restrictions. They must set up mechanisms for everything, from reviewing content and comments to real-time checks and handling gossip online. They should appoint a manager for such activities and improve the related staff. The regulation defines content creators as all persons posting any content online. It also places duties on the creators and managers of online groups and forum community sections. Users of information services, online content creators, and online platforms are not allowed to use them for illegal activities. They are also obliged to actively participate in the ecological governance of network information content, regulate illegal and harmful information on the Internet through complaints and reports, and jointly maintain a healthy network ecosystem.

Despite strict regulation of the media and the Internet, disinformation in this country still seems to permeate the Internet and social media in China. China's law prohibits the publication and online transmission of false information disrupting economic or social order. The law also prohibits other information, such as information that may threaten national security, subvert the socialist system or damage the reputation of others. The dissemination of false information that seriously disturbs public order through a news network or other media is punishable by up to seven years in prison. Network operators are obliged to monitor the information disseminated by their users. When a network operator discovers any information that is prohibited by law, it must immediately stop the transmission of the information, delete it, take measures to prevent its spread, keep

appropriate records and report to the relevant government authority. Social media platforms must be licensed to operate in China. Users must provide service providers with their real full names and other identity details. Specific rules have also been established to regulate online news services. For example, when reprinting news, providers of online news services may only reprint what has been published by official state, provincial or other state-designated news organisations.

As of 1 January 2020, new regulations have come into force, prohibiting the publication of deepfake material without proper marking. Any use of them will have to be clearly marked prominently. Otherwise, the dissemination of such information will be treated as a criminal offence (https://www.reuters.com/article/us-china-technology/china-seeks-to-root-out-fake-news-and-deepfakes-with-newonline-content-rules-idUSKBN1Y30VU[accessed on: 11/12/2019]).

Any service that provides information to online users via the Internet is subject to a regulation under which for-profit Internet service providers must obtain a licence to operate from the state authorities. Non-profit providers must also register with government authorities. The regulation requires ISPs to cooperate with government authorities. For example, service providers must keep records of all information published, including their publication dates, as well as information about users, such as their accounts, IP address or domain name, time spent online, etc. Such records must be kept for 60 days and provided to the relevant government authorities upon request. Users are also required to provide service providers with their real full names and details of their identity. Under the Cybersecurity Act, when delivering information publication services or instant messaging services, service providers must require the identity details of users. Service providers are prohibited from providing the relevant services to those users who fail to perform identity authentication. In cases where service providers fail to authenticate users' identities, competent authorities may order them to take corrective action, suspend their operations, close down their websites, revoke their operational permits or business licenses, or impose a fine of RMB 50,000 to RMB 500,000 (approx. US$ 7,500 to US$ 75,000) on service providers and/or a fine of RMB 10,000 to RMB 100,000 (approx. US$ 1,500 to US$ 15,000) on responsible persons.

Tencent, the operator of China's biggest social media platform WeChat, released a January 2019 report regarding its fight against gossip spread online. According to the report, WeChat intercepted over 84,000 pieces of gossip in 2018. In addition, thousands of "articles" were published through WeChat by government authorities in charge of the Internet, public safety, food and drugs.

4 Russian Federation

In the authoritarian political system of the Russian Federation (RF), power is concentrated in the hands of President Vladimir Putin, who brings together around him loyalist security services, a subservient judiciary, a legislature made up of the ruling party and flexible opposition groups, and above all a controlled media environment. An additional aspect of the functioning of the media market is the rampant corruption that thrives on the close links between officials and organised crime groups.

The Government of the Russian Federation recognises information security as an integral part of national security. Two key documents – the Doctrine of Information Security and the 2017–2030 Strategy for the Development of an Information Society in the Russian Federation – set priorities for information security and identify the main threats and ways to counter them. The Constitution of the Russian Federation contains guarantees of freedom of expression, and various aspects of information integrity, including information on election campaigns, are regulated by federal laws such as the Law on Information, the Law on Mass Media and the Law on Basic Guarantees of Electoral Rights. Recently adopted legislation restricts access to information containing fake news or offensive and disrespectful messages regarding the symbols of the Russian Federation, the Constitution and the authorities. The dissemination of prohibited information is punishable by fines and administrative arrest. The Criminal Code of the Russian Federation contains articles providing for various penalties for disseminating defamatory content. Measures to remove prohibited content and restrict access to websites containing proprietary information were introduced in 2019.

The Russian government has created an open register of fake news sites, with the identification of platforms and their authors. The lower house of the Russian legislator plans to study news aggregators to control the distribution of fake news and disinformation. The Internet and social media are widely accessible and reachable for a large part of the Russian population. According to the statistical website Statista, the number of Internet users in Russia has grown steadily over the past six years, reaching one hundred million users in 2019. According to the same source, the majority of the Russian population uses social media. As of 2017, the most popular social networks in the Russian Federation were YouTube (68%) and VKontakte (61%). For the government of the Russian Federation, information security is an inseparable component of overall national security (Statista, 2019, https://perma.cc/NS4X-ZE3X [accessed on: 21/08/2022]).

The Government's Doctrine on Information Security emphasises the importance of regulating the Internet within the borders of the Russian Federation. It considers all content containing extremist ideology, spreading xenophobia, promoting violent changes to the constitutional order or violating the territorial integrity of the Russian Federation to be a security threat. Based on the principles and priorities outlined in the Doctrine, Russia adopted the Strategy for the Development of an Information Society in the Russian

Federation for 2017–2030 (Resolution of the President of the Russian Federation on Approving Information Security Doctrine (5 December 2016) (in Russian), https://perma.cc/4BEK-4M5R [accessed on: 21/08/2022]). One of the declared objectives of the Strategy is to "create a secure information environment based on information resources that contribute to the dissemination of traditional Russian spiritual and moral values". To pursue this objective, it is planned to amend the legal, regulatory and technological systems to protect the information sphere in Russia by blocking access to and removing prohibited resources (Decree of the President of the Russian Federation on the Strategy for the Development of an Information Society in the Russian Federation for 2017–2030, N 203 (9 May 2017), http://pravo.gov.ru (official legal information portal) (in Russian), https://perma.cc/AQ4H-CE79 [accessed on: 21/08/2022]).

In March 2019, Russia adopted two so-called anti-fake news laws that amended the Federal Law on Information. It introduced provisions establishing a procedure for removing information deemed false and providing for punitive measures for the dissemination of fake news. At the same time, the Law on Information and the Code of Administrative Offences were amended with provisions prohibiting the publication on the Internet of content that insults state symbols, the Constitution and the authorities of the Russian Federation. Some provisions of the Criminal Code provide for penalties for disseminating inaccurate, defamatory and false content (Federal Law on Information, Information Technologies and Protection of Information, No. 149-FZ (27 July 2006) https://perma.cc/86PF-DYTH [accessed on: 21/08/2022).

5 France

Two areas are the subject of French regulation: defamation and fake news, on the one hand, and advertising, including political advertising, on the other. Some laws have been in place for a long time but the emergence of social media has created challenges that have prompted the recent adoption of new ones. Freedom of expression is considered a "fundamental freedom" in France. It is protected by the French Constitution, which includes the 1789 Declaration of the Rights of Man and the Citizen. Articles 10 and 11 of the Declaration protect freedom of opinion and expression, describing the "free communication of ideas and opinions" as "one of the most precious rights of man". However, freedom of speech was never intended to be absolute. Unlike the First Amendment to the US Constitution, the 1789 Declaration of the Rights of Man and the Citizen provides for limitations to freedom of expression in the definition itself. On 22 December 2018, President Emmanuel Macron signed a new law against disseminating false information (Law No. 2018–1202 of 22 December 2018 on the fight against the manipulation of information (22 December 2018), https://perma.cc/QH5N-25MC [accessed on: 21/08/2022]). This legislation was adopted in reaction to new methods of disseminating disinformation, the Internet in general and social media in particular. Under this new Law, online platforms are obliged to establish a way for users to flag false information, especially in content promoted by a third party. This method of flagging fake news must be "easily accessible and visible". Furthermore, online platforms are

encouraged to take measures such as improving the transparency of their algorithms, promoting content from press agencies and radio and television services, fighting against accounts that massively disseminate fake information, informing users of the identity of the person(s) or organisation(s) that bought paid content related to "a debate of national Interest", informing users of the nature, origin, and manner of broadcasting content, and educating people about the media and information. Online platforms must provide the Conseil supérieur de l'audiovisuel (CSA) (the National Council on Audiovisual), France's main regulatory agency for radio and television broadcasting, with a yearly statement indicating what measures they took to fight against fake news. The CSA is then expected to publish regular reports on anti-fake news measures taken by online platforms and their effectiveness. Additionally, online platform operators that use algorithms to organise the display of content related to "a debate of national interest" are required to publish statistics on how they work.

For every item of content, online platform operators must specify how often it was accessed directly, through the platform's recommendation, sorting, and referencing algorithms, and through the platform's internal search function. These statistics are to be published online and made accessible to anyone.

Online platform operators must designate a legal representative in France to serve as a point of contact for applying these provisions. Some provisions of this new Law aim to improve transparency for political advertising on the Internet. Specifically, the Law amended the Electoral Code to provide that online platforms with at least five million unique visitors per month must, during the three months preceding the first day of a month during which a national election is scheduled and until the end of that election, provide users with "faithful, clear, and transparent information on the identity" of the person(s) or organisation(s) that bought paid content related to "a debate of national interest". Additionally, during that same timeframe, online platforms are required to give their users "faithful, clear and transparent information on the use of their data in the context of promoted information content related to a debate of national interest", Furthermore, during the same period, online platforms that are paid €100 (approximately US$110) or more per sponsored content must make the payment amount public. Failure to abide by these requirements is punishable by up to one year in jail and a fine of €75,000 (approximately US$83,150).

The new Law also creates a new legal weapon to combat disseminating fake news during an election period. During the three months preceding the first day of an election month and until the end of that election, a judge may order "any proportional and necessary measure" to stop the "deliberate, artificial or automatic and massive" dissemination of fake or misleading information online. A public prosecutor, candidate, political party or coalition, or any person with standing may file the motion, and the court must rule within 48 hours. Additionally, the CSA may suspend the broadcasting license of an operator controlled by or under the influence of a foreign state if, during an election period, if it broadcasts false information that could affect the election results. While this measure is

aimed at radio and television broadcasters, a suspension ordered by the CSA may apply to broadcasts on "any electronic communication service" (i.e., the Internet) and radio and television broadcasting. The CSA may also, after a first warning, withdraw the broadcasting license of a radio or television operator controlled by or under the influence of a foreign state if it broadcasts harmful content. This provision explicitly states that spreading false information to interfere with the proper functioning of institutions should be considered harmful to fundamental national interests. The CSA may, in deciding to withdraw a broadcasting license, consider content that the broadcaster, its subsidiary or parent organisation published on other services, such as the Internet. However, the CSA may not base its decision to withdraw a license entirely on that factor.

A key factor in countering foreign intervention efforts appears to have been the active role of two government agencies: the Commission Nationale de Contrôle de la Campagne Électoraleenvue de l'Élection Présidentielle (CNCCEP) (the National Commission for the Control of the Electoral Campaign for the Presidential Election), and the Agence Nationale de la Sécurité des Systèmesd'Information (ANSSI) (the National Cybersecurity Agency) These agencies worked with the presidential candidates' campaigns to educate them on cybersecurity and warn them of specific threats and attacks.

The law against disseminating false information adopted in December 2018 provides that French public schools should teach students how to navigate online information. These recommendations largely reiterated those set out in Law No. 2018–1202 of 22 December 2018 and include implementing an accessible and visible reporting mechanism, ensuring transparency of algorithms, promoting content from newspapers, news agencies and audiovisual communication services, detecting and countering accounts that massively disseminate false information, ensuring transparency of promoted content and promoting the skill to media and information.

6 Spain

The Spanish legislator aims to introduce the crime of disinformation or the deliberate dissemination of false information through the use of digital global communication platforms, Internet technologies, any computer system or any means of communication or data transmission technology suitable for altering the regular results of election acts, but this applies to the Election Code. The manipulation of political processes through digital media and social media to cause disinformation, either through confusion, by fragmenting and dividing societies, or by breaking down the social fabric and creating an environment conducive to xenophobic politics, is identified as a threat. In addition, the government is working on introducing a rapid alert system (rapid alerts) against fake news so that it can be responded to immediately. For now, Spain will participate in the coordination of the strategy for the denial of fake news. Joining the European strategy is expected to allow rapid action sufficient to detect fake news (European action plan against disinformation).

7 Israel

Cybersecurity is seen by the Israeli government as an important national security interest due to geopolitical considerations. The rapid pace of technological progress in cyberspace has raised particular concerns in recent years about the ability of external and internal actors to manipulate public opinion through spreading disinformation on social media and the impact of this development on democratic governance. Specific concerns about foreign intervention in Israel's general elections were particularly highlighted in the run-up to the elections of 9 April 2019. Except for media reports of Iranian intelligence hacking into the mobile phone of Benny Gantz, Chairman of the Kahol Lavan political alliance, no specific data have been published on incidents of cyber attacks, the spread of false information or other improper online behaviour concerning the Knesset elections.

However, in the end, the biggest threat may come from people trying to manipulate opinions by spreading misleading information online, for example, through fake Facebook profiles. The number of bots – fictitious social media users – can be huge. Bots can be created and maintained for three or four years and activated when the elections start. The challenge is to maintain credibility and public trust in the process. Sometimes, it is enough to block a government website for a few hours to raise public doubts about the purity of the system.

As claimed by Tamir Pardo, Head of the Mossad (Israel's secret intelligence service),"What we've seen so far with respect to bots and the distortion of information is just the tip of the iceberg. It is the greatest threat of recent years, and it threatens the basic values that we share - democracy and the world order created since World War Two" (Ziv, 2019).

Experts say that although protecting critical infrastructure and organisations from cyber attacks is a challenge that should be mastered, the battle for public opinion caused by the spread of disinformation requires more complex treatment. The complexity of finding appropriate legal remedies stems from the need to balance the objective of cybersecurity with constitutional principles such as freedom of expression, the right to privacy, the purity of elections, the principles of transparency and parliamentary oversight of government activities, etc. An additional challenge for securing cyber systems is that legal regulations often lag behind the continuous development of new technologies. Several legislative proposals have been put forward regarding cybersecurity and the specific threats posed by the spread of disinformation. These include a proposal for a law regulating the mission, functions and objectives of the Israel National Cyber Directorate, and its authority to detect and identify cyber attacks on Israel, and to warn and share information about such attacks.

Other proposed laws specifically address transparency requirements for online political advertising and removing foreign-funded and harmful online content. Although the statutory transparency requirements for election propaganda were originally limited to

print advertisements, the Central Elections Committee (CEC) has extended them to online election advertisements ahead of the national elections on 9 April 2019. The CEC also recognised the government's obligation to refrain from publishing misleading information.

Ahead of the 9 April 2019 elections, Facebook blocked anonymous and paid Israeli political ads on its site, whilst Google blocked all advertising options related to segmentation, retargeting and using a list of names by anyone involved in political advertising. Addressing the challenges of disinformation, the CEC for the upcoming 17 September 2019 national elections has posted recommendations for identifying the government's response to disinformation on social media platforms and video clips to clarify its message on the subject.

Cyberthreats to Israeli targets can come from both foreign and domestic sources. The ability to spread disinformation on social media easily and quickly, and thereby to manipulate public trust in national institutions or public opinion on other issues, is considered a growing challenge by Israeli policymakers and experts. However, tackling the spread of disinformation on social media through legal regulation raises serious constitutional, institutional and ethical concerns. Among the technological tools used in the battle for public opinion, experts cited bots, big data, hacking and trolls. Bots can spread countless messages encouraging controversy, hatred and violence in the form of posts or talkbacks to articles published in online newspapers. The use of big data analytics makes it possible to target specific audiences based on political preferences or perceived susceptibility to manipulation, as revealed by a person's record of online activity on Facebook or other networks. Other means of possible online manipulation included the hacking of legitimate accounts, the use of professional paid "talkbackers" (trolls) and the impersonation of innocent forums to recruit followers in order to prepare the infrastructure of followers for the "command day".

Deepfake is a new AI-based technology that facilitates "a combination of 'deep learning' and 'fake news' [and] enables the creation of audio and video of real people saying words they never said or things they never did". Such technology can be used to create fear, the perception of a lack of control and harm to a person's privacy "in ways never thought of before". Most important are the wider social implications of this technology. It is not just the fear of false imitation of political candidates. According to Israeli experts, deepfake technologies lead to an inability to distinguish truth from lies, increasing challenges in explaining reality and the phenomena and processes taking place, and the distrust of ourselves and our ability to determine right and wrong in the world around us. Together, these three threaten the foundations of government, the functioning of institutions and the ability to maintain viable human and social relationships.

As in other technological contexts, there are three ways to deal with the threat of deepfakes. The first is to raise public awareness to identify fakes, first and foremost, by asking questions. The problem is that sometimes the impact on people's awareness

remains even after they realise it is a fake. Moreover, teaching people not to believe anything comes at a great social cost. The second way is to create a cat-and-mouse race between deepfake creators and those who develop identification technologies. A third way is to regulate the development and distribution of deepfake products. The authors suggest that there may be a basis for distinguishing between the regulation of fake news and deepfakes, noting that in the US, social networks are exempt from liability for the content that passes through them and is created to support the growth of the Internet.

Social polarisation, hate speech and fake news have not yet caused lawmakers to revoke the exemption, but deepfake may be a reason to impose such liability. It is worth recalling the words spoken by Mark Zuckerberg, who claimed that Facebook might treat deepfakes differently from fake news. To illustrate the challenge posed by the use of deepfakes, the authors cite the case of Deep Nude, a deepfake app that allows the creation of nude images of women based on their images in clothing, using a machine learning algorithm. After half a million downloads and a server crash, the software was removed by its creator. The Deep Nude story teaches again that there is no need to do good in technology, and the challenge lies in setting moral boundaries. Recently, there have been claims that it is not enough to take ethical considerations into account when creating educational systems, but there are educational systems that do not need to be created at all, even by legal prohibition, against all the difficulties this creates. The creator of the Deep Nude software removed it from the servers, claiming that "the world is not ready yet". For this, we can say that we are thoroughly ready. We just don't want it. Constitutional challenges associated with regulating the dissemination of disinformation concern the impact of regulating the dissemination of information on protecting the freedom of expression and the right to privacy. In addition, regulating cybersecurity at the national level may undermine, for instance, the principles of transparency, parliamentary oversight and equality in elections.

8 Canada

No regulation in Canada expressly prohibits the dissemination of false news, even if it is defamatory. Attempts to address the problem of disinformation must be balanced against the right to freedom of expression protected by Subsection 2(b) of the Canadian Charter of Rights and Freedoms, which states that everyone has the fundamental freedom of "thought, belief, opinion and expression, including freedom of the press and other media of communication". Fundamental rights, including freedom of expression, are subject to Article 1, which allows for "reasonable" limits on these rights. This means that once a Charter right is found to have been infringed, the courts must decide whether the right has been infringed. Section 181 of the Criminal Code of Canada prohibits the dissemination of false news ("Everyone who wilfully publishes a statement, tale or news that he knows is false and that causes or is likely to cause injury or mischief to a public interest is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years").

The Elections Modernisation Act, passed in December 2017 and entirely in force from 13 June 2019, amended the Canada Elections Act (CEA) and other laws to modernise Canada's election law. According to a government news release, "the new legislation is part of a comprehensive plan to safeguard Canadians' trust in our democratic processes and increase participation in democratic activities".

Among the changes included in the Act was a provision that considered it an offence "to make false statements about a candidate to affect election results". In particular, the Act provided that no person or entity shall, with the aim of influencing the results of an election, make or publish, during the election period: a) a false statement that a candidate, a prospective candidate, the leader of a political party or a public figure associated with a political party has committed an offence under an Act of Parliament or a regulation made under such an Act – or under an Act of the legislature of a province or a regulation made under such an Act – or has been charged with or is under investigation for such an offence; or b) a false statement about the citizenship, place of birth, education, professional qualifications or membership in a group or association of a candidate, a prospective candidate, the leader of a political party or a public figure associated with a political party.

The Elections Modernisation Act also aims to prevent foreign interference in the election process regarding paid political advertising through online platforms. Foreigners and foreign entities may not purchase regulated advertising during the election period, currently defined as a maximum of 15 days. Platform operators or owners may be prosecuted (or other compliance or enforcement action may be taken) for knowingly selling election votes. Third parties may not use funds for regulated activities, including election advertising, if the source of the funds is a foreign entity; prohibits foreign third parties from participating in elections and incurring expenses for regulated activities (including partisan advertising expenses) that are undertaken by foreign entities.

The Elections Modernisation Act also imposes requirements on online platforms to improve transparency and integrity of content during elections. Section 319 of the CEA defines an "online platform" as "an Internet site or Internet application whose owner or operator, in the course of their commercial activities, sells, directly or indirectly, advertising space on the site or application to persons or groups". Platforms in this category must maintain a digital register of all regulated advertisements, publishing the register and details of the agents who have authorised the advertisements. Ads must be placed on the register on the day they first appear on the platform, and each ad must be kept on the register for two years after the election. After this period, operators or platform owners must keep the ad information for five years.

9 Norway

A fact-checking initiative called Faktisk was set up in Norway before the 2017 general elections. It was created jointly by two tabloids, *Verdens Gang* and *Dagbladet*, the public broadcaster NRK and the commercial TV channel TV2. Funding for the initiative comes from the owners of the four publishers and the freedom of expression organisation, Fritt Ord. Faktisk checks news appearing in Norwegian media and social media, in public debates and statements by politicians, and follows up on complaints made by the public. The main topics are climate, Norwegian elections and international affairs. Faktisk ranks each submission on a veracity scale of one to five, making it available as text or a short video on its website, through social media platforms such as Facebook and Snapchat, and on television. It uses open formats for these purposes so that other media companies can use its resources. The Faktisk website is one of the most popular in Norway.

Another initiative aimed at civil society in Norway is a fact-checking tool for newspaper readers, called Reader Critic, developed by *Dagbladet*. This system allows readers to report inaccuracies in the newspaper's content and automatically notifies the author. In the first nine months of the Reader Critic programme, *Dagbladet* received 20,000 opinions on 10,000 articles from 5,000 users. The information most often pointed out grammatical errors. However, some more serious errors were also identified.

10 Sweden

In Sweden, there is a focus on cooperation between the public sector and the private (media) sector. A new government-funded cooperative between the public service and the three largest media houses in Sweden (Schibsted, Bonnier and NTM) has been announced. Together, they will develop a digital platform to counter the spread of fake news, an automated news rating service, and an automated tool for checking and personalising facts. Sweden relies on free media. It takes the position that the best protection against fake news is free media that compete with each other and "breathe down each other's neck". The fact that they now collectively decide what fake news is prevents the misinformation passing through the media network from becoming more widespread and legalised.

As Sweden points out, there is a risk the reaction of the media and social networks to fake news will increase distrust as well as become a tool for silencing divergent views.

The line between opinion and information, and between fake news and true news, is extremely difficult to draw. If done wrong, the effort will be transformed from an attempt to prevent the spread of fake news into a tool to prevent the spread of unpopular opinions. In Sweden, there has been an initiative to create an organised control of information, with the media playing a large role. The cooperating media are to individually review information spread on social media from individuals and political authorities. The collected material is then to be presented on a shared website. Carefully reviewing the

data and searching for its source is very time-consuming, so there is a reliance on media cooperation. By combining multiple media in this project, the public can access accurate information. The cooperation between numerous media also means that the correct information can be more easily accessed on social media. In the case of false information regarding the coronavirus, the AFP News Agency publishes daily fact-checking articles regarding it.

Sweden recognises the right to freedom of expression, including online and through using social media platforms. While private entities are free to block inappropriate content, the government neither prohibits using Twitter or fake Twitter accounts nor has it passed legislation allowing the government to block websites or Internet access. It does not regulate opinion-based advertising either. However, Sweden has recognised spreading false information as a criminal offence and obliges the news media to correct such information. Realising that disinformation is a significant global challenge, the Swedish government is in the process of launching a new agency, the Psychological Defence Agency, which will focus on psychological defence and combating disinformation in Sweden. The agency is expected to be launched in 2022. The Swedish Emergency Agency had previously been tasked with making the Swedish population aware of disinformation campaigns and educating them on how to check the veracity of information and was actively involved in this process. Media companies have begun to address disinformation voluntarily. During the 2018 national election cycle, four Swedish public media corporations created a fact-checking website (now discontinued) that allowed members of the public to verify election-related claims. Bots were used in the 2018 elections, but no successful disinformation campaigns were identified. Facebook removed posts that contained false information produced by fake accounts in connection with the 2018 national elections. TV4 initiated rules prohibiting the purchase of political advertising by foreign entities in the weeks leading up to the 2019 EU parliamentary elections. Disinformation continues to be one of Sweden's challenges, from the perspective of defence and civil emergencies. The mass dissemination of disinformation is recognised by the Swedish authorities as a global problem. The risk of future mass dissemination of information in Sweden, especially about elections, is also recognised. Sweden protects the right to freedom of speech as enshrined in its Constitution (Instrument of Government). Further regulation of freedom of expression is contained in two separate constitutional acts, the Law on Freedom of the Press (Tryckfrihetsförordning, TF) and the Basic Law on Freedom of Expression (Yttrandefrihetsgrundlagen, YGL). Sweden introduced the first legislation concerning freedom of the press in 1766.

References:

Chałubińska-Jentkiewicz, K. (2023) *Prawne granice dezinformacji w środkach społecznego przekazu. Między wolnością a bezpieczeństwem* (Toruń: Wydawnictwo Adam Marszałek).

Chiu, K. (2020) China orders live streamers and gift-giving fans to register with real names, *South China Morning Post*, (November 24, 2020), available at: https://www.scmp.com/tech/policy/article/3111177/china-orders-live-streamers-and-gift-giving-fans-register-real-names (August 21, 2022).

Criminal Code Amendment, available at: https://perma.cc/UV8K-FHD (August 21, 2022).

Decree of the President of the Russian Federation on the Strategy for the Development of an Information Society in the Russian Federation for 2017–2030, N 203, (May 9, 2017), available at: http://pravo.gov.ru, https://perma.cc/AQ4H-CE79 (August 21, 2022).

Federal Law on Information, Information Technologies and Protection of Information, No. 149-FZ, (July 27, 2006), available at: https://perma.cc/86PF-DYTH (August 21, 2022).

Law No. 2018–1202 of 22 December 2018 on the fight against the manipulation of information, (December 22, 2018), available at: https://perma.cc/QH5N-25MC (August 21, 2022).

PRC Cybersecurity Law, adopted by the Standing Committee of the National People's Congress on 7 November 2016, effective from 1 June 2017, available at: https://perma.cc/3HAP-D6M (August 21, 2022).

Resolution of the President of the Russian Federation on Approving Information Security Doctrine, (December 5, 2016), available at: https://perma.cc/4BEK-4M5R (August 21, 2022).

Reuters (2019) *China seeks to root out fake news and deepfakes with new online content rules*, available at: https://www.reuters.com/article/us-china-technology/china-seeks-to-root-out-fake-news-and-deepfakes-with-newonline-content-rules-idUSKBN1Y30VU (December 11, 2019).

Statista (2019) *The number of Internet users in Russia*, available at: https://perma.cc/NS4X-ZE3X (August 21, 2022).

The 2016 Federal Election Interim Report on the authorisation of voter communication. Joint Standing Committee on Electoral Matters, available at: https:/erma. cG753-PB; JSCEM (August 21, 2022).

Ziv, A. (2019) Massive Manipulation, Foreign Influence Campaign and Cyber: The Threats to Israel's Election, What's behind the Shin Bet Chief Warning that a 'Foreign Country' Intends to Intervene in the Israeli Election, *Haaretz.com*, (January 9, 2019), available at: https://perma.cc/LE7Y-79SN?type=image (August 21, 2022).