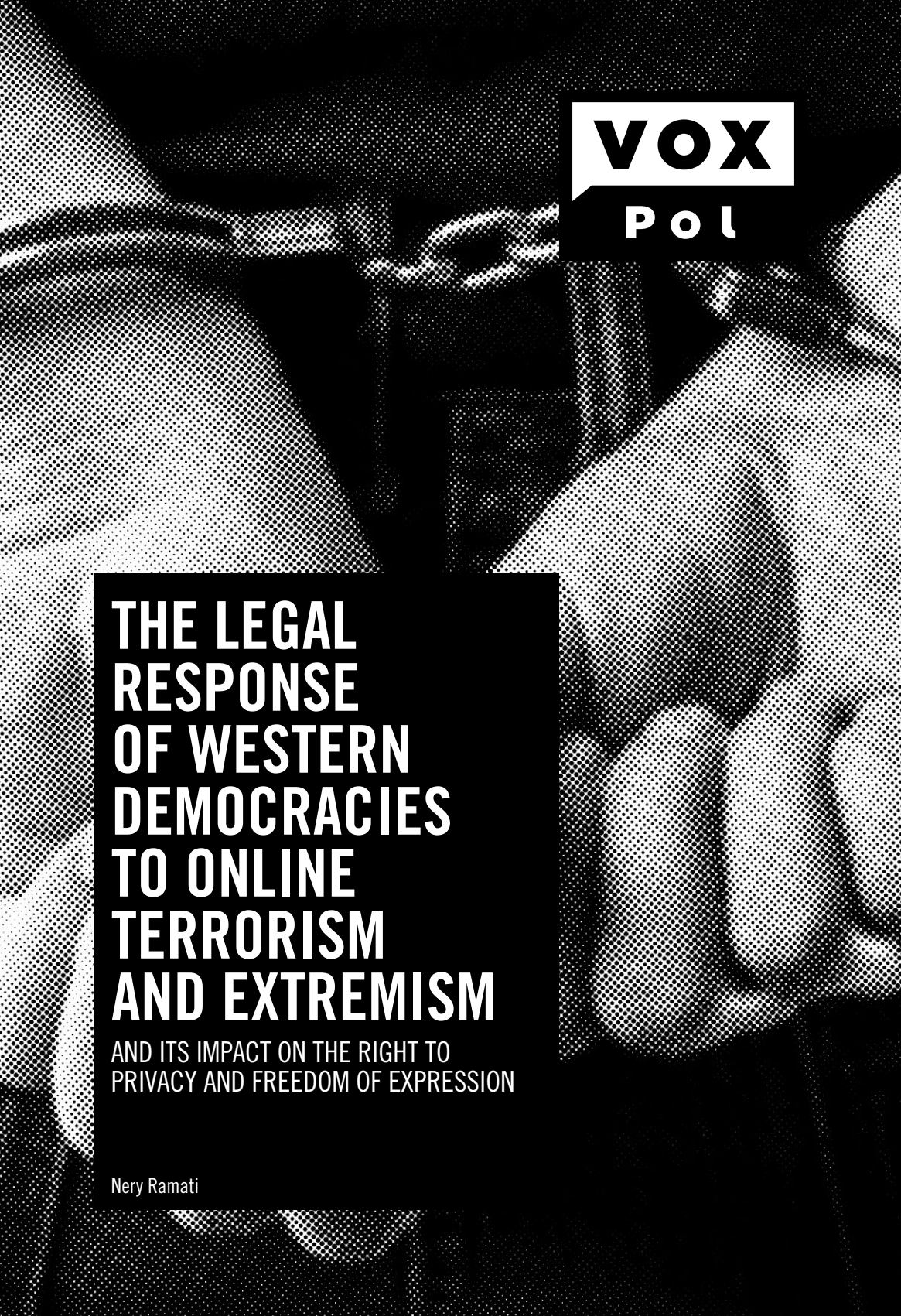


VOX Pol

THE LEGAL RESPONSE OF WESTERN DEMOCRACIES TO ONLINE TERRORISM AND EXTREMISM

AND ITS IMPACT ON THE RIGHT TO PRIVACY AND FREEDOM OF EXPRESSION

Nery Ramati

THE LEGAL RESPONSE OF WESTERN DEMOCRACIES TO ONLINE TERRORISM AND EXTREMISM

AND ITS IMPACT ON THE RIGHT TO PRIVACY AND FREEDOM OF EXPRESSION

About the author

Attorney Nery Ramati LLM was a partner in Gaby Lasky and Partners Law Office, a leading human rights office in Israel specialising in freedom of expression and protest. He has been representing Palestinian, Israeli and international human rights and anti-occupation activists in the military and civil courts since 2008 and specialises in representing in criminal cases relating to freedom of speech. He has provided legal counsel to various organisations engaged in documenting and protesting human rights abuses and violations of international law by the Israeli authorities in the Occupied Palestinian Territories. He is currently conducting research at Dublin City University and the VOX-Pol Network of Excellence on the legal response of liberal countries to online extremism.

Acknowledgements

The author would like to thank Prof Maura Conway of Dublin City University for her kind and patient guidance, Louise Laing of Dublin City University for her help in the publication of the report, Dr Sharon Weill of the American University of Paris for her help on French law, and Dr Anneke Petzsche of the Humboldt University of Berlin for her help with German law. Finally, I would like to thank the many anonymous reviewers around the globe for providing very constructive comments and suggestions on the first draft of this report.

ISBN: 978-1-911669-02-9

Designed and typeset by Soapbox, www.soapbox.co.uk

Cover photo: Bukhta Yurii/Shutterstock.com

TABLE OF CONTENTS

INTRODUCTION

Extremists and terrorists have found the online sphere, and specifically its social networks, to be an efficient tool for advancing their methods and political needs. The legal responses to the resulting threats from this online activity vary from country to country. The immense importance of the Internet in the everyday life of billions of people worldwide has raised difficult questions regarding the attempt to regulate online activity, especially in relation to the right of privacy and freedom of speech. This report examines how western democracies balance, from a legal point of view, the need to protect their populations from terrorist attacks and their duty to preserve the democratic rights of privacy and free speech.

FRAMEWORK

The report examines the legal response to online extremism in six countries: France, Germany, Israel, Spain, the United Kingdom (UK), the United States of America (US), as well as the global response of the United Nations (UN) and the regional response of the European Union (EU). The six countries were chosen because they have experienced incidents of terrorism in recent years and, in all of these countries, recent active internal legislation has been enacted with regard to online extremism. For each country, this report examines the following aspects:

A) The origins of the country's legal system, pyramid of norms and constitutional protections – if they exist – of the right to privacy and freedom of speech;

B) The history of terrorism in the country, specific political conflicts and recent events;

C) The identification of online activity related to recent terrorist attacks;

D) The legislative efforts of each country to tackle the phenomenon;

E) The country's legal policy of blocking and filtering online extremist content and the potential impact on the right to privacy and freedom of speech;

F) The country's online surveillance practices and their potential impact on these rights;

G) The country's criminal law legislation, practices and jurisprudence regarding online statements and their potential impact on the right to privacy and freedom of speech;

H) The country's use of administrative law in relation to online activity and its potential impact on the right to privacy and freedom of speech.

SUMMARY OF FINDINGS

GENERAL LEGAL RESPONSE

The different histories of each country, and the resulting different legal histories, have created diverse paths when it comes to the legal response to online extremism. Countries that were involved in ongoing internal conflicts – such as Spain and the Basque Country, the UK and Ireland, and Israel and Palestine – had pre-existing advanced counter-terrorism legal tools and needed only to adjust some of them to the specific technology change. The ongoing counter-terrorism campaigns in these countries have led to the rights of privacy and freedom of speech being limited as a result of years of legislation and jurisprudence. The extensive use of propaganda by Nazi Germany has impacted the modern German legal system in such a way that the German criminal code contains several felonies that limit the freedom of speech in cases concerning the support of terrorism, hate speech, unconstitutional propaganda and even denying the country's violent history.

On the other side of the spectrum, the fight for freedom from the British Empire by the US, where the Empire imposed severe restrictions on public expression, impacted the drawing up of the US Constitution, making freedom of speech an extremely protected right with almost no direct legislation that limits it. That being said, this report has found that, as online extremist threats have become more evident, most of the countries have reached a common ground in terms of legislation and practice. An example of such unification efforts can be seen in the EU directive on combating terrorism (2017/541) or in the current attempts to pass regulations preventing the dissemination of terrorist content online.

LAW AS A TOOL FOR PREVENTION

All countries in the report had enough legal tools to punish terrorists for their violent actions in the aftermath of terrorist attacks. The main goal of legal counter-terrorism efforts – as seen in the counter-terrorism strategies of the UN, the EU and the individual countries – is to develop legal ways that will help prevent terrorism. The identification of online extremist content as a tool for the planning, radicalisation, dissemination and recruitment that leads to violent attacks has resulted in countries attempting to tackle the issue with preventive measures. This report has identified four commonly seen legal techniques that are used to limit extremist content: the blocking and removal of online content; the surveillance of online activity; the criminalising of certain online public expressions; and the use of online content as a justification for applying restrictive administrative measures.

BLOCKING AND FILTERING

All countries in the report, except the US, have legal mechanisms allowing them to demand that online platforms remove and block extremist content. Europol, the European Union Agency for Law Enforcement Cooperation, also has a specific mechanism. The direct effectiveness of these mechanisms is questionable since the data gathered in the report shows that the number of annual requests to online platforms by the most active countries doesn't exceed tens of thousands, even though, for example, Facebook alone reports that, in the first quarter of 2018, it removed 3.5 million pieces of violent content and 2.5 million pieces of hate speech. It seems that the real success of the 'remove and block' legislation is not so much in the mechanisms it creates to remove and block content but as a catalyst for the social media companies to redefine their terms of use and to develop the technical tools to enforce them.

The global demand to remove content and the massive response by the social media companies raises many questions regarding freedom of expression, and the efficiency of counter-terrorism.

First, the report highlights several examples of mistaken requests to remove innocent content, including important scientific web pages, and where the appeals procedure is not adequate. Second, in the context of internal political conflict, the removal of extremist content may be used in a one-sided and biased way. And third, the removal of violent extremist content as soon as it is published can hamper academic research on the phenomenon and public help in the early identification of the perpetrators.

SURVEILLANCE

The regulatory powers of online surveillance were re-examined in most of the countries featured in the report following *The Guardian*'s Edward Snowden exposure. Revelations of the extent to which the US National Security Agency (NSA) was gathering information on private citizens from all over the world led to the introduction of specific laws dealing with surveillance powers in the US, the UK, France and Germany.

This wave of new legislation still left open some major questions regarding surveillance and the right to privacy however. First, should 'bulk surveillance' be allowed in order to protect state security? The legal answer to that differs from country to country, with the European human rights courts not ruling out the possibility of its use with proper supervision. Second, are the specific warrants for gathering information on a person sufficiently supervised? Once again, the legal situations differ. Some countries allow a non-judicial authority to order surveillance, while others require a judicial warrant. The supervision of the judicial authorities has also been questioned, as in the case of the Foreign Intelligence Surveillance Courts (FISC) in the US. The third point relates to how countries distinguish between restrictions on surveillance of their own citizens and restrictions on surveillance of foreign citizens. While most countries give more power to their intelligence agencies to carry out surveillance of foreign citizens, the essence of the online world, and especially social network platforms, is its 'globality', which

creates a situation where agencies carry out surveillance on foreign citizens while also gathering information on their own citizens using tools that are not allowed for that purpose.

CRIMINAL LAW

The use of criminal law for charging people when it comes to online activity has grown dramatically since 2015 in most of the countries featured in the report. The leaders in this area are the UK, France, Spain and Israel, who charge hundreds of people every year based on their online statements. Increasing numbers of new felonies regarding online activity have been introduced in those countries, including at the European level in the directive on combating terrorism of 2017. This overzealous legislation and use of criminal law has led to criticisms on several points. First, the trend of expanding criminal law when it comes to online content has been constantly pushed, leading to a situation whereby both the UK and France have passed laws that criminalise accessing or viewing extremist content online, without even expressing support for it. Second, many of the new laws contain definitions of the legal terms 'terrorism', 'incitement', 'apology' and 'glorification' that are too widely defined and lack a clear need for intention or acknowledgment of risk. This legislation has created a situation where mild statements, jokes, art or clear political views have been cause for charging people with a criminal offence. Although some will say this phenomenon can be limited by using prosecutorial discretion, it is still contradictory to the rule of law. And third, the report shows evidence from Israel, the US and Spain of biased prosecutions and punishments against jihadi and leftist online statements, but taking a more lenient approach towards right-wing extremist online activity. This kind of situation presents an inherited problem in terms of the prosecution of felonies of speech in countries with a major political conflict, as the current ruling side are more likely to perceive statements made by the opposing political side as more dangerous than statements made by its supporters, extremist as they may be.

ADMINISTRATIVE LAW

Most of the countries in the report use administrative counter-terrorism measures, mainly in order to control and monitor the entry and exit of people from their countries, where an increasing number of the decisions are based on the subject's online profile and activity. These non-judicial actions again raise the fear that, in some cases, decisions are based more on the *political content* of the online activity and less on the security risk that arises from it. France and the UK are the most active in using administrative law when it comes to other aspects of counter-terrorism, such as restrictions on residence, travel, movements, communications, possessions and work. The main problem with these legal mechanisms is that these administrative warrants are oftentimes based, at least in part, on secret evidence gathered by intelligence agencies. Although the use of secret evidence was restricted by the European Court of Human Rights in *A. and Others v. the United Kingdom*, a lot of the secret evidence contains data based on individuals' online activity, creating a situation where a person is sanctioned administratively based on their online activities without being given the chance to explain them, since these activities are part of the secret evidence.

FRANCE

THE FRENCH LEGAL SYSTEM, THE RIGHT TO PRIVACY AND THE RIGHT TO FREEDOM OF SPEECH

France is a constitutional democracy, and the current constitution of 1958 established a Constitutional Council. The Constitutional Council can examine and rule on the legality of French parliamentary laws, according to the constitution. The constitutionality of a law can be examined either as a result of a request from 60 members of parliament or through a petition from a citizen whose case has been affected by the law.[1] The preamble of the constitution refers directly to the Declaration of the Rights of Man and of the Citizen of 1789, which protects the right to freedom of speech. Article 9 of the French civil code provides that everyone has a right to their private life. The Data Protection Act Law No. 78–17 of 1978 specifically protects individuals against violations of their personal data.

The rights to privacy and freedom of expression in France are also protected by several international instruments that have been ratified by France, such as Article 8 (Privacy) and Article 10 (Freedom of Expression) of the Convention for the Protection of Human Rights and Fundamental Freedoms 1950 (European Convention on Human Rights), Article 7 (Privacy) and Article 11 (Freedom of Expression) of the Charter of Fundamental Rights of the European Union, and Article 12 of the UN Universal Declaration of Human Rights 1948. These conventions are strongly interwoven into the French judicial system, in particular the European Convention on Human Rights and the rulings of the European Court of Human Rights.[2] The French data

1 Article 61 of the French Constitution of 1958.

2 'Privacy And Freedom Of Speech In France', *Westlaw,* https://content.next.westlaw.com/Document/I3698ea0e175011e498db8b09b4f043e0/View/FullText.html accessed 7 May 2019.

protection agency is *the Commission Nationale de l'Informatique et des Libertés (CNIL)*, created by Law 7817 of 6 January 1978. The CNIL was given, by law, the powers to protect freedom and privacy on the Internet.[3]

FRANCE AND TERRORISM

The history of terrorism in France is not limited to a specific kind of group or ideology. Terrorist organisations from the extreme left and extreme right along with Basque, Breton, Corsican and Algerian insurgent groups[4] were all involved in attacks in France during the last century. The 2004 Madrid terrorist attack and the 2005 London jihadi terrorist attacks were largely perceived in France as being a response to Spain's and the UK's involvement in the wars of the Middle East, and it was thus widely held that France was more protected due to its stand against those wars.[5]

The Toulouse and Montauban shootings of 2012 came after almost 15 years without serious terrorist attacks in France. The attacks bore signs that would later be repeated in a series of deadly attacks over the years that followed. The attacker was a young French citizen, from the third generation of a family of immigrants, who had been radicalised.[6] The *Charlie Hebdo* newspaper, Hipper kosher, St Denis and Bataclan attacks made 2015 the deadliest year of terrorist attacks in modern French history.[7] Nor was there any let up in 2016, with

3 'France Cyber-Crime Policies/Strategies', *Council of Europe*, June 2017, www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/france accessed 24 May 2019.

4 'L'attentat Le Plus Meurtrier Depuis Vitry-Le-François En 1961', *Le Figaro*, January 2015, www.lefigaro.fr/actualite-france/2015/01/07/01016-20150107ARTFIG00178-historique-des-attentats-en-france-depuis-1994.php accessed 10 May 2019.

5 Michael S. Neiberg, '"No More Elsewhere": France Faces the New Wave of Terrorism', *The Washington Quarterly*, 40(1), 2017.

6 Meredith Boyle, 'Lone Wolf Terrorism and the Influence of the Internet in France', *Digital Commons @ Connecticut College*, 2013.

7 There were 152 killed and hundreds wounded.

the Nice attack, and, in 2018, with the Carcassonne and Trèbes attack and the Strasbourg attack.

Another major security problem that France is dealing with is the continuous flow of French citizens joining jihadi fighters in the Middle East. An estimated 2,000 French nationals joined ISIS and other Syrian jihadist groups, and many of them have returned to France, posing an internal threat.[8]

INTERNET ACTIVITY RELATED TO THE ATTACKS

French authorities identified the widespread involvement of the Internet as a tool in processes of radicalisation and recruitment and in the execution of the aforementioned attacks. There were claims that the Toulouse and Montauban shooter had been radicalised having followed an Islamist group (*Forsane Alliza*) online. Following the attack on *Charlie Hebdo*, there was massive and rapid distribution of high-quality online materials supporting the terrorists, which had been prepared for the event.[9] The different terrorists involved in the St Denis attack had never met each other prior to the attack and communicated using the Telegram messaging app.[10]

THE STATE'S LEGAL RESPONSE

The history of terrorism in France has left its mark on the legal system. For example, it is one of only a few countries in Europe that had in place, prior to the 7 July 2005 attacks in London, a specific law against supporting terrorism or, as it is called in France, against those

8 Richard Barrett, 'Beyond the Caliphate: Foreign Fighters and the Threat of Returnees', *The Soufan Center*, October 2017, https://thesoufancenter.org/research/beyond-caliphate accessed 15 May 2019.

9 Claire Smith, et al., 'The Manipulation of Social, Cultural and Religious Values in Socially Mediated Terrorism', *Religions*, 9(5), 2018.

10 James Billington, 'Paris Terrorists Used WhatsApp and Telegram to Plot Attacks According to Investigators', *International Business Times*, December 2015, www.ibtimes. co.uk/paris-terrorists-used-whatsapp-telegram-plot-attacks-according-investigators-1533880 accessed 20 May 2019.

who offer an 'apology for terrorism'.[11] This can be found in Article 24 of the French Freedom of the Press law of 1881. The state also has the power to declare a state of emergency, according to a law from 1955, which gives administrative bodies extensive temporary powers to act on matters of security.

In 2014, the French parliament passed a new counter-terrorism law, which dealt with various aspects of the criminal and administrative tools used to fight terrorism.[12] A state of emergency was declared after the terrorist attacks in Paris on 14 November 2015 and lasted until 30 October 2017. Although it has ended, the French legislature has adopted some of the mechanisms from the state of emergency law into regular state legislation.[13] By examining these laws, it is possible to identify the relevant legal tools that deal with the specific threat of online terrorist activities.

BLOCKING AND FILTERING ONLINE CONTENT

France does not block sites for political reasons. YouTube, Facebook, Twitter and international blog-hosting services have free access.[14] However, since the 2015 attacks, the government has been trying to persuade the public that, in order to maintain public safety, it is necessary to limit some fundamental rights.[15] A decree issued in the same year resulted in administrative powers to block websites relating

11 Ezekiel Rediker, 'The Incitement of Terrorism on the Internet: Legal Standards, Enforcement, and the Role of the European Union', *Michigan Journal of International Law*, 36, 2014.

12 LOI N° 2014-1353 Du 13 Novembre 2014 Renforçant Les Dispositions Relatives À La Lutte Contre Le Terrorisme, *Légifrance*.

13 LOI n°2017-1510 Renforçant la Sécurité Intérieure et la Lutte Contre le Terrorisme was passed on 30 October 2017.

14 'Freedom on the Net 2017: France', *Freedom House*, 2018, https://freedomhouse.org/report/freedom-net/2017/france accessed 24 May 2019.

15 'Valls: «La Sécurité Est La Première Des Libertés»', *La Dépêche*, January 2016, www.ladepeche.fr/article/2016/01/07/2251151-valls-la-securite-est-la-premiere-des-libertes.html accessed 27 May 2019.

to terrorism.[16] The state of emergency legislation gave power to the Minister for the Interior to block content that 'glorifies or incites acts of terrorism'.[17]

Outside of the state of emergency legislation, the Central Office for the Fight against Crime Relating to Information and Communication Technology (OCLCTIC) is the administrative body that can request editors or hosts to remove content and, after a 24-hour period, can request Internet service providers (ISPs) to block the site. The OCLCTIC blocked five websites suspected of promoting a terrorist agenda shortly after the law passed.[18] The main legal issue that arises from this law is the fact that these actions are carried out without any judicial supervision. The actions of the OCLCTIC are supervised by the National Commission on Informatics and Liberty (CNIL), the data protection agency. The CNIL can question OCLCTIC decisions by filing requests to the administrative courts but, in practice, rarely does so and is therefore accused by some of neglecting its original mission to protect freedom on the Internet.[19]

The 2015 attacks resulted in a surge of requests to block content. Up to 2017, 874 requests were filed by the French authorities, which is almost treble the amount prior to the attack (312).[20] Although the

16 Décret N° 2015-125 Du 5 Février 2015 Relatif Au Blocage Des Sites Provoquant À Des Actes De Terrorisme Ou En Faisant L'apologie Et Des Sites Diffusant Des Images Et Représentations De Mineurs À Caractère Pornographique, *Légifrance*.

17 LOI N° 2015-1501 Du 20 Novembre 2015 Prorogeant L'application De La Loi N° 55-385 Du 3 Avril 1955 Relative À L'état D'urgence Et Renforçant L'efficacité De Ses Dispositions.

18 Lucie Ronfaut, 'La France Bloque Pour La Première Fois Des Sites Web De Propagande Terroriste', *Le Figaro*, March 2015, www.lefigaro.fr/secteur/high-tech/2015/03/16/32001-20150316ARTFIG00153-la-france-bloque-un-premier-site-web-de-propagande-terroriste.php accessed 2 May 2019.

19 'France Implements Internet Censorship Without Judicial Oversight', *EDRi*, March 2015, https://edri.org/france-censorship-without-judicial-oversight accessed 19 May 2019.

20 Alexandre Linden, 'Le Blocage De Sites Internet Et La Menace Terroriste', *Commission Nationale de l'Informatique et des Libertés*, 2016, www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_blocage_sites_internet_2016_0.pdf accessed 21 May 2019.

OCLCTIC and the CNIL do not publish exactly what content was blocked, from the few cases CNIL did decide to challenge, a worrying picture arises. For example, a link to a video of the 2016 Nice attack, accompanied by the neutral text "Nice attack July 14, 2016, video of truck" was blocked and returned after the CNIL challenged it in court.[21] The 2014 anti-terrorism law gave the OCLCTIC the power to request that site editors and hosts remove inciteful content or content that apologises for terrorism. If the request is not answered within 24 hours, the OCLCTIC can block the site.[22] The 2015 decree also gave the OCLCTIC the power to remove online content from search results, using the same procedure.[23] In the years 2016–2017, the OCLCTIC filed 1,975 requests to remove terrorist-related content from sites and 2,077 from search engines; both are double the number of requests in comparison to 2014–2015.[24]

French authorities have been criticised for asking companies to remove content from the Internet where terrorism is suspected, without ensuring that the request is accurate.[25] The Internet Archive is a non-profit organisation that has been archiving Internet content for research and academic purposes. It revealed that, in one week, it received 550 false requests from the French government to remove URLs where terrorism was suspected. The URLs included works from the American Libraries collection, old television adverts and programmes, the Smithsonian Libraries, television broadcasts of the US House of Representatives, and even an academic paper entitled 'Spectrum Sharing in Cognitive Radio with Quantized Channel

21 Ibid.

22 See Note 12.

23 Décret N° 2015-253 Du 4 Mars 2015 Relatif Au Déréférencement Des Sites Provoquant À Des Actes De Terrorisme Ou En Faisant L'apologie Et Des Sites Diffusant Des Images Et Représentations De Mineurs À Caractère Pornographique.

24 See Note 20.

25 'Statewatch News Online: EU: French Anti-terrorist Unit Demands Removal of Adverts, Books, US-government Produced Reports from Web Archives', *Statewatch*, April 2019, www.statewatch.org/news/2019/apr/iru-internet-archive1.htm.

Information'.[26] The organisation reported: "It would be bad enough if the mistaken URLs in these examples were for a set of relatively obscure items on our site, but the lists include some of the most visited pages on archive.org and materials that obviously have high scholarly and research value."[27] The current French government is trying to advance a proposal that will force Internet companies to remove content within an hour of an official government request.[28] Following the described failure of the French authorities to correctly identify these sites, the dangers inherent in this proposal are clear.

SURVEILLANCE

The number of legal tools allowing electronic surveillance has increased, and they have changed dramatically since the introduction of French surveillance legislation in 2015.[29] The law gives the power of surveillance, without a court order, to several security agencies.[30] It allows them to install information-gathering devices with artificial intelligence (AI) powers in order to gather meta-data and identify terrorism threats. The law allows the targeting of not only those identified as a security threat, but also people who are related to these suspects or even likely to be related to them.[31]

The 2016 law on 'the fight against terrorism and organised crime' gave prosecutors and judges powers of electronic surveillance that,

26 Chris Butler, 'Official EU Agencies Falsely Report More Than 550 Archive.org URLs as Terrorist Content', *The Internet Archive Blog*, April 2019, https://blog.archive.org/2019/04/10/official-eu-agencies-falsely-report-more-than-550-archive-org-urls-as-terrorist-content accessed 24 May 2019.

27 Ibid.

28 Ryan Browne, 'New Zealand And France Unveil Plans To Tackle Online Extremism Without The US On Board', *CNBC*, May 2019, www.cnbc.com/2019/05/15/new-zealand-france-unveil-plans-to-tackle-online-extremism-without-us.html accessed 17 May 2019.

29 See Note 14.

30 LOI N° 2015-912 Du 24 Juillet 2015 Relative Au Renseignement.

31 'Aperu De L'amendement', *Sénat*, July 2016, www.senat.fr/amendements/commissions/2015-2016/803/Amdt_COM-15.html accessed 13 May 2019.

up to that point, were only reserved for the intelligence services.[32] In 2011, an amendment to the order of criminal procedure gave police investigators, with the agreement of the court, permission to install 'Trojan horse' software on the computers of terrorist suspects.[33]

CRIMINAL LAW

The main criminal offence that is used in France in connection to terrorist activity on the Internet is 'apology for terrorism', in the sense of advocating for terrorism. While this offense has existed in France since the French Press Law of 1881, its enforcement was restricted and limited until the 2014 counter-terrorism law.[34] Since then, it specifies that this crime is punishable by up to seven years in prison and a €100,000 fine, if committed online.

Following the *Charlie Hebdo* attacks in January 2015, the Justice Minister issued a directive[35] to prosecutors to extend the fight against 'hateful' speech, while referring directly to the crime of 'apology for terrorism'. The result was swift, and the number of cases increased dramatically. Interior Ministry statistics[36] show that the police opened investigations into more than 2,300 suspected cases relating to apology for terrorism in 2015 and 1,850 in 2016. The Justice

32 LOI N° 2016-731 Du 3 Juin 2016 Renforçant La Lutte Contre Le Crime Organisé, Le Terrorisme Et Leur Financement, Et Améliorant L'efficacité Et Les Garanties De La Procédure Pénale.

33 Décret N° 2011-1431 Du 3 Novembre 2011 Portant Modification Du Code De Procédure Pénale (Partie Réglementaire: Décrets Simples) Pris Pour L'application De L'article 706-102-6 De Ce Code Relatif À La Captation Des Données Informatiques.

34 See Note 12.

35 'Ministry Of Justice Publications', *Ministère de la Justice*, January 2015, www.justice.gouv.fr/publication/circ_20150113_infractions_commises_suite_ attentats201510002055.pdf accessed 25 May 2019.

36 'Insécurité Et Délinquance En 2016: Premier Bilan Statistique', *Ministère l'Intérieur*, January 2017, www.interieur.gouv.fr/Interstats/Actualites/Insecurite-et-delinquance-en-2016-premier-bilan-statistique accessed 29 May 2019.

Ministry statistics show that, in 2016 alone, there were 306 convictions – with resulting prison sentences in 232 of those.

In 2018, the French Constitutional Court rejected[37] a challenge to the law brought by Jean-Marc Rouillan, an ex-member of the French leftist terrorist organisation 'Action Directe'. Rouillan said after the 2015 attacks that, although he condemned the action of the terrorists and their ideology, he can appreciate their courage. For this Rouillan was sentenced to 18 months in jail.

Another borderline case[38] was that of a vegan activist who, following the attack in Trèbes in 2018 where a butcher was killed, posted on Facebook: "It shocks you that an assassin is killed by a terrorist? Not me, I have zero compassion for him. There is justice after all." The court found her guilty and she was given a seven-month suspended sentence. Following the same event, a former member of the French political party 'La France Insoumise', wrote on Twitter, after it was found that a policeman had been killed: "Whenever a policeman is shot [...] I think of my friend Rémi Fraisse [a young environmental activist killed in 2014 by a policeman] still ... one less voter for Macron." The ex-politician received a one-year suspended prison sentence.[39]

These rulings, which are intended to define the limits of free speech, were accompanied by attempts by the French government to criminalise the action of visiting websites that are considered 'pro terrorist'. The 2016 law[40] was rejected in 2017 by the

37 'Décision N° 2018-706 QPC Du 18 Mai 2018', *Conseil Constitutionnel*, May 2018, www.conseil-constitutionnel.fr/decision/2018/2018706QPC.htm accessed 22 May 2019.

38 'Une Militante Vegan Condamnée Pour «Apologie Du Terrorisme» Après Un Message Sur Le Boucher Du Super U De Trèbes', *Libération*, March 2018, www.liberation.fr/direct/element/une-militante-vegan-condamnee-pour-apologie-du-terrorisme-apres-un-message-sur-le-boucher-du-super-u_79754 accessed 21 May 2019.

39 'Apologie Du Terrorisme: Un An De Prison Avec Sursis Pour Poussier (Ex-LFI)', *Le Point*, March 2018, www.lepoint.fr/politique/apologie-du-terrorisme-un-an-de-prison-avec-sursis-pour-poussier-ex-lfi-27-03-2018-2205942_20.php accessed 26 May 2019.

40 See Note 32.

Constitutional Council amid claims that the *mens rea*[41] elements of it were too vague and unclear. An attempt to amend the law was rejected again by the Constitutional Court in December 2017.[42]

Some see irony in the fact that all the legal actions that put restraints on freedom of speech started after the January 2015 attack on *Charlie Hebdo*, a publication that became a symbol of freedom of expression because it insisted on its right to be irreverent and insensitive.[43] These developments were addressed recently by Fionnuala Ní Aoláin, the UN Special Rapporteur on Counter-Terrorism and Human Rights, who was concerned by the vague nature of the criminal prohibitions in the French counter-terrorism criminal law: "Precision is essential in the use of exceptional counter-terrorism powers, and ambiguity must be remedied to ensure adherence to international human rights obligations."[44]

ADMINISTRATIVE MEASURES

The administrative legal system in France is a separate legal branch that originated in the French Revolution. It has three separate court instances[45]: First Instance, Court of Appeal and Supreme Court. The administrative judges are administrators who are not required

41 'Mens rea' is defined by the *Oxford Dictionary of Law* as '[t]he state of mind that the prosecution must prove a defendant to have had at the time of committing a crime in order to secure a conviction. Latin: a guilty mind.' Law, J. (Ed.), *A Dictionary of Law*, OUP Oxford, 2015.

42 'Décision N° 2017-682 QPC Du 15 Décembre 2017', *Conseil Constitutionnel*, December 2017, www.conseil-constitutionnel.fr/decision/2017/2017682QPC.htm accessed 29 May 2019.

43 Nadim Houry, 'France's Creeping Terrorism Laws Restricting Free Speech', *Human Rights Watch*, May 2018, www.hrw.org/news/2018/05/30/frances-creeping-terrorism-laws-restricting-free-speech accessed 27 May 2019.

44 David Sullivan, 'The Consequences of Legislating Cyberlaw After Terrorist Attacks', *Just Security*, April 2019, www.justsecurity.org/63560/the-consequences-of-legislating-cyberlaw-after-terrorist-attacks accessed 27 May 2019.

45 There are 44 first instance courts and 8 courts of appeal.

to hold a law degree.[46] A major part of the French legal response to the terrorist attacks has consisted of giving more legal powers to the administrative branch, a situation that reached its peak during the state of emergency (2015–2017).[47] Most of those powers were given permanently to the state after the end of the state of emergency via the 2017 counter-terrorism law.[48]

The administrative powers were used mainly to perform surveillance without a court order, to issue warrants which prevent citizens leaving the country,[49] warrants for house arrests[50] and warrants limiting communication. Those warrants are based on intelligence gathered by the Ministry of the Interior and the security agencies. A good deal of this intelligence is gathered through monitoring the online activities of the suspects involved. If the administrative warrant is challenged, the intelligence is presented to the administrative court in the form of what is called '*notes blanches*' as evidence. The *note blanche* is an anonymous report that summarises the intelligence findings and is the only evidence presented to the administrator judge in order to examine the need for the administrative warrant. Administrative judges have confirmed their total dependency on *notes blanches* as evidence without the need to examine their content.[51] A more principled criticism relates to the pre-emptive nature

46 Ordonnance N° 2016-131 Du 10 Février 2016 Portant Réforme Du Droit Des Contrats, Du Régime Général Et De La Preuve Des Obligations.

47 Sharon Weill, 'Terror In Courts. French Counter-Terrorism: Administrative And Penal Avenues', *Antiterrorisme, Droits et Libertés*, May 2018, https://antiterrorisme-droits-libertes.org/spip.php?article44 accessed 7 May 2019.

48 See Note 13.

49 As of April 2016, 308 travel bans had been issued and, in December 2017, the number reached 500.

50 Under the state of emergency laws, 521 house arrest warrants have been issued, and 20 under the new law.

51 ''Conseil D'état, Juge Des Référés, 06/01/2016, 395622, Inédit Au Recueil Lebon', *Légifrance*, January 2016, www.legifrance.gouv.fr/affichJuriAdmin.do?idTexte=CETATEXT000031861482 accessed 25 May 2019.

of the administrative powers as pre-emptive justice, since the subjects of the administrative warrants have not yet performed any illegal actions and are only suspected of *planning* them.[52]

52 See Note 46.

GERMANY

THE LEGAL SYSTEM OF GERMANY, THE RIGHT TO PRIVACY AND THE RIGHT TO FREEDOM OF SPEECH

Germany is a federal, parliamentary constitutional republic. The 1949 constitution, the basic law,[53] lays down the principal legal foundations of the country, such as the separation of powers, the federal structure, guarantees for human dignity and the rule of law. The basic law can be changed only with a special majority of the federal parliament.[54]

The Federal Constitutional Court is in charge of observing the constitutionality of legislation. If a lower court finds that a law is incompatible with the constitution, a judicial review proceeding can be brought before the Federal Constitutional Court. The Federal Constitutional Court is the only court that can rule that a law that was already enacted is in contradiction with the constitution and is therefore not valid. As part of the continental law system, the lower courts are not bound by precedents but, generally, rulings by a higher court are respected.

A specific article in the German constitution (Article 10) is dedicated to the right to 'privacy of correspondence, posts and telecommunications'. This right is not absolute and can be limited by law in order to protect 'the existence or security of the Federation or of a Land'. In a decision of the German Federal Constitutional Court from 1983,[55] the court ruled that, based on Articles 1

53 'The Basic Law', *The Federal Government*, 2019, www.bundesregierung.de/breg-en/chancellor/basic-law-470510 accessed 10 July 2019.

54 Some articles require a 2/3 majority while others require an absolute majority.

55 BVerfGE 65, 1 – Volkszählung Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden.

(human dignity) and 2 (personality right) of the constitution, every German has the right to determine, in principle, the disclosure and use of his or her personal data. This right was called by the court the right to 'informational self-determination'and was understood as "the authority of the individual to decide himself, on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others".

The right to freedom of speech is protected by Article 5 of the German constitution, which declares that every person shall have the right to "express and disseminate his opinions in speech, writing and pictures, and to inform himself without hindrance from generally accessible sources". The same article protects the freedom of the press and forbids censorship. This article can also be limited by law in order to protect the safety of the state and, as explained below, the German legislature has been very active in this aspect.

GERMANY AND TERRORISM

Modern Germany has been affected by terrorism from several groups with different affiliations, although it has not suffered from as many attacks as other countries in this report, mainly since it is not part of any major internal political conflicts (unlike the UK and Ireland, Israel and Palestine, Spain and the Basque region, and so on). Up until the year 2000, terrorist attacks were largely carried out by leftist groups, the most prominent being 'The Red Army Faction', as well as right-wing and neo-Nazi groups and individuals, like the one that carried out the Oktoberfest bombing in 1980, and Palestinian terrorists like the 'Black September' group.

In recent years, Germany has experienced a wave of refugees and asylum seekers, the majority from Muslim countries. At its peak in 2016, 746,000 asylum applications were processed.[56] German

56 'Asylum Figures', *Bundesamt für Migration und Flüchtlinge*, 2019, www.bamf.de/EN/Themen/Statistik/Asylzahlen/asylzahlen-node.html accessed 12 July 2019.

authorities have predicted[57] two possible dangers arising from this, the first being the possibility of jihadi terrorists radicalising some of the asylum seekers, and the second being a violent response to the immigration wave by extreme right-wing groups. Both predictions have proved right. In 2016, there was a wave of attacks by radicalised jihadi terrorists. The worst of them was the Berlin truck attack that ended with 12 dead and 48 injured. Violent extreme right-wing activity has also dramatically increased – for example, the murder of the president of the district of Kassel by an individual with links to the terrorist group 'Combat 18' and the National Democratic Party of Germany.[58] A third active extremist movement comprises groupings and individuals who self-identify with the Citizens of the Reich (*Reichsbürger*) and Sovereigns (*Selbstverwalter*). Their ideology rejects the idea of the federal government and legal system, and their activity is usually limited to "verbal abuse, coercion, blackmail, resistance to law enforcement, document fraud and illegal possession of firearms".[59] In addition, it has been estimated that over a thousand German citizens joined the ISIS fighters in their self-proclaimed Islamic State. With the collapse of the caliphate, around 200 have returned to Germany and others have been arrested in camps in different states in the Middle East.[60]

57 'Brief Summary 2018 Report on the Protection Of The Constitution', *The Federal Government*, June 2019 www.bundesregierung.de/breg-en/service/information-material-issued-by-the-federal-government/brief-summary-2018-report-on-the-protection-of-the-constitution-1641850 accessed 7 July 2019.

58 'Germany: Extremism & Counter-Extremism', *Counter Extremism Project*, 2019, www.counterextremism.com/countries/germany accessed 2 July 2019.

59 Ibid.

60 'Inhaftierte IS-Kämpfer: Behörden Arbeiten An Haftbefehlen', *Tagesschau*, February 2019, www.tagesschau.de/inland/bundesregierung-is-kaempfer-strafverfolgung-101.html accessed 7 July 2019.

TERRORISM AND ONLINE EXTREMISM

According to the 2018 report[61] of the Federal Office for the Protection of the Constitution (BfV), out of 36,062 politically motivated offences in 2018, 14,088 were propaganda offences, which are mostly performed online. The report identifies that "members of the right-wing extremist scene and sympathisers make intensive use of the Internet, for example to advertise their campaigns, mobilise support for events or plan activities." The right wing is highly active on social media and is very active on YouTube – for example, the YouTube channel '*Der Volkslehrer*' (The People's Teacher), which had more than 60,000 subscribers in 2018.[62] The report also identified a rise in the online activity of ISIS and other jihadi terrorists, claiming that "after a period of keeping a low profile, the scene in Germany has resumed its activity, especially on the messenger service Telegram".

THE STATE'S LEGAL RESPONSE

The rise of National Socialism, as well as the Second World War and its devastating consequences, of course had a profound impact on the shape of the modern German legal system. The response can be seen in the creation of a strong constitution with checks and balances between the different branches of the state. Understanding the importance of freedom of speech as an essential component in the democratic process has led to the inclusion of this right in the constitution. A different and, in a way, contrary lesson that was learned from that period in history is how dangerous the propaganda and incitement of anti-democratic forces can be to democracy. This lesson has led to the German legal system's heightened intolerance, as compared to other western democracies, when it comes to propaganda incitement and hate speech. The German criminal code[63]

61 See Note 57.

62 The channel was closed by YouTube in 2019.

63 'German Criminal Code', *Gesetze im Internet*, www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html accessed 11 July 2019.

includes several articles, dating from as early as the 1950s, which limit freedom of speech in the name of the protection of democracy. Section 86 forbids the dissemination of propaganda material by unconstitutional organisations, while Section 86a forbids the use of the symbols of unconstitutional organisations (e.g. the swastika and other neo-Nazi symbols), with the ISIS flag added in 2014. Section 90a forbids the defamation of the state and its symbols such as its flag while Section 91 forbids the displaying or supplying of material "which by its content is capable of serving as an instruction to the commission of a serious violent offence endangering the state (Section 89a (1)), if the circumstances of its dissemination are conducive to awakening or encouraging the preparedness of others to commit a serious violent offence endangering the state". In addition, Section 111 forbids the inciting or committing of an unlawful act "publicly, in a meeting or through the dissemination of written materials", and Section 129a forbids the forming of a terrorist organisation.

Sections 130, 130a and 131 deserve special attention as they all deal directly with limitations on publication. Section 130, which is entitled 'incitement to hatred', forbids the inciting of hatred against a national, racial, religious or ethnic group, forbids insulting someone based on being a member of one of those groups, and forbids the public approval, denying, or downplaying of an act committed under Nazi rule. Section 130a forbids the dissemination, public display, posting, presenting or otherwise making accessible of material that could serve as an instruction for an unlawful act and intended by its content to encourage or cause others to commit such an act. Section 131 forbids the dissemination of materials "which describe cruel or otherwise inhuman acts of violence against humans or humanoid beings in a manner expressing glorification or which downplays such acts of violence or which represents the cruel or inhuman aspects of the event in a manner which violates human dignity".

On 1 January 2018 the 'Network Enforcement Act'[64] (NetzDG) came into full force, whereby large social media companies are held

64 Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken – NetzDG.

responsible for enforcing and removing flagged content that breaches any of the 22 identified statutory offences existing in the German criminal code. A few amendments have also been made to the criminal code procedure to allow the authorities to use advanced methods of surveillance, as will be explained later. In August 2019, Section 28 of the Nationality Act was amended so that it will allow German nationality to be deprived from those who have dual nationality and who joined militias in Syria or Iraq as foreign fighters.[65]

BLOCKING AND REMOVAL OF ONLINE CONTENT

The NetzDG aims to impose German criminal law standards regarding content on the large social media companies with more than two million registered users in Germany. The law creates a binding mechanism of blocking or removing illegal content from the social networks. Illegal content in the context of the NetzDG is defined as content whose publication is illegal according to the 22 sections of the German criminal code. Content that is identified as 'manifestly unlawful' should be dealt with immediately and the content must be removed or blocked within 24 hours of receiving the complaint. The rest of the unlawful content should be blocked or removed within seven days. A decision about accepting the complaint, or rejecting it, should be given to the complainant during that time period. Section 2 contains a reporting obligation; namely, a company that receives more than 100 complaints per year must also produce, twice a year, a report showing its efforts to reduce such content. Failing to keep to the standards of the law could result in heavy fines of up to €50 million. Indeed, in July 2019, Germany's Federal Office of Justice (BfJ) issued a regulatory fine of €2 million against Facebook for violating the provisions of the NetzDG. The BfJ cited that Facebook provided 'incomplete' information in its transparency report for the first half of 2018. The BfJ argued that this was likely due to its dual reporting structure, which seems to prioritise reporting content according to violations of

65 'Staatsangehörigkeitsgesetz', *Gesetze im Internet*, www.gesetze-im-internet.de/stag/StAG.pdf accessed 2 December 2019.

Facebook's Community Standards, rather than through the NetzDG. In addition to this, Facebook was accused of inaccurately reporting on measures to inform complainants and users.[66]

The NetzDG has been criticised by activists and academics, fearing that it will limit possibilities for Germans to participate in dialogue with people from other countries where there are less limits on freedom of speech. Another fear was that social media companies, in order to protect themselves from potential fines, will be overzealous in their content removal[67] and the dangers of political involvement in it.[68] Facebook, Twitter and YouTube have published bi-annual reports on their activity with regard to the NetzDG and it seems that the law is more relevant to Twitter and YouTube (which reported on more than 200,000 complaints in the first six months) compared to Facebook (which reported on 1,700 complaints and found only 21% of the complaints justifiable).[69] Nearly two years after the NetzDG came into force, the German government put forward proposals in October 2019 to extend the law to oblige social media companies to not only remove, but also report, illegal content to a dedicated special unit at the Federal Criminal Police Office. The providers would also be obliged to transmit the IP addresses of the senders of such postings.[70]

66 'Federal Office Of Justice Issues Fine Against Facebook', *Bundesamt für Justiz*, July 2019, www.bundesjustizamt.de/DE/Presse/Archiv/2019/20190702_EN accessed 2 December 2019.

67 'Netzdg As A Source Of Censorship – A Summary Of Recent Effects', *HÄRTING Rechtsanwälte*, September 2018, www.haerting.de/neuigkeit/netzdg-source-censorship-summary-recent-effects accessed 14 July 2019.

68 Wolfgang Schulz, 'Roles And Responsibilities Of Information Intermediaries', *Lawfare*, November 2019, www.lawfareblog.com/roles-and-responsibilities-information-intermediaries accessed 2 December 2019.

69 'Facebook: We've Removed Hundreds Of Posts Under German Hate Speech Law – CNET', *NewsFlash*, July 2018, https://newsflash.one/2018/07/27/facebook-weve-removed-hundreds-of-posts-under-german-hate-speech-law-cnet accessed 16 July 2019.

70 'Bundesregierung Geht Gegen Rechtsextremismus Und Hasskriminalität Vor', *The Federal Government*, 2019, www.bundesregierung.de/breg-de/aktuelles/gegen-extremismus-und-hass-1686442 accessed 2 December 2019.

SURVEILLANCE

The issue of online surveillance powers in Germany has also been under scrutiny since the exposure of the Edward Snowden documents in 2013.[71] Three major laws regulate surveillance practices in Germany. The 2016 amendment to the Federal Intelligence Service Act (BND law)[72] allows German intelligence to monitor Internet traffic of foreigners abroad in order "to identify and combat risks, at an early stage, to the domestic or foreign security of the Federal Republic of Germany, to guarantee the Federal Republic of Germany's capacity to act, or to gain intelligence."[73] Critics of the law say that the law allows the intelligence services to use bulk surveillance methods which also gather information on German citizens. In 2018, Reporters without Borders filed a complaint to the European Court of Human Rights (ECtHR) over the mass surveillance practices of Germany's foreign intelligence agency under the BND Law.[74] A second law that deals with surveillance is the 'Act on Restrictions on the Secrecy of Mail, Post and Telecommunications', also known as the 'G-10 Act' as it limits the scope of Article 10 in the German constitution, which protects the privacy of communications. In 2016, there were more than 4,000 electronic surveillance warrants issued by the intelligence services based on the G-10 Act, while only 1% of them resulted in further inquiry. These results of the use of the law have led to Amnesty International filing a complaint with the Federal Constitutional Court, arguing that the interpretation of the law by the security services has been too

71 'The NSA Files', *The Guardian*, 2013, www.theguardian.com/us-news/the-nsa-files accessed 1 July 2019.

72 'Federal Intelligence Service Act', *Global-Regulation*, www.global-regulation.com/translation/germany/385659/the-federal-intelligence-service-act.html accessed 4 July 2019.

73 Section 2 of the BND Law.

74 'RSF Lodges ECHR Complaint Over German Foreign Intelligence Agency's Mass Surveillance', *RSF Reporters Without Borders*, December 2017, https://rsf.org/en/news/rsf-lodges-echr-complaint-over-german-foreign-intelligence-agencys-mass-surveillance-0 accessed 4 July 2019.

extensive.[75] The 'Online Search' (*Online-Durchsuchung*[76]) is the third measure that has a direct effect on the surveillance powers of the state. The measure enables security forces with a court order to install 'Trojan horse' programs on suspects' devices that can gather data in order to investigate potential acts of terrorism.

CRIMINAL LAW

According to Europol's *European Union Terrorism Situation and Trend Report 2018* (TESAT),[77] the total number of clear-cut terrorism cases brought in front of German courts in the years 2015, 2016 and 2017 was relatively low (17, 30 and 33 respectively). The cases are divided into felonies regarding participation in a terrorist organisation and felonies regarding supporting a terrorist organisation, mostly via online platforms. The interpretation of the supporting terrorist organisation felony (Section 129 (5) of the German criminal code) has been limited by the German courts. For example, take the case of where a person had posted a link to a video showing the beheading of an American hostage, followed by a talk by Musab al-Zarqawi calling for the killing of all foreigners. The lower court found the defendant guilty of providing support to a terrorist organisation, according to Section 129(5). The Federal Supreme Court overturned the conviction on this article however, finding that the posting of the video did not result in a tangible benefit for the terrorist organisation and therefore the defendant should have been convicted according to Section 131

75 Kai Biermann, 'Amnesty klagt gegen Überwachungsgesetz' [Amnesty files complaint against surveillance law], *Zeit Online*, November 2016, www.zeit.de/digital/datenschutz/2016-11/bnd-ueberwachung-verfassung-g10-klage accessed 5 July 2019.

76 A measure enabled through the Federal Criminal Police Office Act (BKA Gesetz).

77 'European Union Terrorism Situation and Trend Report 2018 (TESAT 2018)', *Europol*, June 2018, www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018 accessed 5 July 2019.

that deals with dissemination of glorifying materials,[78] which is a less severe felony. The German courts' approach towards the publication of terrorist materials has been criticised as intolerant. For example, Petzsche and Malie[79] have suggested that the state cannot differentiate between what they describe as 'terrorist speak' and 'speaking about terrorism'. While the first is part of a terrorist plan and organisation and therefore should be stopped, the other should be protected by freedom of speech.

This issue is highlighted more dramatically when examining the German criminal legal system's approach to extremist speech and hate speech online. As already mentioned, the 2016 refugee crisis evoked a wave of right-wing hate speech online. While in 2015, there were 2,670 convictions for hate speech, in 2016, the number rose to 6,014 cases, most of them against right-wing activists attacking immigrants and leftists online. The criminalisation of hate speech online does not seem to have produced the deterrence the state was looking for, as according to the BfV report, the numbers of online criminal cases continued to rise during 2017 and 2018. Germany's vigorous criminalisation of speech has also been criticised in a special report by Article 19,[80] a global NGO promoting freedom of speech worldwide. According to the report,[81] the German criminal code contains too many different felonies regarding limitations on speech, which can create confusion, and the court interpretations of those laws are not unified and place much more attention on the question of 'pursuit of truth' in publications rather than on the question of intent or possible harm.

78 BGH 3 StR 314/12 – Beschluss vom 20. September 2012.

79 Chapter 10 in Genevieve Lennon, Colin King and Carole McCartney (Eds.), *Counter-Terrorism, Constitutionalism and Miscarriages Of Justice*, November 2018, Bloomsbury Publishing.

80 For more, see www.article19.org accessed 5 December 2019.

81 'Germany: Responding to 'Hate-Speech'', *ARTICLE 19*, 2018, www.article19.org/wp-content/uploads/2018/07/Germany-Responding-to-%E2%80%98hate-speech%E2%80%99-v3-WEB.pdf accessed 8 July 2019.

ADMINISTRATIVE MEASURES

Germany's administrative counter-terrorism measures have concentrated on improving control at the entry and exit points to and from Germany. A few laws have been amended, such as the Federal Act on the Protection of the Constitution, the Military Counterintelligence Service Act, the Federal Intelligence Service Act, the Federal [Border] Police Act, the Federal Office of Criminal Police Act, and the Foreigners Act in order to allow the prevention of entry for those who have been identified as supporters of terrorism. In addition, the police and security forces have been given the power to withhold passports and identity cards from those who were suspected of planning to join the fighters in Syria.[82] As in most administrative pre-emptive procedures, the evidence to be provided in order to justify the measures is secret and often based on the online activity of the person subjected to the measures. Some of those measures have been criticised as targeting only potential Islamic terrorists and ignoring potential right-wing violence.[83]

82 'Profiles On Counter-Terrorist Capacity: Germany', *Council of Europe*, September 2016, https://rm.coe.int/1680641010 accessed 12 July 2019.

83 Kilian Roithmaier, 'Germany and Its Returning Foreign Terrorist Fighters: New Loss Of Citizenship Law And The Broader German Repatriation Landscape', *The International Centre for Counter-Terrorism*, April 2019, https://icct.nl/publication/germany-and-its-returning-foreign-terrorist-fighters-new-loss-of-citizenship-law-and-the-broader-german-repatriation-landscape accessed 9 July 2019.

ISRAEL[84]

THE ISRAELI LEGAL SYSTEM, THE RIGHT TO PRIVACY AND THE RIGHT TO FREEDOM OF SPEECH

Israel is a parliamentary democracy with no official constitution. The Israeli legal system inherited common law from British rule, albeit with some differences, such as there being no jury system in addition to all rulings being made by professional judges. The Israeli Supreme Court sits both as the High Court of Appeals and the High Court of Justice. Under specific guidelines, every resident can petition against the state in the High Court of Justice.

In 1992, the Israeli parliament brought in two basic laws regarding human rights that the High Court understood as enabling it to overrule the parliament's regular legislation.[85] The laws refer directly to the right to privacy[86] but do not mention the right to freedom of speech, which is not mentioned in any law of the Israeli legal codex. The Israeli High Court of Justice has, however, since 1953, recognised the right to freedom of speech as part of the basic rights of every Israeli.[87] The ruling was reaffirmed on several later occasions and the High Court described the right as the 'heart and soul of democracy'.[88] The court also ruled on several occasions however that both rights,

84 This report will examine Israeli legal activity as applied within the 1948 ceasefire agreement border. The legal activities of Israel as an occupier in the Palestinian occupied territories are governed by a military legal system that cannot be compared to Western democratic legal systems.

85 Justice Aharon Barak, 'A Constitutional Revolution: Israel's Basic Laws' (2011) 4 *Constitutional Forum / Forum Constitutionnel*.

86 Article 7 of the Basic Law: Human Dignity and Liberty 1992.

87 *73/53 Kol Ha'am v Minister of Interior* (1953) HCJ, 7 Padi (HCJ).

88 Barak, A. 'Human Rights In Israel' (2006) 39 *Israel Law Review.*

the right to privacy and freedom of speech, are not absolute and can be limited by other rights or interests.[89]

ISRAEL AND TERRORISM

The history of terrorism in Israel has always been connected to the Israeli–Palestinian conflict. Both Palestinian organisations and right-wing Jewish organisations have been involved in attacking citizens throughout the history of Israel, especially since the 1967 war and the occupation of the Palestinian territories. Terrorist attacks in Israel reached a peak during the second Intifada of 2000–2005. Although terrorism didn't end in 2005, the next significant wave of terrorism started with the 2014 Gaza War and 2015–2016 'Knife Intifada', which was a wave of knife attacks by Palestinian attackers who did not identify with a specific organisation.[90] This period also included right-wing Jewish attacks on Palestinians as part of the so-called 'Price Tag'[91] actions.

INTERNET ACTIVITY RELATING TO ATTACKS

Although both Israelis and Palestinians have been accusing each other of promoting incitement online since the Internet arrived in the region, a surge in online extremism, with a direct influence on terrorism, became apparent during the 2014 operation 'Brother's Keeper' and during the Gaza War.[92] This extremist online activity, both Palestinian and Jewish right-wing, has been directly linked

89 Ibid.

90 During that period, 38 Israeli citizens were killed along with more than 150 Palestinian attackers or alleged attackers.

91 'Price Tag' actions are terrorist activities carried out by right-wing Jewish individuals or groups mainly targeting the property of Palestinians in villages in Israel and in the Occupied Palestinian Territories. Between the years 2012 and 2017, there were around 700 documented such attacks yearly.

92 Inna Lazareva, 'Far-Right Extremism on the Rise In Israel As Gaza Conflict Continues', *The Telegraph*, July 2014, www.telegraph.co.uk/news/worldnews/middleeast/israel/10992623/Far-Right-extremism-on-the-rise-in-Israel-as-Gaza-conflict-continues.html accessed 13 June 2019.

by the security forces to several terrorist attacks and other violent behaviour.[93] At that time, 2014–2016, Facebook was the main platform that hosted Israeli and Palestinian extremists, and the platform was used as a tool to incite, recruit and conspire; recently Twitter has become more popular.[94]

THE STATE'S LEGAL RESPONSE

The history of terrorism in Israel can be traced back in its legal system to the country's first days. The first legal codex adopted British criminal law, which included the felony of 'calling to insurrection'.[95] In September 1948, a few months after Israel declared independence, the UN ambassador to the region was murdered by Jewish right-wing terrorists. The legal response was quick and, a few days later, the 'order of prevention of terror' was declared, making it illegal to publish any support for a terrorist organisation, its actions, its symbols and its members.[96] In response to the rise of Palestinian activity nationwide in the 1980s, and the formation of the Kahana right-wing party, the felonies of 'incitement to racism' and 'incitement to violence' were introduced into law, which also prohibited holding and distributing inciting materials.[97] The first serious wave of indict-

93 'Wave Of Terror 2015–2019', *Israel Ministry of Foreign Affairs*, December 2019, https://mfa.gov.il/MFA/ForeignPolicy/Terrorism/Palestinian/Pages/Wave-of-terror-October-2015.aspx accessed 14 June 2019.

94 Noa Landau and Oded Yaron, 'Justice Minister: Terror Groups Have Switched to Twitter Because Facebook Cooperates With Israel', *Haaretz*, March 2018, www.haaretz.com/israel-news/.premium-shaked-terror-groups-use-twitter-because-facebook-works-with-israel-1.5918301 accessed 13 June 2019.

95 Article 136 of the Israeli Penal Code defines insurrection as: (1) the promoting of hatred, disdain or disloyalty to the State or its duly constituted governmental or legal authorities; (2) inciting or provoking the inhabitants of the country in an attempt to obtain, by improper means, the change of a matter established by law; (3) arousing dissatisfaction among the inhabitants of the country; (4) provoking strife and hostility between different parts of the population.

96 Article 4 of the Order of Prevention of Terror 1948.

97 Articles 144A-E of the Israeli Penal Code 1977.

ments involving these sets of felonies followed the murder of the Israeli Prime Minister, Yitzhak Rabin, in 1995. In a series of cases that reached the Supreme Court, the court ruled that, because these felonies limit the right to freedom of speech, they should be used and interpreted in a very strict manner, which led to the very moderate use of the felonies by Israeli prosecutors.[98]

Following these cases and the court's criticism of the use of the 1948 Prevention of Terror order, the article relating to 'support of terror organisations' was changed to 'incitement to violence and terror', which made it illegal to support any kind of terrorism with or without a connection to a specific terrorist organisation.[99] With regard to all of these felonies, the High Court was conflicted about the question of causality. Some judges felt the expression should be 'a clear and immediate danger to violence', while others talked about 'close probability' or 'concrete probability'.[100] Following the 2014–2016 violence, a new criminal law was brought in, 'the law against terrorism', which replaced the 1948 order against terrorism. The law includes a specific article that forbids 'identification with a terrorist organisation and incitement to terrorism'.[101]

BLOCKING AND REMOVAL OF ONLINE CONTENT

Israel's blocking and removal of online content is based mainly on its connections with tech companies. Israeli web provider companies have strict filtering protocols for blocking access to content like child pornography and terrorist sites. Since 2015, and the rise in awareness of incitement on social networks, Israeli cyber departments have

98 Daphne Barak-Erez and David Zechariah, 'Incitement To Terrorism And The Boundaries Of Freedom Of Speech: Between Direct And Indirect Restrictions', *Tel Aviv University Law Review*, 35, 2013.

99 The Amended Article 4 the Order of Prevention of Terror 1948.

100 Michael Birnhack, *Be Quiet! Someone Is Speaking: The Legal Culture of Freedom of Speech*, Tel Aviv University, 2006.

101 Article 24 of the Law against Terrorism 2016.

established a productive relationship with Facebook and Twitter.[102] A Facebook representative noted that the company works "very closely with the cyber departments in the justice ministry and the police and with other elements in the army and the Israeli Security Agency."[103] In 2017, Facebook and Twitter accepted 85% of the Israeli cyber units' 12,351 requests to remove content deemed harmful or dangerous by the Israeli authorities.[104] Even though this solution seems to work quite effectively, the Israeli Ministry of Justice has been advancing a new law to deal with content blocking and removal. The 'law for the removal of content from the Internet whose publication constitutes an offense', or its popular name 'The Facebook Law', is in the last stages of legislation in the Israeli parliament.[105] The law allows the cyber departments to appeal to the Israeli administrative court to issue a warrant to the company or host of online content to remove the content. This law has been subject to criticism from NGOs, legal scholars and Internet companies for its wide definitions.[106] The proposed law allows the court to issue a warrant regarding content that is published on any platform and in any country without any Israeli geographical or objective connection. The law allows a request to remove content that has the potential to harm a person, public safety or the security of the state, which are all very wide definitions that can be interpreted in different ways.

102 'Hashtag Palestine 2018: Digital Rights Of Palestinians Between Restrictive Legislations And The Complicity Of Internet Companies', *7amleh*, March 2019, https://7amleh.org/2019/03/26/hashtag-palestine-2018-digital-rights-of-palestinians-between-restrictive-legislations-and-the-complicity-of-internet-companies accessed 20 April 2019.

103 'Facebook Doesn't Listen To Your Phone', *Calcalist*, December 2017, www.calcalist.co.il/local/articles/0,7340,L-3728279,00.html accessed 16 June 2019.

104 'Social Media Giants Continue To Collaborate With Israel's Illegal 'Cyber Unit'', *Adalah*, December 2018, www.adalah.org/en/content/view/9652 accessed 12 June 2019.

105 The law passed from the constitutional committee to the last stage of legislation on 14 July 2018.

106 Tehilla Shwartz Altshuler, 'The Facebook Bill Must Be Amended So That It Can Serve Its Original Purpose', *The Israel Democracy Institute*, July 2018, https://en.idi.org.il/articles/24237 accessed 14 June 2019.

SURVEILLANCE

The Israel National Cyber Directorate was established in 2017 by a decision of the government.[107] The directorate combined two previous cyber authorities in charge of the protection and advancement of cyber space.[108] As such, the cyber authority is constantly scanning the Internet activity of millions of users without a specific law to regulate its power.

In 2007, the Israeli parliament brought in the Criminal Procedure Law (Enforcement – Communication Data), known as the 'Big Brother Law'. The law allows the police and other security services to issue a warrant to communication providers, such as cell phone companies and Internet providers, with a view to exposing personal information of its end users in terms of phone and online activities. The warrant can be issued for 24 hours with the approval of a police officer and for longer periods with the approval of a judge, while the only criteria needed for approval is *suspicion* of any crime.[109] There has been a sharp rise in these requests since 2014. While, during the first few years of the law, there were around 8,000 requests a year, in recent years, the number has reached almost 30,000 a year.[110]

CRIMINAL LAW

As already mentioned above, the Israeli prosecution policy on criminalisation when it comes to online publications has changed dramatically since the 2014 Gaza War and the 2015–2016 so-called 'Knife Intifada'. In the years previous to 2015, there had been only a few cases a year, if any, regarding the felony of incitement to violence, racism or terrorism, but since 2015, the number has risen to more than 100 a year, dealing mostly

107 Israeli Government Decision No. 3270 from 17 December 2017.

108 'About Israel National Cyber Directorate', *GOV.IL*, 2017, www.gov.il/en/departments/about/newabout accessed 11 June 2019.

109 Articles 3–6 in the Criminal Procedure Law (Enforcement – Communication Data) 2007.

110 Amitai Ziv, 'Police Obtaining More Phone Data, Personal Information', *Haaretz*, January 2018, www.haaretz.com/israel-news/police-obtaining-more-phone-data-personal-information-1.5729384 accessed 15 June 2019.

with posts on social networks.[111] While the Israeli security services have praised this policy and credited it with leading to a decline in violent actions, others have been more critical of it and have identified two major problems in the policy.

The first problem is that prosecution in Israel is devoted almost solely to the Palestinian population. Out of hundreds of cases that have been brought in front of the Israeli courts since 2015, fewer than ten defendants were Israeli Jews while the rest were Palestinians, even though they make up only 20% of the population of the country.[112] This could be explained if there was no online extremist incitement activity by Israeli Jews, but the reality is quite different. The 'Hate Report', a project that monitors online incitement in Hebrew, has found that 90% of online incitement in Hebrew is directed against Palestinians, African asylum seekers and leftists. In 2016, it identified 170,000 such comments and a third of those comments were direct calls for murder.[113]

The second problem regarding Israeli indictment policy is that, while it shows great leniency to the online expressions of Israeli Jews, it shows almost no leniency when it comes to the right to freedom of speech of Palestinian Israelis. Some of the cases that were brought to the court were questionable in terms of the potential harm they could produce. For example, in a series of cases, East Jerusalem Palestinians were accused of writing Facebook posts supporting Hamas. While Hamas is considered a terrorist organisation by Israel and some other countries, it is also the government for over two million Palestinians in the Gaza Strip, and has a highly active official online presence through websites and social media. In the case of Atta al Issa, a 21-year-old from Jerusalem, the charges were that he was

111 Shoshanna Solomon, 'Israel Getting Better Grip On Online Incitement, Justice Minister Says', *Times of Israel*, June 2017, www.timesofisrael.com/israel-getting-better-grip-on-online-incitement-justice-minister-says accessed 10 June 2019.

112 John Brown and Noam Rotem, 'Imprisoned For Incitement On Facebook? Only If You're Arab', *+972 Magazine*, July 2015, https://972mag.com/imprisoned-for-incitement-on-facebook-only-if-youre-arab/108720 accessed 6 June 2019.

113 'The Hate Report', *Berl Katznelson Center*, 2016.

a friend on Facebook of a student organisation that identified with Hamas and that he published on his Facebook account a picture of Hamas activists holding the Hamas flag that got 62 likes. He also posted a picture of a boy wearing a hat with the Hamas name on it and the text 'praise the lord' near it that got 55 likes. For these actions, he was sentenced to seven months in prison.[114] It is very difficult to assume that this particular online activity could cause violence under any test of probability, given that the Internet is full of official and active Hamas sites, Facebook accounts and Twitter pages.

Another example of prosecutorial overreach could be seen in the case of the Palestinian poet Dareen Tatour, who was charged with incitement for posting one of her poems on YouTube. The poem was entitled 'Resist Them' and was read with a background of a video showing clashes between Palestinian demonstrators and soldiers. The trial lasted for two years and raised questions relating to translating from Arabic to Hebrew. While in the Peace Court, the judge, who did not speak Arabic, accepted the prosecution claim that the song encouraged terrorist attacks,[115] the District Court bench, which included an Arab-speaking judge, reversed the decision.[116]

The question of the language barrier between Hebrew speakers and Arabic speakers, combined with the Israeli authorities' eagerness to spot Palestinian inciters, also came up in the arrest of the Palestinian activist Anas Abudaabes, who wrote a satirical post condemning Arabs from neighbouring countries. The court considered that the high language of the satirical piece could be misunderstood by non-educated readers as incitement.[117] Another example of the language barrier was the arrest of a farmer who posted

114 *42335-11-17 The State of Israel vs Atta al Issa* (2018) Peace Court, Beer Sheba (Peace Court, Beer Sheba).

115 *4480-11-15 The State of Israel vs Dareen Tatour* (2018) Peace Court, Nazareth (Peace Court, Nazareth).

116 *24933-09-18 Dareen Tatour vs The State of Israel* (2019) District Court, Nazareth (District Court, Nazareth).

117 John Brown, 'If You're Palestinian In Israel, Satire Can Land You In Jail', *+972 Magazine*, November 2016, https://972mag.com/if-youre-palestinian-in-israel-sarcasm-can-land-you-in-jail/123380 accessed 1 June 2019.

a picture of himself near his tractor with the text 'good morning to you'. The police artificial intelligence (AI) program translated the text by mistake as 'slaughter them' which, in combination with the picture of the tractor, introduced to the farmers arrest a suspicion of inciting terrorism through vehicle attacks. As none of the policemen involved in the arrest knew how to read Arabic, only the arrival of an Arab-speaking officer hours later led to the release of the farmer.[118]

ADMINISTRATIVE MEASURES

Unlike the common practice of administrative arrests in the Occupied Palestinian Territories, within Israel, administrative arrests and administrative measures are rare. One area where administrative powers are used against those whom the authorities deem to be online extremists is at the entry points to Israel. In recent years, there has been a huge rise in refusals at the entry points. In 2011, 2,000 were refused entry but in 2016, the number reached 16,534 without a dramatic increase in the number of people looking to enter.[119] 'Security reasons' is one of the main reasons given for refusal and many tourists report that they were asked to reveal their social network correspondence to the border guards in order to enter.[120]

118 Yotam Berger, 'Israel Arrests Palestinian Because Facebook Translated 'Good Morning' To 'Attack Them'', *Haaretz*, October 2017, www.haaretz.com/israel-news/ palestinian-arrested-over-mistranslated-good-morning-facebook-post-1.5459427 accessed 3 June 2019.

119 Ilan Lior, 'Searches, Detentions, Arbitrary Decisions: Israeli Refusal Of Visitors' Entry Surges 785%', *Haaretz*, February 2017, www.haaretz.com/israel-news/.premium-israeli-refusal-of-visitors-entry-surges-ninefold-in-five-years-1.5435357 accessed 12 June 2019.

120 Najwa Doughman and Sasha Al-Sarabi ''Do You Feel More Arab Or More American?': Two Women's Story Of Being Detained And Interrogated At Ben Gurion', *Mondoweiss*, June 2012, https://mondoweiss.net/2012/06/do-you-feel-more-arab-or-more-american-two-arab-american-womens-story-of-being-detained-and-interrogated-at-ben-gurion accessed 21 June 2019.

SPAIN

THE LEGAL SYSTEM OF SPAIN, THE RIGHT TO PRIVACY AND THE RIGHT TO FREEDOM OF SPEECH

Spain is a parliamentary monarchy, based on parliamentary representation. The end of Franco's dictatorship led to Spain approving a new constitution in 1978.[121] The constitution created a system of checks and balances between the judicial system, government and parliament. The King, who is officially the head of state, has a mainly ceremonial role, though his functions include international and national representation and arbitration between other state institutions. Legislative power belongs to the Spanish parliament, comprising two houses: the Congress of Deputies and the Senate. The executive power belongs to the government, which is led by an elected president.

The Constitutional Court is the highest court in the state for constitutional questions, while the Spanish Supreme Court is the highest court for every other issue. The Constitutional Court can examine the constitutionality of a law using several procedures such as a direct reference to examine the constitutionality of a law by state-specific bodies such as the parliament or the president, or a petition of a person whose fundamental rights and freedoms were violated by a law and they had exhausted all other judicial appeals (such as by Amparo Appeal).

Chapter 2 of the Spanish constitution discusses the protected rights of the Spanish people. Article 16 protects freedom of ideology. Article 18 protects the right to privacy, and specifically "secrecy of

121 'Constitution And Rules', *Congreso de los Diputados*, 1978, www.congreso.es/portal/page/portal/Congreso/Congreso/Hist_Normas/Norm accessed 28 July 2019.

communications is guaranteed, particularly of postal, telegraphic and telephonic communications, except in the event of a court order to the contrary".

Freedom of expression is protected in the constitution by a well-elaborated article (Article 20). The article protects "the right to freely express and disseminate thoughts, ideas and opinions through words, in writing or by any other means of communication". It specifically states that "the exercise of these rights may not be restricted by any form of prior censorship". The article also proclaims that "the law shall regulate the organisation and parliamentary control of social communications media under the control of the State or any public agency and shall guarantee access to such media to the main social and political groups, respecting the pluralism of society and of the various languages of Spain". A law that wishes to limit the scope of a right in the constitution is called an organic law and must pass with an absolute majority in order to do so.

SPAIN AND TERRORISM

Spain was affected by continuous terrorist attacks from the 1960s onwards, following the establishment of ETA, the Basque separatist terrorist organisation.[122] ETA attacks continued until 2011 when the organisation declared that it was abandoning the armed option and it finally dissolved in 2018. The total number of attacks – and casualties of ETA attacks – is disputed, as some unidentified attacks and some attacks by renegade organisations are sometimes accredited to ETA. However, the Spanish government's official numbers point to more than 3,000 attacks since the late 1960s, causing the death of 829[123] people with more than 2,000 wounded.[124] Other terrorist groups

122 William S. Shepard, 'The ETA: Spain Fights Europe's Last Active Terrorist Group', *Mediterranean Quarterly*, 13(1), 2002.

123 'Spain: Extremism & Counter-Extremism', *Counter Extremism Project*, 2019, www.counterextremism.com/countries/Spain accessed 12 July 2019.

124 Most of the ETA attacks targeted the security forces. However, among the 829 dead, there were 343 civilians.

that were active during the 1970s were GRAPO, who were Marxist Leninists, and the Galician Resistance. Spain was also, and is still, a target of jihadi terrorism from several terrorist organisations, including al-Qaeda and ISIL. The two most noted attacks were on 11 March 2004, when blasts from ten bombs killed 191 people on four Madrid-bound commuter trains,[125] and on 17 August 2017, when a van drove into a crowd of people in a popular tourist area of Barcelona, killing 13 and wounding more than 100 others.[126] The 2016 immigration wave has not by-passed Spain, and with it the right-wing reaction of extremism. One such group in Spain is 'Generación Identitaria', which believes it is defending European culture from the so-called 'Great Replacement'.[127] This group was identified by the Spanish government as encouraging violence against immigrants.[128] This reaction has taken on a political form in the success of the far-right populist Vox party in the most recent Spanish elections.

According to the Spanish Ministry of the Interior, since 2016, more than 230 citizens have joined fighters in Syria and Iraq and around 20% have returned to Spain and are under continuous surveillance by the Spanish security forces.[129]

125 Elaine Sciolino, 'Bombings In Madrid: The Attack; 10 Bombs Shatter Trains In Madrid, Killing 192', *The New York Times*, March 2004, www.nytimes.com/2004/03/12/world/bombings-in-madrid-the-attack-10-bombs-shatter-trains-in-madrid-killing-192.html accessed 24 December 2019.

126 Anne-Sophie Bolon, Palko Karasz and James C. McKinley Jr., 'Van Hits Pedestrians In Deadly Barcelona Terror Attack', *The New York Times*, August 2017, www.nytimes.com/2017/08/17/world/europe/barcelona-catalunya-van.html accessed 24 December 2019.

127 For a description of the 'Great Replacement', see www.nytimes.com/2019/08/06/us/politics/grand-replacement-explainer.html

128 See Note 122.

129 'International Terrorism Reports', *Ministerio del Interior*, 2016, www.interior.gob.es/en/web/interior/prensa/balances-e-informes/lucha-antiterrorista-contra-eta-y-el-terrorismo-internacional-xi-legislatura-2016- accessed 31 July 2019.

TERRORISM AND ONLINE EXTREMISM

Online radicalisation and propaganda have been of major concern to the Spanish authorities. In 2016, 'Islam en Español', a Facebook page that glorified ISIS and promoted militancy, had approximately 32,500 followers. The first ISIS video in Spanish was distributed online following the 2017 attacks.

In research carried out by Torres-Soriano,[130] a correlation was found between the amount of terrorist communication and propaganda online and the number of terrorist attacks, attempts and plots. Right-wing extremism is also using online platforms in order to spread its agenda and gain more influence and political power.[131]

THE STATE'S LEGAL RESPONSE

The laws that were used during the long conflict in the Basque country – and with ETA especially – have resulted in the Spanish criminal code[132] having a lot of articles that can be used, and are used, against what the Spanish government perceives as online support for terrorism and extremism. A whole chapter in the law is dedicated to 'terrorist organisations and groups', Articles 571–580. The definition of terrorism in the code is found in Article 573. The definition itself is very vague as it includes serious crimes against concepts like 'liberty', 'moral integrity', and 'heritage', committed in order to 'destabilise the functioning of political institutions or the economic or social structures of the State' or 'to force the public authorities to perform and act, or refrain from doing so', or even to 'seriously alter public peace'. The article, later in Sub-article 3, also includes in its definition of terrorism

130 Manuel Ricardo Torres-Soriano, 'Jihadist Propaganda As A Threat Indicator: The Case Of Spain', *Terrorism and Political Violence*, 2017.

131 Anne Applebaum, 'Want To Build A Far-Right Movement? Spain's Vox Party Shows How', *The Washington Post*, May 2019, www.washingtonpost.com/graphics/2019/opinions/spains-far-right-vox-party-shot-from-social-media-into-parliament-overnight-how accessed 1 August 2019.

132 'Spanish Criminal Code', *Agencia Estatal Boletín Oficial del Estado*, November 1995, www.boe.es/eli/es/lo/1995/11/23/10 accessed 2 August 2019.

the incitement to terrorism and the glorification of terrorism without mentioning the need for possible risk or intent. The specific articles about those felonies are Article 589 for incitement and Article 578 on glorification. Article 578, which was introduced in the year 2000, forbids not only glorification but also 'justification' or the 'contempt or humiliation of the victims of terrorist crimes or their relatives'.

The Spanish criminal code also includes a list of 'insult' felonies which forbid the insulting of the King and the Queen (490–491), the country, its communities and its symbols (543), parliament members (496), and judges and members of the armed forces (504). In 2014 the Spanish government passed a new version of the law of citizen security.[133] The law gives administrative powers to the police to impose sanctions for 'disrespect' of the authority or for having lack of consideration to the authority. The law – which was criticised by Amnesty International[134] – was named 'the law of the kick in the mouth' and the 'gag rule' and it is still under revision in the Constitutional Court.

In 2015, Spain legislated a major amendment to its criminal code as an organic law.[135] The amendment included an extensive new article regarding hate crimes (510). The article forbids the inciting of "discrimination, hate or violence against groups or associations due to racist or anti-Semitic reasons or any other related to ideology, religion or belief, family situation, belonging to an ethnic group or race, national origin, gender, sexual preference, illness or handicap". It also forbids anyone to "publicly deny, gravely trivialise or glorify the crimes of genocide, crimes against humanity or against persons and property protected in the event of armed conflict, or to exalt their perpetrators, when they have been committed against a group or a part thereof, or against a person determined by reason of their membership, for racist, anti-Semitic or other reasons related to

133 Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.

134 'España: El Derecho A Protestar, Amenazado', *Amnesty International*, 2014, www.amnesty.org/download/Documents/8000/eur410012014es.pdf accessed 2 January 2020.

135 Ley Orgánica 1/2015, De 30 De Marzo, Por La Que Se Modifica La Ley Orgánica 10/1995, De 23 De Noviembre, Del Código Penal.

ideology, religion or beliefs". The article also targets those "who, with knowledge of its falseness or reckless disregard for the truth, were to distribute defamatory information or associations in relation to their ideology, religion or belief, or their belonging to an ethnic group or race, national origin, gender, sexual preference, illness or handicap".

In 2002, the Spanish government passed The Information Society Services and Electronic Commerce Act (Ley de servicios de la sociedad de la información y de comercio electrónico, or LSSI)[136] in order to control online activities and allow it to block and filter online content. Following the attacks in France in 2015, the government passed an amendment[137] to the criminal procedure law that will allow it to deal better with the technological aspects of crime and terrorism.

In 2019, the Spanish government published its new national strategy for counter-terrorism,[138] which replaces the 2012 one. The strategy document recognises the tendency of terrorists and extremists to use social media platforms in order to advance their ideology and recruit members and suggests a tighter control on content by government bodies and tech companies.

BLOCKING AND REMOVAL OF ONLINE CONTENT

There are several laws that allow Spanish government bodies to ask for, or order, the removal and blocking of online content. The LSSI[139] is the main law allowing for the blocking and removal of content. Article 8 of the law defines the protected principles that underpin the removal or blocking of content. Among them is 'the safeguard of public order, criminal investigation, public security and national defence'.

136 Ley 34/2002, De 11 De Julio, De Servicios De La Sociedad De La Información Y De Comercio Electrónico.

137 Ley Orgánica 13/2015, De 5 De Octubre, De Modificación De La Ley De Enjuiciamiento Criminal Para El Fortalecimiento De Las Garantías Procesales Y La Regulación De Las Medidas De Investigación Tecnológica.

138 'Estrategia Nacional Contra El Terrorismo 2019', *Departamento de Seguridad Nacional*, February 2019, www.dsn.gob.es/eu/actualidad/sala-prensa/estrategia-nacional-contra-terrorismo-2019 accessed 3 August 2019.

139 See Note 134.

The law refers to and recognises several relevant technological groups and their duties and responsibilities in publishing, blocking and removing data, such as intermediary service providers, network operators and Internet access providers, service providers who make temporary copies of data, hosting and storage service providers, and service providers who offer links to search tools or content. The LSSI gives the Ministry of Industry, Energy and Tourism the general responsibility of monitoring the Internet but there are several other administrative bodies that can be found monitoring the Internet such as the National Cyber Security Council[140] and, in the police, the 'technological brigade'[141] and the Telematic Crime group.

The criminal code also has legal tools that allow the blocking and removal of content from online platforms. As part of the article on hate speech (510), which was amended in 2015, there is a provision that allows the court to remove or block content that meets the definition of hate crime in the article.[142] Similar provision appears in the terrorism crimes section, specifically in Article 578.4.

There is no one administrative authority in Spain in charge of removing and blocking content. Because freedom of speech is protected by the Spanish constitution, an order to remove content or block it can only be given in a judicial decision. That said, because the LSSI imposes liability on Internet service providers (ISPs) and others, it is encouraging Internet companies to remove content by themselves and to obey requests from administrative organisations who monitor the web.[143] In two different cases, the court ruled on the limits of

140 'Consejo Nacional De Ciberseguridad', *Departamento de Seguridad Nacional*, www.dsn.gob.es/es/comites-especializados/consejo-nacional-ciberseguridad accessed 5 August 2019.

141 'Página Oficial De La DGP-Comisaría General De Policía Judicial', *Policía Nacional*, www.policia.es/org_central/judicial/udef/bit_quienes_somos.html accessed 5 August 2019.

142 The definition of what constitute a hate crime was given by the Spanish constitutional court in 235/2007, FJ 5; 117/2015, FJ 3; and 86/2017, FJ5.

143 'Blocking, Filtering and Take-Down of Illegal Internet Content', *Council of Europe*, 2015 www.coe.int/en/web/freedom-expression/country-reports accessed 5 August 2019.

liability for Internet sites. In the first case,[144] the appellant had hosted pages containing insults against the Spanish Society of Authors and Publishers. The Spanish Supreme Court, which heard the appeal on the case, ruled that the host was 'effectively aware' of the insults and therefore should have shown due diligence at the moment they became aware. In a different case,[145] an electronic newspaper had published offensive remarks against a local police chief. The court ruled that the responsibility placed on Internet hosting services, according to the LSSI, did not intend to lead to a narrowing of free speech in terms of a pre-censorship of everything published but, rather, it was intended to lead to due diligence and co-operation once the publication is identified by authorities as illegal. The fact the site removed the publication immediately when it was identified by the authorities helped the court to find that it had acted with due diligence. The Spanish Government recently passed a controversial new decree[146] allowing it to remove or block pro-Catalan independence online activity. This decree was used by the government in order to block many of the political sites used by the Catalan supporters.[147]

SURVEILLANCE

The Edward Snowden story[148] did not have a noticeable impact in Spain, mostly because Spain was not presented as a major target of the NSA. The privacy of electronic communication is protected by the Spanish constitution (Article 18), and by the

144 Tribunal Supremo, (Sala de lo Civil, Sección 1ª) Sentencia num. 773/2009 de 9 diciembre, available at RJ\2010\131.

145 Audiencia Provincial de Cádiz (Sección 2ª) Sentencia num. 326/2010 de 4 noviembre, available at AC\2011\652.

146 'Documento BOE-A-2019-15790', *Agencia Estatal Boletín Oficial del Estado*, November 2019, www.boe.es/diario_boe/txt.php?id=BOE-A-2019-15790 accessed 24 December 2019.

147 'Spain Passes Decree To Shut Down Websites And Social Media Over 'Public Order Threats'', *Catalan News*, November 2019, www.catalannews.com/politics/item/spain-passes-decree-to-shut-down-websites-and-social-media-over-public-order-threats accessed 24 December 2019.

148 See Note 71.

Law of Communication.[149] This law specifically mentions, in Article 6, that electronic information stored by providers can be given to "the personnel of the National Intelligence Centre in the course of security investigations on persons or entities, in accordance with the provisions of the law".

In 2014, Spain passed a law[150] that created the Intelligence Centre against Terrorism and Organised Crime (Centro de Inteligencia contra el Terrorismo y el Crimen Organizado, or CITCO) out of two former bodies, The Intelligence Centre against Organised Crime and The Spanish National Centre for Antiterrorist Coordination. CITCO was created in order "to improve the information exchange between specialised agencies when analysing threats from terrorism, organised crime and violent radicalism".[151] In practice, CITCO is the main intelligence body when it comes to the fight against terrorism and, therefore, the main organisation using online surveillance relating to terrorism, organised crime and violent radicalism.

The 2015 organic law, regarding the amendment of criminal procedure,[152] has created a clearer procedure when it comes to electronic surveillance measures. Article 588 defines the rules that apply regarding the interception of text, WhatsApp or Telegram messages as well as covert listening devices, the reception and recording of oral communications through the use of electronic devices, the use of technical devices for imaging, tracking and location, the registration of devices of mass storage, and even remote logs on computers. These activities introduce the concept of undercover agents on the web under false identities.[153]

149 'Lay 9/2014, Of May 9, General Of Telecommunications.'

150 'Royal Decree 873/2014, Of October 10, Which Modifies Royal Decree 400/2012, Of February 17, Which Develops The Basic Organic Structure Of The Ministry Of Interior.'

151 'Surveillance By Intelligence Services – Volume I: Member States' Legal Frameworks', *European Union Agency for Fundamental Rights*, November 2015, https://fra.europa.eu/en/publication/2015/surveillance-intelligence-services accessed 5 August 2019.

152 See Note 135.

153 See Note 146.

CRIMINAL LAW

The wide scope of the articles in the Spanish criminal code that place limits on the freedom of expression is creating a problematic situation where the same action could fit several different articles in the criminal code. For example, for the action of disseminating terrorist propaganda, one could be indicted for inciting others to commit terrorist offences (579.1) or provoking others to commit terrorist offences (579.2) or collaborating with a terrorist organisation by way of indoctrination (577.2) or justifying terrorist acts (578). This situation has arisen, as Petzsche and Malie[154] have recognised, due to "the recent Spanish legislative approach of consistently adding 'something' to the relevant provisions every few years, without properly considering compatibility with previous layers of legislation".[155]

The questions that Spanish criminal legislation raises are not only theoretical, since those articles are used relatively extensively by the Spanish police and prosecution. According to the European Union Terrorism Situation and Trend Report 2018 (TESAT),[156] the number of arrests and convictions in terrorist cases in the years 2015, 2016 and 2017 is second only to France in all of Europe. Most of the cases are related to online activity, though there is a difference between the criminal articles that are used against jihadi online content dissemination and separatist and leftist content. Jihadi supporters are usually indicted on membership of, or collaboration with, a terrorist organisation,[157] which results in heavy punishments such as in the case of a man who used social platforms to spread the word and symbols of ISIL in an attempt to recruit female minors to travel to the ISIL-controlled areas in Iraq and Syria and marry fighters there. He was

154 See Note 79.

155 Ibid. p. 158.

156 'European Union Terrorism Situation and Trend Report 2018 (TESAT 2018)', *Europol*, June 2018, www.europol.europa.eu/activities-services/main-reports/ european-union-terrorism-situation-and-trend-report-2018-tesat-2018 accessed 5 July 2019.

157 Rodriguez, L. P., 'El Nuevo Delito De Autoadoctrinamiento Terrorista' (2017) Nº 8967 *Diario La Ley*.

sentenced to five years in prison.[158] Most of the criticism against the Spanish policy of indictment for statements made online relates to the use of Article 578 against 'anti-Franco' and Basque nationalist supporters, activists, artists and reporters.[159] According to an extensive report by Amnesty International, Article 578, which was introduced into law in the year 2000, only started being used repeatedly in 2015 after its amendment by the conservative government. By using what is called by the Spanish government 'Spider Operations', the Spanish police arrested groups of anti-fascist or ETA sympathisers as a result of their online statements. The report includes several case studies[160] showing the problematic use of the law, especially in terms of its connection to ETA activity. The fact that ETA and GRAPO have ceased their activity has not stopped the Spanish courts from convicting people of the felony of glorifying them. The court also ruled, on several occasions, that there is no need for an 'intent to glorify' in order to gain a conviction. Another problematic side of Article 578 is its use in relation to insulting victims of terrorism, especially when the victims of terrorism were controversial figures in the Franco dictatorship.[161]

ADMINISTRATIVE MEASURES

Spain's most notorious and criticised administrative counter-terrorism measure is the use of incommunicado detentions.

158 See Note 79 p. 18.

159 Ana Pastor, 'Terrorism Laws Are Threatening Freedom of Expression in Spain', *Freedom House*, April 2018, https://freedomhouse.org/blog/terrorism-laws-are-threatening-freedom-expression-spain accessed 6 August 2019.

160 The most well-known ones are the puppet makers who were arrested for dressing one of their puppets in a symbol similar to the ETA symbol or the case of all 12 rappers of La Insurgencia who were charged with 'glorifying terrorism' on the basis of their song lyrics: "We must fight decisively, only the ideological line of the Communist Party-Reconstituted will save us."

161 One especially notorious case was regarding a young woman who was charged because of jokes and memes she had posted on Twitter regarding Franco-era Prime Minister Carrero Blanco who was killed by ETA Terrorists.

Spanish criminal procedure law[162] gives a person who is arrested on suspicion of a felony the regular basic rights, such as notifying a lawyer or family member, a phone call and a limited amount of time before being brought before a judge. However, the legal situation is changed dramatically when the suspicion is terrorism related, there is a direct security connection and there is a need for further investigation. Terrorism suspects may be held for a total of five days in incommunicado police detention. Persons being held incommunicado do not have the right to notify a third party about their detention or whereabouts; to receive visits from family members, spiritual advisors or a doctor of their own choosing; or to communication or correspondence of any kind (Article 527). Incommunicado detainees do not have the right to designate their own lawyer but must be assisted by a legal aid attorney.[163] Furthermore, these detainees do not have the right to a private consultation with their lawyer. This method of investigation has been criticised heavily by human rights organisations[164] over the years and even more recently when, as described above, very innocent statements could be defined as terrorist-related offences and lead to arrests.

162 'Act On Criminal Judicial Procedure (1961, Amended 2002)', *Legislationline.org*, 2002, www.legislationline.org/documents/id/3850 accessed 6 August 2019.

163 Article 55 of the Spanish constitution does allow to suspend some rights of prisoners in cases of terror.

164 'Setting An Example? Counter-Terrorism Measures In Spain: The Use Of Incommunicado Detention', *Human Rights Watch*, 2005, www.hrw.org/reports/2005/spain0105/6.htm accessed 6 August 2019; 'Spain's Incommunicado Detention Violates Human Rights', *Liberties*, October 2014, www.liberties.eu/en/news/spain-incommunicado-detention/1960 accessed 6 August 2019; 'Spain: Incommunicado Detention – Out Of Sight, Out Of Mind', *Amnesty International*, September 2009, www.amnesty.org/en/press-releases/2009/09/spain-incommunicado-detention-e28093-out-sight-out-mind-20090915 accessed 6 August 2019.

UNITED KINGDOM

THE LEGAL SYSTEM OF THE UK, THE RIGHT TO PRIVACY AND THE RIGHT TO FREEDOM OF SPEECH

The United Kingdom (UK) is a parliamentary democracy with a constitutional monarchy. The country does not have a written constitution but, rather, a *de facto* constitution based on a combination of historical documents[165] and Common Law precedents. The legal system is a combination of three legal systems: that of England and Wales, the Scottish system, and the Northern Irish system. The Constitutional Reform Act of 2005[166] has created a new Supreme Court of the United Kingdom, which hears appeals of civil cases from all over the UK and appeals on criminal cases from all over the UK except Scotland. The court sits also on matters of important constitutional questions. However, the UK Supreme Court cannot interfere with laws enacted by parliament because of the constitutional principle of parliamentary supremacy.

The Human Rights Act[167] of 1998 incorporated the European Convention on Human Rights into UK law and thus declared by law that the rights of the convention are binding on the British government. The right to privacy (Article 8) and freedom of speech (Article 10) are key components of the convention. Although, as explained, the court cannot nullify primary parliamentary legislation that contradicts the Human Rights Act, it can issue a declaration of incompatibility as an advice to the parliament where the court believes a new law contradicts the Human Rights Act.

165 Such as the Acts of Union of 1707 and 1800.

166 Constitutional Reform Act 2005.

167 Human Rights Act 1998.

UK AND TERRORISM

Until 2000, the main terrorism concerns in the UK were in regard to the conflict in Northern Ireland and the need to deal with threats from both the Irish Republican Army (IRA) and loyalist groups. The 7 July 2005 attack in London, which caused the deaths of 52 people and wounded hundreds, shifted the attention to jihadi terrorism. After a relatively quiet period with some successes for the UK security services, a series of deadly attacks in 2017 by jihadi terrorists raised the security alert twice to its highest level for a couple of days.[168]

Another identified security problem was the flow of British citizens joining up with extremist fighters in Syria. It is estimated that more than 900 British citizens made the journey and many of them have since returned to the UK.[169] Right-wing activity has also risen dramatically, with the murder of Jo Cox MP by a right-wing extremist in June 2016 being the most well-known incident, followed by some attempts to hurt other leftist politicians and the immigrant population.[170] In addition, for various political reasons, 2018 saw signs of the re-emergence of violence in Northern Ireland.[171]

168 Claire Phipps, 'The Snap: UK Threat Level Is Raised To Critical After Manchester Bombing', *The Guardian*, May 2017, www.theguardian.com/politics/2017/may/24/the-snap-uk-threat-level-critical-manchester-bombing accessed 27 June 2019.

169 Lizzie Dearden and Richard Hall, 'What Happened To The Britons Who Went To Join Isis?', *The Independent*, February 2019, www.independent.co.uk/news/world/middle-east/uk-isis-recruits-syria-return-british-caliphate-terrorism-jihadis-a8781056.html accessed 2 July 2019.

170 Between April 2017 and March 2018, the UK government noted an increase of 36% in the number of people referred to the government's counter-extremism programme for far-right activities.

171 Dan Haverty, 'Paramilitaries Are Surging Again In Northern Ireland', *Foreign Policy*, May 2019, https://foreignpolicy.com/2019/05/24/paramilitaries-are-surging-again-in-northern-ireland accessed 25 June 2019.

INTERNET ACTIVITY RELATING TO ATTACKS

In 2019, the Commission for Countering Extremism[172] published a series of research papers on online extremism in the UK. In the extensive report 'Challenging Hateful Extremism',[173] which is based on the work of the commission with academics and NGOs, the commission identified massive online extremist activity by the far right, the far left and radical Muslims in England and Wales. For example, the commission identified that "in the UK alone, there are approximately 170,000 online anti-Semitic searches each year". According to a 2017 report by Policy Exchange,[174] a British conservative think tank, the UK population is ranked first in Europe and fifth in the world in terms of the consumption of extreme content online. This high rate of access to and distribution of extreme online materials had, according to the report, a direct effect on the radicalisation of potential terrorists. The report found that 69% of Islamic-related attacks in the UK were carried out by attackers who, prior to the incidents, had been exposed to such materials.

THE STATE'S LEGAL RESPONSE

The UK has been one of the most active European countries in terms of legislating for counter-terrorism criminal and administrative measures. The Terrorism Act 2000,[175] the Anti-terrorism, Crime and Security Act 2001,[176] the Prevention of Terrorism Act 2005,[177]

172 'Commission For Countering Extremism', *GOV.UK*, 2019, www.gov.uk/government/organisations/commission-for-countering-extremism accessed 25 November 2019.

173 'Challenging Hateful Extremism', *GOV.UK*, October 2019, www.gov.uk/government/publications/challenging-hateful-extremism accessed 25 November 2019.

174 'The New Netwar: Countering Extremism Online', *Policy Exchange*, September 2017, https://policyexchange.org.uk/publication/the-new-netwar-countering-extremism-online accessed 1 July 2019.

175 Terrorism Act 2000.

176 Anti-Terrorism, Crime And Security Act 2001.

177 Prevention Of Terrorism Act 2005.

the Terrorism Act 2006,[178] the Counter-Terrorism Act 2008,[179] the Terrorist Asset-Freezing etc. Act 2010,[180] the Terrorism Prevention and Investigation Measures Act 2011,[181] the Protection of Freedoms Act 2012,[182] the Counter-Terrorism and Security Act 2015,[183] the Investigatory Powers Act 2016,[184] and the Counter-Terrorism and Border Security Act 2019[185] have created a powerful – some will say *too* powerful – counter-terrorism legal response that includes a few specific tools regarding online activity.

BLOCKING AND REMOVAL OF ONLINE CONTENT

The Terrorism Act 2006 makes UK Internet service providers (ISPs) liable by law if they do not remove or block terrorist-related content after they have been given notice to do so.[186] In order to implement the law and encourage the removal, blocking and filtering of extremist content, a special unit was formed in 2010 – the Counter-Terrorism Internet Referral Unit (CTIRU). The CTIRU has been referring suspected URLs to UK Internet and tech companies in order to block and remove extremist content. Freedom House in the UK reports that 304,000 online items have been removed from the Internet at the request of CTIRU since 2010.[187] This process has been criticised for its lack of accuracy, as it seems that around 20% of requests by the

178 Terrorism Act 2006.

179 Counter-Terrorism Act 2008.

180 Terrorist Asset-Freezing Etc. Act 2010.

181 Terrorism Prevention And Investigation Measures Act 2011.

182 Protection Of Freedoms Act 2012.

183 Counter-Terrorism And Security Act 2015.

184 Investigatory Powers Act 2016.

185 Counter-Terrorism And Border Security Act 2019.

186 Section 3 of the law was never used in practice. For more, see: Walker, C. 'The War Of Words With Terrorism: An Assessment Of Three Approaches To Pursue And Prevent' (2017) 22 *Journal of Conflict and Security Law*.

187 'Freedom on the Net 2018: United Kingdom', *Freedom House*, 2019, https://freedomhouse.org/report/freedom-net/2018/united-kingdom accessed 2 July 2019.

CTIRU have been identified by Internet companies as mistakes or as being unjustified.[188] CTIRU has also created a governmental filtering system that applies to all public Internet access,[189] including an AI computer program that was aimed at issuing alerts about jihadi online content.[190] A specific site was also developed that encourages the public to report online terrorist content.[191] The official government position is to put more pressure on Internet companies to remove extremist content faster than they are currently doing, if necessary, through legislation.[192]

SURVEILLANCE

The issue of the online surveillance powers of the UK has been widely discussed since *The Guardian* published Edward Snowden's documents in 2013.[193] Most of the criticism has been aimed at the practices of the Government Communications Headquarters (GCHQ), and especially the bulk surveillance methods that allowed GCHQ to obtain data on people who were not suspects or posing any potential harm to the state. This policy was executed by using a very wide interpretation of the Regulation of Investigatory Powers 2000.[194] In 2018, the ECtHR

188 TJ McIntyre, 'Internet Censorship in the United Kingdom: National Schemes and European Norms', in Edwards (ed), *Law, Policy and the Internet*, Hart Publishing, 2018.

189 'Freedom of Information about URL Filtering', *WhatDoTheyKnow*, June 2013, www.whatdotheyknow.com/request/160774/response/404100/attach/ html/3/attachment.pdf.html accessed 2 July 2019.

190 Patrick Greenfield, 'Home Office Unveils AI Program To Tackle Isis Online Propaganda', *The Guardian*, February 2018, www.theguardian.com/uk-news/2018/feb/13/home-office-unveils-ai-program-to-tackle-isis-online-propaganda accessed 1 July 2019.

191 'Report Online Material Promoting Terrorism Or Extremism', *GOV.UK*, 2019, www.gov.uk/report-terrorism accessed 28 June 2019.

192 'Online Harms White Paper', *HM Government*, April 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf accessed 7 July 2019.

193 See Note 71.

194 Regulation of Investigatory Powers Act 2000.

ruled that some aspects of that policy were violating Article 8 of the European Convention on Human Rights, in terms of the right to privacy. The court found that there was "insufficient oversight both of the selection of Internet bearers for interception and the filtering, search and selection of intercepted communications for examination, and the safeguards governing the selection of 'related communications data' for examination were inadequate".[195] The ruling, however, didn't forbid bulk surveillance as a technique, but asked for an 'adequate system of safeguards, including controls exercised by independent bodies'[196] when using it. The court procedures, which started in 2013, related to the legal situation under the Regulation of Investigatory Powers 2000. In 2016, the UK parliament passed the Investigatory Powers Act 2016,[197] which created a stricter regulatory mechanism, to allow bulk surveillance by creating a double-lock approval system of surveillance and appointing a specific regulator to examine the implementation of the law. However, the law was still highly criticised by activists,[198] and was challenged in the High Court. In 2018, the Court found that the law did not comply with EU law and that the government should amend the legislation regarding safeguards for retaining data.[199] In 2019, the case returned to the court to examine the rest of the arguments raised by the claimant which challenged the bulk surveillance part of the law – a claim that was rejected by the court, which ruled that sufficient safeguards were installed in the act.[200]

195 'Case Of Big Brother Watch And Others V. The United Kingdom', *HUDOC – European Court of Human Rights*, 2018, https://hudoc.echr.coe.int/eng#_Toc524359882 accessed 1 July 2019.

196 Ibid.

197 See Note 182.

198 Ewen MacAskill, ''Extreme Surveillance' Becomes UK Law With Barely A Whimper', *The Guardian*, November 2016, www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper accessed 1 July 2019.

199 'Liberty V Home Office', *Judiciary*, April 2018, www.judiciary.uk/wp-content/uploads/2018/04/liberty-v-home-office-judgment.pdf accessed 3 July 2019.

200 'Liberty Judgment Final', *Judiciary*, July 2019, www.judiciary.uk/wp-content/uploads/2019/07/Liberty-judgment-Final.pdf accessed 25 November 2019.

CRIMINAL LAW

The response under UK criminal law to online extremism has been evolving quickly and dramatically at the legislation level. In the Terrorism Act of 2000, Section 12 forbids inviting 'support for a proscribed organisation' while Section 58 addresses anyone who 'collects or makes a record of information of a kind likely to be useful to a person committing or preparing an act of terrorism'. The Terrorism Act 2006 already mentioned specific Internet-related offences. It presented the 'encouragement of terrorism' offence,[201] which has a very wide definition that forbids expressing 'direct or indirect encouragement or other inducement to them to the commission, preparation or instigation of acts of terrorism'. According to the law, the *mens rea* that is needed for conviction can be recklessness regarding 'whether members of the public will be directly or indirectly encouraged or otherwise induced by the statement to commit, prepare or instigate such acts or offences'. Another relevant offence from the Terrorism Act 2006 is the 'dissemination of terrorist publications'.[202] This offence again spreads a very wide net in terms of terrorist publications as it could apply, for example, to someone who 'provides a service to others that enables them to obtain, read, listen to or look at such a publication' and doing so even if he is just reckless in terms of the possibility that 'his conduct [could] be a direct or indirect encouragement or other inducement to the commission, preparation or instigation of acts of terrorism'. An even more drastic step was taken by UK legislators in the Counter-Terrorism and Border Security Act 2019, which amended the Terrorism Act 2000 in a few ways. The first is by entering the recklessness *mens rea* to the felony of supporting proscribed organisations.[203] The second amendment,[204] and the more problematic one, added to the existing Section 58 of the law an offence of just *viewing* online what is defined as information

201 Article 1 of the Terrorism Act 2006.
202 Article 2 to the Terrorism Act 2006.
203 Article 1 to the Counter-Terrorism and Border Security Act 2019.
204 Article 3 to the Counter-Terrorism and Border Security Act 2019.

that could be 'useful to a person committing or preparing an act of terrorism'. This law which is known as the 'one click law' does provide some defences such as journalism or research purposes but it is still the first law in the EU that criminalises entering or watching terrorist materials for a single online entry, without the need to prove any terrorist intentions, and as such was subject to criticism by NGOs and academics.[205]

As for important UK jurisprudence, the most important case regarding terrorist and online activity that has reached the Supreme Court was the case of R v Gul.[206] The defendant in this case was a British citizen where a police search on his computer found several videos of al-Qaeda attacks on military forces in Iraq and Afghanistan and some videos of attacks on civilians such as the 9/11 attacks. Gul was charged with and convicted of committing an offence under Section 2(1) of the Terrorism Act of 2006 for distributing or circulating a terrorist publication. He was then sentenced to five years in prison. The question that was raised in the Appeal Court and, later, at the Supreme Court was: do all of the videos portray terrorism? Is a video of a battle between armed al-Qaeda militias and armed coalition forces to be considered a terrorist publication? The answer from the UK court was 'yes', although the Supreme Court did express concern about the scope of the offence. This decision evoked a mixed reaction as Simeon[207] analyses it: some considered it an important tool in the fight against terrorism while others saw it as widening the definition of terrorism to the extreme, defining every internal armed conflict fighter as a terrorist.[208]

205 'Freedom of Expression and The Counter-Terrorism and Border Security Act', *Index on Censorship*, February 2019, www.indexoncensorship.org/2019/02/freedom-of-expression-and-the-counter-terrorism-and-border-security-act accessed 1 July 2019.

206 See Note 198.

207 James Simeon, 'The Evolving Common Law Jurisprudence Combatting The Threat Of Terrorism In The United Kingdom, United States, And Canada', *Laws*, 8(1), 2019.

208 Ibid p. 15.

As for the enforcement of those laws and practices, *The Times*[209] reported in 2017 on a dramatic increase in arrests in relation to Internet extremist content – up to 3,300 arrests a year. The article further reports that the majority of these arrests do not end in criminal charges and are, in fact, mostly the result of an over-eager police force. A known example of the result of an over-reaching arrest policy is the case of Rizwaan Sabir, a master's student who was held under arrest for six days for researching al-Qaeda tactics online.[210] Some of the charges that resulted from the online extremism arrests were borderline and raised criticisms and questions about the policy of charging. An example of this is the case of a man who was charged for violating the Communications Act 2003 by posting on YouTube a video of his dog making the Nazi salute in response to him making anti-Semitic remarks.[211]

According to a report by Max Hill QC on the operation of the Terrorism Acts in 2017,[212] 110 people were charged with terrorism-related offences in 2017, most of them (78) were charged under the Terrorism Acts: "The Principal offences for which persons were charged under the Terrorism Acts included membership offences (8 persons), fundraising offences (4 persons), collection of information useful for an act of terrorism (15 persons), encouragement of terrorism (9 persons), dissemination of terrorist publications (13 persons), preparation for terrorist acts (28 persons) and provision

209 Charlie Parker, 'Police Arresting Nine People A Day In Fight Against Web Trolls', *The Times*, October 2017, www.thetimes.co.uk/article/police-arresting-nine-people-a-day-in-fight-against-web-trolls-b8nkpgp2d accessed 1 July 2019.

210 Polly Curtis and Martin Hodgson, 'Student Researching Al-Qaida Tactics Held For Six Days', *The Guardian*, May 2008, www.theguardian.com/education/2008/may/24/highereducation.uk accessed 2 July 2019.

211 'Man Fined For Nazi Pug Video Raises More Than £100K For Appeal', *The Scotsman*, April 2018, www.scotsman.com/regions/glasgow-strathclyde/man-fined-for-nazi-pug-video-raises-more-than-100k-for-appeal-1-4730165 accessed 10 July 2019.

212 'Reports Of Former Reviewers 'Independent Reviewer Of Terrorism Legislation', *Independent Reviewer of Terrorism Legislation*, 2018, https://terrorismlegislationreviewer.independent.gov.uk/category/reports/reports-former-reviewers accessed 1 July 2019.

of information related to a terrorist organisation (1 person). One person was charged for using or threatening to use noxious substances to cause harm under the Antiterrorism, Crime and Security Act 2001 and two persons were charged for contravening a control order under the Terrorism Prevention and Investigation Measures Act 2011."

All of the cases described in the report contain some use of online activity while more than half of them deal only with online activity. The UK punishment level for holding, posting or just retweeting content that is described as being 'terrorist related' is considerably high, as most of the cases in the report had punishments of between two and five years' imprisonment.

ADMINISTRATIVE MEASURES

The UK had developed administrative measures as a way to counter terrorism as early as the 1970s, as a response to the conflict in Northern Ireland. In a series of changes, starting from the year 2000, the legislator gave powerful administrative powers to counter-terrorism units.[213] The Prevention of Terrorism Act 2005 allowed the imposing of restrictions on residence, travel, movements within the UK, communications, possessions and work. Forty-five control orders were issued from 2005 to 2011 for different periods 'ranging from a few months to more than four-and-a-half years'.[214] The 2005 Prevention of Terrorism Act was replaced by the Terrorism Prevention and Investigation Measures Act 2011, which was more elaborate and created some more checks and balances on the procedure.

213 'Berenice Boutin, 'Administrative Measures Against Foreign Fighters: In Search Of Limits And Safeguards', *The International Centre for Counter-Terrorism*, December 2016, https://icct.nl/publication/administrative-measures-against-foreign-fighters-in-search-of-limits-and-safeguards accessed 3 July 2019.

214 'Final Report Of The Independent Reviewer On The Prevention Of Terrorism Act 2005', *GOV.UK*, March 2012, www.gov.uk/government/publications/final-report-of-the-independent-reviewer-on-the-prevention-of-terrorism-act-2005 accessed 3 July 2019.

Issuing warrants under both laws concerns online activity in two ways. The first is that some of the orders were issued in order to limit the online access of the persons they were issued against. And the second is that some of the intelligence that was presented in order to approve such warrants was gathered from the person's online activity. These practices, although approved to some extent by the ECtHR, have been criticised by activists and academics for violating basic human rights without proper procedure.[215]

Another administrative mechanism that has been highly controversial in the counter-terrorism discourse is the 'Prevent Programme'. Prevent is a part of 'Contest',[216] the UK government programme for counter-terrorism initially presented as early as 2003. In 2015, the Counter-Terrorism and Security Act adopted Prevent into law and ordered several public authorities, such as higher education institutions, to have 'due regard to the need to prevent people from being drawn into terrorism'. This act has made it a legal duty for teachers, social workers, medical doctors and many other state employees to search within their clients, students and co-workers for signs for potential radicalisation. The programme actively encourages looking for signs online and on social media like these two case studies from the Contest programme: "Callum was a teenager whose teacher became aware of his involvement in promoting a far-right Facebook page" or "Yusuf was at university and was aged 24 when a university staff member saw him handing out leaflets which, it turned out, were promoting a website containing extremist, homophobic and violent material." The Prevent Programme was, and is still, criticised by many as it is considered to be encouraging civil surveillance and Islamophobia.[217] Another aspect of the programme that was highly criticised is the use of the data that is gathered as secret evidence

215 Ibid.

216 'Counter-Terrorism Strategy (CONTEST) 2018', *GOV.UK*, 2018, www.gov.uk/government/publications/counter-terrorism-strategy-contest-2018 accessed 3 July 2019.

217 Fahid Qurashi, 'The Prevent Strategy And The UK 'War On Terror': Embedding Infrastructures Of Surveillance In Muslim Communities', *Palgrave Communications*, 4(1), 2018.

in family courts where the state removes children from families to protect them from radicalisation. According to a report by Cage, more than 100 children were removed from home under the Prevent Programme, without proper scientific back-up on the effectiveness of such drastic measures.[218]

218 'Separating Families – How PREVENT Seeks The Removal Of Children Report', *CAGE*, 2017, www.cage.ngo/product/separating-families-how-prevent-seeks-the-removal-of-children-report accessed 3 July 2019.

UNITED STATES

THE LEGAL SYSTEM OF THE US, THE RIGHT TO PRIVACY AND THE RIGHT TO FREEDOM OF SPEECH

The United States of America is a federal republic, based on parliamentary representation. The United States (US) Constitution of 1789[219] is the document that founded the US system of government and it is based on the concept of 'separation of powers'. Article 1of the constitution defines the two houses of parliament and their legislative powers. Article 2 defines the power of the president and the government, Article 3 gives the power to the judicial system and the Supreme Court, and Articles 4–6 define the relationship between the states and the federal government.

The US Supreme Court is the highest court in the country. This court can examine the validity of Congress legislation and presidential decisions in light of the constitution. These appeals can only take place as part of a specific case affected by those decisions or legislation. Since its ratification, the US Constitution has been amended 27 times. The first 10 amendments are called 'The Bill of Rights'.

Freedom of expression is protected in the First Amendment of the constitution. The amendment forbids Congress from enacting any law 'abridging the freedom of speech'. The US Supreme Court is probably the most zealous court in the world when it comes to protecting freedom of speech.[220] That said, the court has approved some restrictions on speech over the years, through direct or indirect rulings such as Near v. State of Minnesota Ex Rel. Olson, 283 U.S. 697 (1931), Dennis v. United States, 341 U.S. 494 (1951), Miller v. California,

219 'Constitution Of The United States – We The People', *Constitutionus.com*, https://constitutionus.com accessed 10 August 2019.

220 Meiklejohn, A. 'The First Amendment Is An Absolute' (1961) 1961 The Supreme Court Review.

413 U.S. 15 (1973) and Holder v. Humanitarian Law Project (130 S.Ct. 2705 (2010)).

Unlike freedom of expression, the right to privacy is not mentioned directly in the constitution. It was adopted by the US Supreme Court as part of the right to liberty that appears in section 1 of the Fourteenth Amendment.[221] Although the Fourth Amendment protects the right to not be searched without a warrant, which gives additional constitutional protection to the right of privacy, the interpretive character of the right makes it a less protected right than the right to freedom of speech in the eyes of the US Supreme Court.

THE US AND TERRORISM

Although the US has a long history of terrorist attacks carried out by multiple organisations and individuals against a variety of targets, including presidents of the country, there is no doubt that the defining moment of terrorism in our times was the 9/11 combined attack by al-Qaeda terrorists in 2001. This terrorist attack, the deadliest attack in modern times,[222] has changed the history of the US and the Middle East, and brought jihadi terrorism to centre stage. In the following years, during the 'War on Terror', and later the war against ISIS, the word 'terrorism' in the US has become, culturally, shorthand for jihadi terrorism.

A study[223] carried out in collaboration with *The Nation* newspaper and the Center for Investigative Reporting has presented a more complex picture. According to the report, between 2008 and 2016, there were 115 right-wing-related terrorist attacks and attempted attacks and, out of these, 33% were foiled before execution. There

221 Douglas Linder, 'The Right Of Privacy: Is It Protected By The Constitution?', *University of Missouri-Kansas City*, http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html accessed 10 August 2019.

222 In the attack, 2,996 people were killed and more than 6,000 were injured, and the direct financial damage was estimated at $10 billion.

223 David Neiwert, 'Far-Right Extremists Have Hatched Far More Terror Plots Than Anyone Else In Recent Years', *Reveal*, June 2017, www.revealnews.org/article/home-is-where-the-hate-is accessed 10 August 2019.

were also 66 jihadi-related attacks and attempted attacks and, out of those, 75% were stopped during planning. The issue of right-wing terrorist attacks has been more and more discussed in the US following the New Zealand Christchurch attack,[224] the El Paso attack[225] and the Pittsburgh attack[226] where the attackers referred to the same ideology, one driven by Replacement Theory.

TERRORISM AND ONLINE EXTREMISM

All terrorist attacks between 2008 and 2016 mentioned in the report by the Center for Investigative Reporting had aspects that connected them to online activity.[227] The US government has identified the risks associated with online radicalisation and the propaganda of extremists. The 2018 National Strategy for Counter-Terrorism, published by the White House,[228] identifies that "despite many setbacks, ISIS maintains a sophisticated and durable media and online presence that allows it to encourage and enable sympathisers worldwide to conduct dozens of attacks within target countries, including the United States". The strategy, being a publication of the Trump administration, ignores any dangers from, or online activity by, the American right-wing. A more detailed picture can be found in the Anti-Defamation League's annual report 'Murder

224 Evelyn Aswad, 'Why The Christchurch Call To Remove Online Terror Content Triggers Free Speech Concerns', *Just Security*, May 2019, www.justsecurity.org/64189/why-the-christchurch-call-to-remove-online-terror-content-triggers-free-speech-concerns accessed 10 August 2019.

225 Sam Levin, 'Police Thwarted At Least Seven Mass Shootings And White Supremacist Attacks Since El Paso', *The Guardian*, August 2019, www.theguardian.com/world/2019/aug/20/el-paso-shooting-plot-white-supremacist-attacks accessed 10 August 2019.

226 'At Least 10 People Dead In Pittsburgh Synagogue Attack', *Irish Examiner*, October 2019, www.irishexaminer.com/breakingnews/world/at-least-10-people-dead-in-pittsburgh-synagogue-attack-881656.html accessed 18 October 2019.

227 See Note 221.

228 'National Strategy For Counter-Terrorism Of The United States Of America', *Whitehouse.gov*, October 2018, www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf accessed 10 August 2019.

and Extremism in the United States in 2018'.[229] According to that report, 'extremist-related murders in 2018 were overwhelmingly linked to right-wing extremists' and every one of the perpetrators had some online ties to at least one right-wing extremist movement. The online home of a lot of the far-right extremists is Gab, a social media networking site created as the 'free speech' alternative to Twitter where extreme content of all kinds finds a home. It was used by the Pittsburgh attacker.[230]

THE STATE'S LEGAL RESPONSE

The 9/11 attacks led to immediate legislation in the shape of the 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001', commonly referred to as the USA PATRIOT Act (or simply the Patriot Act).[231] The law was legislated in a very hasty manner; it passed all stages of legislation and was signed by the president by 25 October. It carries an arsenal of tools that were intended to strengthen the power of the investigative bodies in their fight against terrorism. The law included amendments to existing laws that expanded the powers of the FBI and the police when searching, arresting and interrogating suspects of terrorism on terms and in conditions that had never previously been allowed. With regard to online activities, the law allowed the intelligence services to use wide-ranging electronic surveillance, as will be explained later. In order to keep some supervision above

229 'Murder And Extremism In The United States In 2018', *Anti-Defamation League*, 2019, www.adl.org/murder-and-extremism-2018 accessed 11 August 2019.

230 Jane Coaston, 'Gab, The Social Media Platform Favored By The Alleged Pittsburgh Shooter, Explained', *Vox*, October 2018, www.vox.com/policy-and-politics/2018/10/29/18033006/gab-social-media-anti-semitism-neo-nazis-twitter-facebook accessed 17 October 2019.

231 'Text – H.R.3162 – 107th Congress (2001–2002): Uniting And Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism (USA PATRIOT ACT) Act Of 2001', *Congress.gov,* 2001, www.congress.gov/bill/107th-congress/house-bill/3162/text/enr accessed 12 August 2019.

the law, some articles had to be renewed every few years. The USA PATRIOT Act Improvement and Reauthorization Act of 2005 made most of these articles permanent,[232] while others still had to be renewed. Following the Snowden exposure in 2013, the Obama administration passed the 'Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015', known as the FREEDOM Act.[233] This act did narrow the powers given to the authorities in the Patriot Act but still reaffirmed most of the legal tools that pre-existed in the law.[234]

BLOCKING AND REMOVAL OF ONLINE CONTENT

As part of the American commitment to their First Amendment rights, the US is the only country in this research that didn't create an administrative procedure to remove or block extremist content[235] online. Surprisingly, one of the more powerful legal protections for Internet service providers (ISPs) can be found in the Communications Decency Act.[236] Article 230 of the act protects websites and social networks from liability over third-party content published on their platform. The importance of the article to the freedom of the Internet in the US is second to none and it has been described as 'the law that gave us the Internet'.[237] The US courts have generally interpreted the

232 '#06-113: 03-02-06 Fact Sheet: USA Patriot Act Improvement And Reauthorization Act Of 2005', *Justice.gov*, 2005.

233 'Text – H.R.2048 – 114th Congress (2015–2016): USA FREEDOM Act Of 2015', *Congress.gov*, 2015, www.congress.gov/bill/114th-congress/house-bill/2048/text accessed 12 August 2019.

234 'The USA Freedom Act: What Is It and How Does It Affect Your Online Activities', *Pixel Privacy*, 2018, https://pixelprivacy.com/resources/freedom-act accessed 13 August 2019.

235 Some mechanisms exist on government sites in relation to sex trafficking.

236 The act is part of the Telecommunication Act: 'S.652 – 104th Congress (1995–1996): Telecommunications Act Of 1996'

237 Derek Khanna, 'The Law That Gave Us The Modern Internet – And The Campaign To Kill It', *The Atlantic*, September 2013, www.theatlantic.com/business/archive/2013/09/the-law-that-gave-us-the-modern-internet-and-the-campaign-to-kill-it/279588 accessed 13 August 2019.

law by giving wide protection to ISPs.[238] That said, the US government has joined in with the global political pressure on major social media platforms to tighten their own regulations regarding extremist content. This has led to a change in the attitude of the platforms towards such content.[239]

SURVEILLANCE

The Patriot Act gave the security agencies of the US extensive powers to monitor activity on the web. Edward Snowden[240] revealed that the FBI, the CIA and mainly the NSA have been using the law to collect an immense amount of data on foreign and American citizens. The collection was done using a few techniques: bulk surveillance; the PRISM Program, which allowed the NSA to demand, from Internet companies like Google and Facebook, data about their users without having to publish that they were asked to do it; and warrants approved by the Foreign Intelligence Surveillance Court (FISC) to enter a person's computer or phone and collect data.[241] The FISC is a secret court which issues judicial warrants for surveillance upon request by an agency where discussions are only carried out between the agency representative and the judge. The court has been criticised for the overwhelming approval rate of requests. It was discovered that, out of 33,900 *ex-parte*[242] requests to the court over

238 Eric Goldman, 'The Ten Most Important Section 230 Rulings', *Tulane Journal of Technology & Intellectual Property*, 20(1), 2017.

239 Julia Greenberg, 'Facebook And Twitter Face Tough Choices As ISIS Exploits Social Media To Spread Its Message', *WIRED*, November 2015 www.wired.com/2015/11/facebook-and-twitter-face-tough-choices-as-isis-exploits-social-media accessed 13 August 2019; Nancy Scola, Cristiano Lima, and Alexandra S. Levine, 'How Do You Solve A Problem Like 8Chan?', *POLITICO*, May 2019, www.politico.com/story/2019/08/05/8chan-donald-trump-shootings-1635690 accessed 13 August 2019.

240 See Note 148.

241 See Note 230.

242 'Ex-parte' is defined by the Oxford Dictionary of Law. as 'On the part of one side only', Law, J. (Ed.). *A Dictionary of Law*. OUP Oxford, 2015.

a period of 30 years, the judges denied only eleven.[243] The Freedom Act stopped the practice of bulk surveillance, allowed tech companies to reveal to the public that they are being requested to provide information by the security services and tightened the supervision of the FISC.[244] These changes to the law were accepted with some suspicion because many still thought that there was not enough supervision of the actions of the NSA.[245]

CRIMINAL LAW

The First Amendment gives strong protection to statements made online; therefore, US law doesn't contain the kind of direct free speech felonies found in Europe, such as apology for terrorism, glorification of terrorism or viewing offences. That said, in practical terms, a lot of the terrorist or terrorist-related offenses brought before US courts are based on online activities. A report[246] carried out by Colombia Law School and Human Rights Watch shows that, out of all the terrorist or terrorist-related offences that were brought to court in the ten years after 9/11 (500+), more than half were charged with the felony of material support,[247] based mainly on online correspondence and communications. This felony was amended in the Patriot Act and was expanded so that 'material

243 Conor Clarke, 'Is The Foreign Intelligence Surveillance Court Really A Rubber Stamp?', *Stanford Law Review*, February 2014, www.stanfordlawreview.org/online/is-the-foreign-intelligence-surveillance-court-really-a-rubber-stamp accessed 16 August 2019.

244 'Freedom On The Net 2018: United States', *Freedom House*, 2019, https://freedomhouse.org/report/freedom-net/2018/united-states accessed 16 August 2019.

245 Sharon Bradford Franklin, 'Fulfilling The Promise Of The USA Freedom Act: Time To Truly End Bulk Collection Of Americans' Calling Records', *Just Security*, March 2019, www.justsecurity.org/63399/fulfilling-the-promise-of-the-usa-freedom-act-time-to-truly-end-bulk-collection-of-americans-calling-records accessed 16 August 2019.

246 'Illusion Of Justice Report', *Columbia Law School*, 2014, www.law.columbia.edu/human-rights-institute/counterterrorism/domestic-counterterrorism/illusion-justice-report accessed 16 August 2019.

247 Title 18 of the United States Code, sections 2339A and 2339B.

support' includes 'expert advice or assistance' to a terrorist organisation and it made the punishment for attempts and conspiracies to provide material support the same as providing support. The US Supreme Court validated the wide interpretation of this felony in 'Holder v. Humanitarian Law Project'.[248] In this ruling, the court concluded, with a majority of six to three, that providing training in International Humanitarian Law to PKK Kurdish fighters, who are registered in the US as a terrorist organisation, could amount to a material support felony.[249] The Colombia Law Report has also found that there is excessive use by the FBI of online sting and undercover agents in an attempt to lure potential terrorists into action in order to charge them with a pre-emptive action.[250] The case of Adel Daoud[251] is an infamous one. He was a Muslim teenager with a slight mental disability who was recruited online by an FBI undercover agent who, through long conversations online, radicalised Daoud and later arrested him in a counter-terrorist sting operation. Another criticism that is often heard against law enforcement agencies in the US is the different legal approach taken in cases of jihadi terrorism as opposed to right-wing terrorism. As Shirin Sinnar[252] identifies, there are two kinds of terrorism laws in the US: international and domestic. And "law enforcement agencies frequently consider US Muslims 'international' threats even when they have

248 'Holder V. Humanitarian Law Project – Global Freedom Of Expression', *Global Freedom of Expression*, https://globalfreedomofexpression.columbia.edu/cases/holder-v-humanitarian-law-project accessed 16 August 2019.

249 Another case raising a similar question was the Tarek Mehanna case, which included a conviction for translating into English an Islamic text available online that is identified with al-Qaeda ideology. For more about that see: Innokenty Pyetranker, 'Sharing Translations Or Supporting Terror? An Analysis Of Tarek Mehanna In The Aftermath Of Holder V. Humanitarian Law Project', *American University National Security Law Brief*, 2, 2012.

250 Note 243 p. 13.

251 Criminal Complaint at 28, United States v. Daoud, No. 1:12-cr-00723 (N.D. Ill. filed Sept. 15, 2012).

252 Shirin Sinnar, 'Separate and Unequal: The Law of "Domestic" and "International" Terrorism', *Michigan Law Review*, 117, 2019.

scant foreign ties. As a result, they police and punish them more intensely than white nationalists and other 'domestic' threats."[253] Evidence to support this accusation of double standards when it comes to these two kinds of terrorism can be found in the US 2018 National Strategy for Counter-Terrorism,[254] the document that details at length the potential dangers of ISIS and al-Qaeda in radicalising US citizens. It ignores other domestic dangers and does not even contain the term 'right-wing'. This approach, as Sinnar identified, "not only harms individuals and communities but also reinforces distorted public perceptions of terrorism that fuel anti-immigrant and discriminatory policies".[255]

ADMINISTRATIVE MEASURES

As part of the Trump administration policy of connecting terrorism to immigration,[256] US visa procedures now require any applicant to agree that the US border control can check their social media activity over the previous five years.[257] These searches end up in denials of entry being given to more than 700 people a day.[258] The absurdity of this situation can be seen when we consider that the denial can be as a result of a post that was published by someone else in the applicant's feed. In a noted case, a Palestinian student (17) who received a scholarship

253 Ibid p. 1.

254 See Note 227.

255 See Note 248 p. 1.

256 Sarah Pierce and Andrew Selee, 'Immigration Under Trump: A Review Of Policy Shifts In The Year Since The Election', *Migration Policy Institute*, December 2017 www.migrationpolicy.org/research/immigration-under-trump-review-policy-shifts accessed 6 February 2020.

257 'United States: Online Visa Application Now Requests Social Media History', *Berry Appleman & Leiden LLP*, May 2019, www.balglobal.com/bal-news/online-visa-application-now-requests-social-media-history-united-states accessed 16 August 2019.

258 Zack Whittaker, 'U.S. Has Denied Entry To Some Because Of Others' Social Media – TechCrunch', *TechCrunch*, August 2019, https://techcrunch.com/2019/08/27/border-deny-entry-united-states-social-media accessed 16 August 2019.

to Harvard University was denied entry following remarks by some of his friends on his Facebook feed which the border agent identified as not in accordance with US policies.[259]

259 Sean Keane, 'Harvard Student Gets To Classes After Being Denied US Entry Over Friends' Social Media Posts', *CNET*, September 2019, www.cnet.com/news/harvard-student-gets-into-us-after-entry-denied-over-friends-social-media-posts accessed 16 August 2019.

POLICIES OF THE UNITED NATIONS AND THE EUROPEAN UNION

Terrorism can also, at times, be viewed as a global phenomenon, not only because it can impact countries all over the world but also because, in its new forms, it attempts to use the global interconnectedness of the world in order to arrange and execute its plans. The response to terrorism can be found not only at the level of country legislation but also in the policies, resolutions, conventions and directives of the UN and the EU.

THE UNITED NATIONS

Terrorist attacks in western countries have affected UN resolutions, its establishment of task forces, and policy developments in the area of counter-terrorism. Following the 9/11 attacks in the US, the UN Security Council passed a resolution[260] establishing the Counter-Terrorism Committee (CTC) and calling all countries to fight terrorism and to stop the financing of terrorism and the harbouring of terrorists. The 2004 attacks in Madrid resulted in another Security Council resolution,[261] this time establishing the Counter-Terrorism Committee Executive Directorate (CTED). Following the 7 July 2005 attacks in London, the Security Council passed a resolution[262] that calls on all states to adopt a law that prohibits the 'incitement to commit a terrorist act or acts'. In September 2006, the UN General Assembly adopted[263] the 'United Nations Global Counter-Terrorism

260 S/RES/1373 (2001).
261 S/RES/1535 (2004).
262 S/RES/1624 (2005).
263 A/RES/60/288 (2006).

Strategy'.[264] This strategy is reviewed every two years and is presented as leaning on four pillars:

1. Addressing the conditions that lead to the spread of terrorism;
2. Measures to prevent and combat terrorism;
3. Measures to build the capacity of states to prevent and combat terrorism and to strengthen the role of the United Nations system in that regard;
4. Measures to ensure respect for human rights for all and the rule of law as the fundamental basis for the fight against terrorism.

As part of the measures to combat terrorism, the strategy identifies, from the beginning, the need to "co-ordinate efforts at the international and regional level to counter terrorism in all its forms and manifestations on the Internet and use the Internet as a tool for countering the spread of terrorism". In 2013, a Security Council resolution[265] expressed concern over the "increased use, in a globalised society, by terrorists and their supporters, of new information and communication technologies, in particular the Internet, for the purposes of recruitment and incitement to commit terrorist acts, as well as for the financing, planning and preparation of their activities, and underlining the need for Member States to act cooperatively to prevent terrorists from exploiting technology". In 2017, the Security Council adopted, in a resolution,[266] the Counter-Terrorism Committee's 'Comprehensive International Framework to Counter Terrorist Narratives'. The resolution includes some general statements regarding the development of counter narratives and a call for the Counter-Terrorism Committee to "develop models for effectively countering terrorist narratives, both online and offline".

264 'UN Global Counter-Terrorism Strategy, Counter-Terrorism Implementation Task Force', *United Nations*, 2006, www.un.org/counterterrorism/ctitf/en/un-global-counter-terrorism-strategy accessed 17 August 2019.

265 S/RES/2129 (2013).

266 S/RES/2354 (2017).

UN counter-terrorism activity is constantly reviewed, according to the protections of human rights, as it is one of the four pillars of the UN counter-terrorism strategy. In parallel to the adaptation of the UN counter-terrorism strategy, the Commission on Human Rights appointed a special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.[267] The rapporteur publishes yearly reports, country reports and special reports.[268] In some of these reports, there is strong criticism of online counter-terrorism policies.[269]

THE EUROPEAN UNION

The EU, as a regulatory body, began its involvement in counter-terrorism after the 9/11 attacks. Prior to it, counter-terrorism was mainly dealt with by the European countries that were impacted by internal terrorism, such as the UK, Spain and Germany.[270] In December 2001, the European Council passed two initial important decisions, one was the 'framework decision on combating terrorism' and the second was the 'framework decision on the European arrest warrant and the surrender procedures between the Member States'.[271] The 'combating terrorism' decision included the first European common definition of 'terrorism' at a time when several member states did not have

267 Resolution 2005/80 of the Commission.

268 'OHCHR Special Rapporteur on Counter-Terrorism and Human Rights', *Office of the United Nations High Commissioner for Human Rights*, 2019, www.ohchr.org/EN/Issues/Terrorism/Pages/SRTerrorismIndex.aspx accessed 17 August 2019.

269 For example, see: *Office of the United Nations High Commissioner for Human Rights*, 2019, https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=24234 accessed 17 August 2019.

270 Peter Chalk, *West European Terrorism and Counter-Terrorism*, Springer, 1996.

271 '1. On The Commission Proposal For A Council Framework Decision On Combating Terrorism; 2. On The Commission Proposal For A Council Framework Decision On The European Arrest Warrant And The Surrender Procedures Between The Member States', *European Parliament*, 2001, www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A5-2001-0397&language=EN accessed 1 September 2019.

any legal definition of 'terrorism'.[272] The 'arrest warrant' decision enabled European countries to help each other in fighting terrorism on a European level.[273] Following the terrorist attack in Spain (2004), the European Council published its Declaration on Combating Terrorism,[274] urging countries to adopt into legislation the guidelines contained in the 2001 frameworks. Following the attack in the UK (2005), the European Council adopted the 'EU counter-terrorism strategy to fight terrorism globally and make Europe safer'.[275]
The strategy, like the UN strategy, is based on four pillars: Prevent, Protect, Pursue and Respond. It was revised in 2014 in order to adapt to recent developments in terrorism. Following the ISIS attacks in Europe from 2015 on, the movement of foreign fighters and waves of immigration, as well as the internal response to them, a new wave of activity relating to counter-terrorism was promoted by the EU. In July 2015, Europol created a dedicated unit to tackle terrorist propaganda on the Internet, the EU Internet Referral Unit (EU IRU).[276] The goals of the unit are to identify terrorist and violent extremist content online and to advise member states. Data from the unit's first report tells us that it has referred 11,050 items to be removed from 70 different platforms with a success rate of 91%.[277] In January 2016, Europol

272 Christian Kaunert and Sarah Léonard, 'The Collective Securitisation of Terrorism in the European Union', *West European Politics*, 42(2), 2019.

273 Cristian Kaunert, 'The External Dimension Of EU Counter-Terrorism Relations: Competences, Interests, And Institutions', *Terrorism and Political Violence*, 22(1), 2009.

274 'Declaration On Combating Terrorism', *European Council*, 2004, www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/79637.pdf accessed 1 September 2019.

275 'EU Counter-Terrorism Strategy', *European Council*, 2005, www.consilium.europa.eu/en/policies/fight-against-terrorism/eu-strategy accessed 1 September 2019.

276 'Europol's Internet Referral Unit To Combat Terrorist And Violent Extremist Propaganda', *Europol*, July 2015, www.europol.europa.eu/newsroom/news/europol%E2%80%99s-internet-referral-unit-to-combat-terrorist-and-violent-extremist-propaganda accessed 2 September 2019.

277 'EU Internet Referral Unit – Year One Report – Highlights', *Europol*, February 2016, www.europol.europa.eu/publications-documents/eu-internet-referral-unit-year-one-report-highlights accessed 1 September 2019.

created a specific unit to co-ordinate all of its counter-terrorism activity, the European Counter-Terrorism Centre (ECTC), which then took charge of EU IRU activities.

In February 2017, the European Council and Parliament approved the most extensive counter-terrorism directive ever introduced at a European level – Directive 2017/541.[278] The directive gave the member states[279] 18 months to adopt its rules to their national laws. The directive gives a wide definition for 'terrorist offences' (Article 3) which includes a list of violent actions against humans or property but also 'threatening to commit any of the acts'. The directive introduces several offences that can relate to online activity such as: 'supplying information or material resources' to terrorist organisations (Article 4); 'public provocation to commit a terrorist offence' (Article 5), which includes prohibition of incitement and glorification directly or indirectly; 'recruitment for terrorism' (Article 6); and 'providing training for terrorism' (Article 7), which includes providing instructions. Article 14(2) forbids 'inciting an offence referred to in Articles 3 to 12', which makes, for example, inciting to incitement a felony (Article 14(2)+5). Article 21 is dedicated to the blocking and removal of content from online platforms and calls on the member states to adopt a mechanism allowing them to 'ensure the prompt removal of online content constituting a public provocation to commit a terrorist offence'. The directive was intended to create a standard for the criminalisation of terrorism offences in Europe, though all the European countries in this research already had similar internal legislation of their own, prior to the directive.

278 'EU Strengthens Rules To Prevent New Forms Of Terrorism', *European Council*, March 2017, www.consilium.europa.eu/en/press/press-releases/2017/03/07/rules-to-prevent-new-forms-of-terrorism accessed 2 September 2019.

279 Ireland and the UK were not bound.

Since 2018, the European Commission has been advancing a new regulation regarding preventing the dissemination of terrorist content online.[280] The proposed regulation[281] includes among other aspects: the one-hour rule, proposing a legally binding one-hour deadline for content to be removed; a definition of terrorist content as material that incites or advocates committing terrorist offences, promotes the activities of a terrorist group or provides instructions and techniques for committing terrorist offences; and proactive measures for social media platforms to better protect their platforms and their users from terrorist abuse. The regulation was criticised by experts of the United Nations Human Rights Council[282] and the EU Fundamental Rights Agency (FRA)[283] for its broad definition of terrorist content and it is still at the negotiation stage and has not yet been approved.

280 'Preventing The Dissemination Of Terrorist Content Online', *European Parliament*, 2019, www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-preventing-the-dissemination-of-terrorist-content-online/07-2019 accessed 2 September 2019.

281 'Proposal for a Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online', *EUR-Lex*, September 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0640:FIN.

282 See: *Office of the United Nations High Commissioner for Human Rights*, 2019, https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=24234 accessed 2 September 2019.

283 'Proposal for a Regulation on Preventing the Dissemination of Terrorist Content Online and Its Fundamental Rights Implications', *European Union Agency for Fundamental Rights*, February 2019, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-opinion-online-terrorism-regulation-02-2019_en.pdf accessed 3 September 2019.

DISCUSSION

This report presents the wide range of legal tools that different countries use in order to cope with violence and terrorism which are connected to online activity and the possible impact of these tools on the human rights to privacy and freedom of speech. Some of the findings of the report might be outdated in as little as a year's time, considering the increasing global awareness of the situation, the rapid changes in technology and the constant regulation attempts. Thus, the issues that are raised will remain present and will only intensify – such as the tension between the need to prevent violence and stop online extremism as an accelerator for it and the need to preserve basic freedoms for the citizens in democracies. The following paragraphs will discuss the possible future legal and political questions that may arise from the described tensions.

RE-DISCUSSING THE RIGHTS TO PRIVACY AND FREEDOM OF SPEECH IN THE ONLINE SPHERE

The legal rights to privacy and freedom of speech were first formulated in a world extremely different to the world where most citizens of western liberal democracies live today. Therefore, the original theoretical and philosophical justifications for the protection of the rights may seem outdated.[284] For example, the basic philosophical justification for freedom of speech was the idea developed by John Stuart Mill in his book *On Liberty* from 1859. According to Mill, silencing opinions is wrong because the truth or real knowledge only comes from the argument between different opinions. Silencing an opinion,

284 For more about this, see: Will Thomas DeVries, 'Protecting Privacy in The Digital Age' *Berkeley Technology Law Journal*, 18, 2003; Dawn C. Nunziato, *Virtual Freedom: Net Neutrality and Free Speech In The Internet Age*, Stanford University Press, 2009.

according to Mill, even if the opinion is false, is wrong because, without the triumph of the true opinion over the false opinion, there is no validity to the truth, and this is the basis of the right to free speech. In the years that have passed since Mill's book, the tragic impacts that false propaganda have had on the history of the world and the theories of postmodern philosophers have created many holes in Mill's theory. The emergence of the Internet, which gave billions of people a voice, has created a discourse that is very different from the time when Mill's ideas were formed.

Having said that, up until today, the main legal theoretical justification for freedom of speech is based on Mill's ideas. It is true that more philosophical justifications for freedom of speech have been added to Mill's ideas, such as the understanding that revoking freedom of speech can hurt the right to autonomy and self-fulfillment,[285] but the legal philosophical discourse is far from keeping pace with technological impacts on speech and privacy. A continuous discourse on the justifications for the rights to privacy and free speech in light of the technological and political changes is essential, not only for the advancement of knowledge but also for confronting the challenges to these rights. On the one hand, it is important in order to have a robust legal argument against countries who put severe restrictions on speech and knowledge online and who constantly monitor private online correspondence – such as China or Iran. On the other hand, it is important in order to define the limits to those rights in light of the use of the online sphere by extremists and violent organisations and individuals. Only by creating a clear understanding of the current legal justifications for these rights can we determine what kind of protections do they require, in what situations and what legal tools should be used in order to achieve them.

285 In Procunier v. Martinez, the US Supreme Court noted that "The First Amendment serves not only the needs of the polity but the needs of the human spirit – a spirit that demands self-expression."

THE ROLE OF THE LAW IN THE DISCUSSION ABOUT FAKE NEWS AND THE TRUTH

As more and more people in the world have started to rely on social media platforms as their main source of news,[286] the temptation for interest groups to control and navigate the discourse to suit their agenda has grown. The possibility of creating anonymous or fake users on most of the social platforms has opened the way to massive and multinational operations to influence public opinion using social media. Those using this media have learned quickly, studies have shown, that the more outrageous, conspiratory and fake the post is, the quicker it will spread and impact opinions, as humans apparently will always prefer the sensational over the mundane truth.[287] These facts have not escaped those who wish to spread extremist and violent agendas online. They have started to spread propaganda using fake and inflammatory material in order to create the required impact to go with their views. The interesting question is what the role of the law should be when it comes to this phenomenon.

Trying to regulate by law the issue of fake/truth expressions takes us into a political and philosophical minefield. The first challenging question is what should be regulated – facts, opinions, beliefs? The mere attempt to differentiate between these is problematic. Let's take, for example the 'flat earth theory', which seems like an easy case. We know the earth is not flat and therefore it is wrong. But it is not that simple. The people who are supporting the flat earth theory believe the earth is flat in the same way some of the people who believe in the monotheistic religions believe the world was created in seven days. Philosophically, there is no difference between those beliefs, but it is still unthinkable to create a law that forbids mentioning the creation

286 Amy Watson, 'Usage Of Social Media As A News Source Worldwide 2019', *Statista*, September 2019, www.statista.com/statistics/718019/social-media-news-source accessed 1 December 2019.

287 Brian Resnick, 'Social Media's Conspiracy Theory Problem Isn't Going Away', *Vox*, August 2019, www.vox.com/science-and-health/2019/8/13/20802068/epstein-conspiracy-theory-clintonbodycount-psychology accessed 5 December 2019.

according to religious scriptures. To add to that, as post-modernist philosophy has taught us, the understanding that truth is based on the way each of us experience it is another aspect that will make it difficult to give an absolute legal definition of 'truth'.

A narrow test that examines if 'non-truth' has the potential to create or encourage harm does not lead to clear solutions. Let's take, for example, the popular conspiracy theory that Apollo 11 never landed on the moon. *Prima facie*, there is no real harm in allowing this ridiculous story to stay within the online sphere but, as we know, the harm and danger of conspiracy theories are in the cumulative effects, which encourage a general mistrust of authority-based information.[288] This tendency is used by extremists to encourage others to support more dangerous conspiracy theories like 'Jewish world domination' and replacement theories. So once again the question is asked where and how should the law draw the line.

Adding to those conceptual problems of using the law to regulate truth, there are always the practical dangers. Some truths are very not pleasant to hear or do not fit the political atmosphere in a specific area; a tool to erase 'non-truths' can be easily used to make unpleasant truth disappear. In this way, the Turkish government will have legitimacy in erasing claims regarding the Armenian genocide since they perceive it as untrue. Also, the Polish government could rewrite Polish history and present the Polish people as the leaders of the resistance to Nazi Germany in a way that fits their understanding of the truth, and the Chinese could argue that it is fake news that their president is similar to cartoon bear Winnie the Pooh.

It can't be ignored that the law is (or more specifically the courts are) dealing on a daily basis with the question of what the truth is, including in specific cases such as those concerning defamation where 'truth of expression' could be a legitimate defence. The difference is that finding the truth in those cases is only a tool

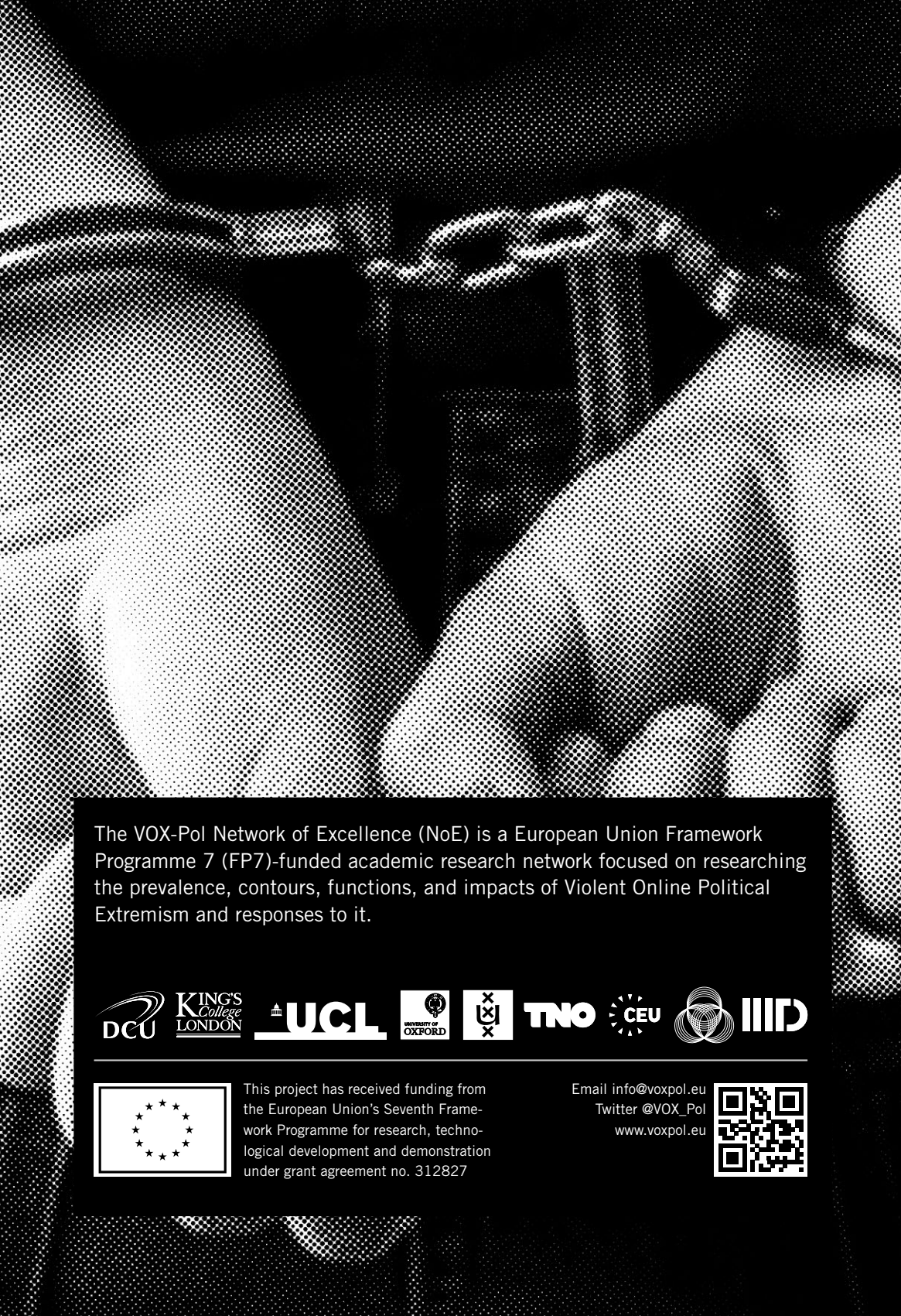
288 Melissa Chan, 'Conspiracy Theories Might Sound Crazy, But Here's Why Experts Say We Can No Longer Ignore Them', *Time*, August 2019, https://time.com/5541411/conspiracy-theories-domestic-terrorism accessed 26 December 2019.

in order to solve a specific conflict between two sides, and not a main goal in itself. The law, in this author's opinion, should not be the arena to decide on the basic philosophical arguments we have as a society, no matter how absurd they seem to us.

A CLOSING REMARK ABOUT THE FUTURE OF LEGAL DISCOURSE

The current political atmosphere in many western liberal democracies is extremely polarised and the academic discourse has not been immune from this polarisation. The discourse about online extremism has created an interesting opportunity to reshuffle the usual stands taken by each side on the human rights/security axis. The fact that right-wing extremist content and activity is, in some countries, directly aimed at those who usually promote human rights such as freedom of speech has created some confusion in the automatic reaction of both sides. While groups and individuals who are usually avid defenders of human rights find themselves calling for more restrictions on online expressions, those who usually call for stricter law enforcement when it comes to online jihadi terrorism, find themselves as avid protectors of freedom of speech.

This situation, which shifts the sides from their usual comfortable positions, creates the potential for a more honest discourse regarding the dangers and legal protections that need to be developed when regulating the online sphere.



The VOX-Pol Network of Excellence (NoE) is a European Union Framework Programme 7 (FP7)-funded academic research network focused on researching the prevalence, contours, functions, and impacts of Violent Online Political Extremism and responses to it.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 312827

Email info@voxpol.eu
Twitter @VOX_Pol
www.voxpol.eu