SOCIAL MEDIA REGULATIONS:
A comparative study of six jurisdictions

Table of Contents:

1. Introduction..... 3
2. European Union..... 4
3. United Kingdom..... 6
4. United States..... 10
5. India..... 13
6. Turkey..... 16
7. France..... 18

Introduction

This comparative study by Bolo Bhi titled “Social media regulations: A comparative study of six jurisdictions” summarises the current social media related regulations in the European Union, United Kingdom, United States, India, Turkey, and France. This was done in order to facilitate an informed discussion about social media related regulations around the world in the more prominent jurisdictions, to be able to learn from the lapses in these regulations and the process of consultation with relevant stakeholders.

We are thankful to Shumaila Shahani, Research Associate; and Rachna Rajput, Legal Intern for undertaking the research for this study.

In relation to the six jurisdictions, the study includes:

1. Prevailing laws and time of introduction,
2. Process of legislation, consultation, and implementation timeline
3. Views for and against these
4. Protections

The study is in no way exhaustive, and does not reflect any endorsement by Bolo Bhi.

EUROPEAN UNION

Prevailing laws and time of introduction

In May 2016, the European Commission agreed with Facebook, Microsoft, Twitter and YouTube a "Code of conduct on countering illegal hate speech online" aiming to prevent the spread of illegal hate speech online, as defined by framework Decision 2008/913/JHA of 28 November 2008. Under the code, the IT companies are required to implement the commitments in the Code.[1]

Process of legislation, consultation, and implementation timeline

According to the European Commission's website, the implementation of the Code of Conduct "is evaluated through a regular monitoring exercise set up in collaboration with a network of organisations located in the different EU countries. Using a commonly agreed methodology, these organisations test how the IT companies are implementing the commitments in the Code".[2] Later, Instagram, Google+, Snapchat, Dailymotion and Jeuxvideo.com also joined the Code of Conduct.[3]

It was created in response to increasing racist and xenophobic hate speech online.[4] The results of a first monitoring exercise were published on 07 December 2016[5] and the results for a second monitoring round and a third monitoring round published on dated 01 June 2017[6].

A Commission Recommendation on measures to tackle effectively illegal content online was published on 01 March 2018[7]. "It contains two parts, a general part on measures applicable to all types of illegal content and a specific part addressing the special actions that platforms would need to take to address terrorist content. In terms of the rules applicable to all types of illegal content the recommendation includes clearer 'notice and action' procedures, more efficient tools and proactive technologies, stronger safeguards to ensure fundamental rights, special attention to small companies and closer cooperation with authorities".[8]

Views for or against these

Critics say that disadvantaged and ethnic minorities are sometimes the ones charged with violating laws against hate speech.[9] Kim Holmes, critic of the theory of hate speech, has argued that it "assumes bad faith

---

[1] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en#theeucodeofconduct

[2] *ibid*

[3] *ibid*

[4] Countering illegal hate speech online – EU Code of Conduct ensures swift response (https://ec.europa.eu/commission/presscorner/detail/en/IP_19_805)

[5] https://ec.europa.eu/information_society/newsroom/image/document/2016-50/factsheet-code-conduct-8_40573.pdf

[6] https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=71674

[7] https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_1170

[8] Code of Conduct on countering illegal hate speech online: Questions and answers on the fourth evaluation (https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vkvqhdpz9bph?ctx=vggbnhigl7xa)

[9] 'Minorities suffer the most from hate-speech laws' (https://www.spiked-online.com/2018/12/14/minorities-suffer-the-most-from-hate-speech-laws/)

on the part of people regardless of their stated intentions" and that it "obliterates the ethical responsibility of the individual".[10]

Protections

1. Ismayilova v. Azerbaijan 2020

   The European Court of Human Rights (ECtHR) ruled in February 2020[11] that the 2014 arrest and pre-trial detention of Azerbaijani journalist and Organized Crime and Corruption Reporting Project (OCCRP) contributor Khadija Ismayilova was unlawful and politically motivated[12]. The Court held that Azerbaijan violated several articles of the European Convention on Human Rights[13] by arresting Ismayilova "without a reasonable suspicion of an offence"[14].

2. Digital Rights Ireland Case 2014

   The European Court of Justice in the Digital Rights Ireland Case in 2014[15] held that the Data Retention Directive 2006, under which the telecoms companies were obliged to collect and retain location and traffic data about phone calls, text messages, emails and internet use for between six months and two years, is invalid for causing interference with the fundamental right to privacy and right to the protection of personal data[16].

3. CJEU's 2016 Judgment

   In 2016, the Court of Justice of the European Union (CJEU) repeated arguments made previously in the 2014 Digital Rights Ireland case, and ruled that the generalised data retention is disproportionate and unlawful[17].

   The CJEU held that access to retained data be made subject to a prior review by courts or independent administrative bodies and laws should be made proportional, even if they pertain to fighting crime[18]. The CJEU has further held that suspects should be notified prior to accessing their information and that requirement be seen as a basic component of laws around surveillance[19].

---

[10] The Origins of "Hate Speech" (https://www.heritage.org/civil-society/commentary/the-origins-hate-speech)
[11] https://hudoc.echr.coe.int/fre-press#{%22itemid%22:[%22003-6649321-8835799%22]}
[12] https://www.occrp.org/en/daily/11706-echr-arrest-of-khadija-ismayilova-was-unlawful
[13] https://www.echr.coe.int/Documents/Convention_ENG.pdf
[14] https://hudoc.echr.coe.int/fre-press#{%22itemid%22:[%22003-6649321-8835799%22]}
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293
[16] European Court of Justice finds data retention directive invalid (https://www.openrightsgroup.org/press/releases/european-court-of-justice-finds-data-retention-directive-invalid)
[17] http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=516300
[18] EU Court slams UK data retention surveillance regime (https://www.openrightsgroup.org/blog/2016/eu-court-slams-uk-data-retention-surveillance-regime)
[19] EU Court slams UK data retention surveillance regime (https://www.openrightsgroup.org/blog/2016/eu-court-slams-uk-data-retention-surveillance-regime)

UNITED KINGDOM

Prevailing laws and time of introduction

1. The Digital Economy Act 2017:

   The Digital Economy Act 2017 creates a legal right for users to request a minimum standard of broadband connectivity of at least 10 megabits per second (Mbps).

   "The Act also introduces reform of the Electronic Communications Code, and provides greater clarification on data sharing between public bodies."[20]

   Section 103 is the part of Digital Economy Act 2017 where the Code of Practice is written. This law deals with online communication. It gives material about what will happen when someone breaks the law. The Act is made up of six parts as follows:

   I. Access to digital services
   II. Digital infrastructure
   III. Online pornography
   IV. Intellectual property
   V. Digital government
   VI. Miscellaneous."

   The Act was presented by culture secretary John Whittingdale in the House of Commons on 5 July 2016 and finished its parliamentary stages and acknowledged Royal Assent on 27 April 2017.

   Critics raised concerns about the privacy implications of collecting user data, and the possible ineffectiveness of a method focused on restricting payments. Moreover they also highlighted the potential unprotected age verification system to hacking, and advised that it would result in more people using Virtual Private Networks (VPNs).[21]

   A number of expert witnesses to the Digital Economy Bill Committee voiced concerns about the bill. Jerry Fishenden, co-chair of the Cabinet Office's Privacy and Consumer Advisory Group said that the bill was based on an "obsolete" model of data sharing. He commented: "I find it surprising the bill doesn't have a definition of what data sharing is, both practically and legally. I'd like to see some precision around what's meant by data sharing. The lack of detail is concerning." He also argued that the bill "appears to weaken citizens' control over their personal data"[22][23]

2. Counter-Terrorism and Border Security Act 2019:

[20] Digital Economy Act 2017 (https://www.legislation.gov.uk/ukpga/2017/30/contents/enacted)
[21] Porn check critics fear data breach (https://www.bbc.com/news/technology-43292457)
[22] the canary that ceased to be (https://ntouk.wordpress.com/2017/05/03/the-canary-that-ceased-to-be/)
[23] Digital Economy Bill lacks clarity on data sharing, experts say (https://www.computerweekly.com/news/450401071/Economy-Bill-lacks-clarity-on-data-sharing)

The Counter-Terrorism and Border Security Act 2019[24] criminalizes the viewing of online content that can be useful for terrorism, intentionally or unintentioanally, penalising it with up to 15 years in prison. The Act also criminalises the publication of certain images of clothing and the expression of support for a proscribed organisation among other items[25].

3. The Online Harms White Paper 2019:

The Online Harms White Paper[26] was published in 2019. The Government published their initial response to the consultation feedback on February 12, 2020[27] and a draft bill is expected to be published later in the year. Under the proposals, social media companies would have a 'duty of care' to their users "to make companies take more responsibility for the safety of their users and tackle harm caused by content or activity on their services"[28]. The list of harms incudes: "child exploitation; terrorist content; organised immigration crime; modern slavery; extreme pornography; revenge pornography; harassment and cyberstalking; hate crime; encouragement to suicide; violence incitement; sales of weapons or drugs; prisoners' use of the internet; and sexting between minors"[29]. Overseeing all of this, we have now learned, will be poor old Ofcom. There is a possibility that Ofcom will be appointed as a regulator to oversee compliance with the duty of care[30].

Article 19 said the failure to comply may also make social media bosses personally liable.[31]

Process of legislation, consultation, and implementation timeline

1. Counter-Terrorism and Border Security Act 2019:

The Counter-Terrorism and Border Security Bill was introduced into parliament on 06 June 2018[32]. Stakeholders published their criticisms and comments before the Bill received Royal Assent on 12 February 2019[33].

2. The Online Harms White Paper 2019:

---

[24] http://www.legislation.gov.uk/ukpga/2019/3/contents

[25] https://www.independent.co.uk/news/uk/home-news/terrorist-propaganda-law-thought-crime-click-link-online-prison-a8866061.html

[26] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

[27] https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response

[28] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

[29] https://www.wired.co.uk/article/online-harms-uk

[30] https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response

[31] Freedom of expression in the UK Policy briefing, March 2020 (https://www.article19.org/wp-content/uploads/2020/03/Fex_UK_briefing.pdf)

[32] https://services.parliament.uk/Bills/2017-19/counterterrorismandbordersecurity/stages.html

[33] https://www.parliament.uk/business/news/2019/february/royal-assent--counter-terrorism-and-border-security-bill-signed-into-law/

The Online Harms White Paper was published in 2019[34]. Consultation process commenced from 08 April 2019 to 01 July 2019, which received over 2,400 responses from stakeholders that include tech companies, think tanks, rights groups, governmental organisations etc.[35] The Government published their initial response to the consultation feedback on February 12, 2020[36].

Views for or against these

1. Counter-Terrorism and Border Security Act 2019:

Rebecca Vincent, UK Bureau Director Reporters Without Borders said that, "We welcome the inclusion of specific journalistic exemptions in some clauses of the bill, which would have created 'no-go' zones for journalists and otherwise restricted their ability to do their jobs. However, other provisions of the bill remain threatening to the protection of journalistic sources and broader press freedom, which is worrying indeed given other ongoing legislative moves that could further restrict press freedom in the UK".[37]

ARTICLE 19 criticised this legislation as overly broad and unnecessary[38] stating that "it could criminalise the expression of opinions or beliefs, the documentation of human rights abuses or the making of misguided jokes"[39].

Under the Counter-Terrorism and Border Security Act 2019, the government was supposed to appoint an independent reviewer assigned with the task to independently review Prevent Strategy and submit it to the Parliament[40]. The Rights Watch (UK) has said that they are taking the government to court by for failing to appoint an independent reviewer of its Prevent strategy[41]. Conor McGinn, the shadow security minister, said, "The introduction of a new counter-terrorism bill before the Prevent review has even begun underlines just how much time the government has wasted".[42]

---

34 rpc.co.uk/snapshots/technology-digital/online-harms-white-paper-consultation-response/
35 https://www.rpc.co.uk/snapshots/technology-digital/online-harms-white-paper-consultation-response/
36 https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response
37 https://rsf.org/en/news/new-uk-counter-terrorism-legislation-contains-some-journalistic-protections-threatens-press-freedom
38 ARTICLE 19 written evidence in House of Commons Public Bill Committee – Counter-Terrorism and Border Security Bill 2018 (https://www.article19.org/wp-content/uploads/2018/07/UK-CT-and-Border-Security-Bill-FINAL-Public-Bill-Committee-26062018.pdf)
39 Freedom of expression in the UK Policy briefing, March 2020 (https://www.article19.org/wp-content/uploads/2020/03/Fex_UK_briefing.pdf)
40 Government to be challenged in court over Prevent reviewer (https://www.theguardian.com/uk-news/2020/feb/06/government-to-be-challenged-in-court-over-prevent-reviewer)
41 Government to be challenged in court over Prevent reviewer (https://www.theguardian.com/uk-news/2020/feb/06/government-to-be-challenged-in-court-over-prevent-reviewer)
42 https://www.theguardian.com/uk-news/2020/jun/09/labour-attacks-complacency-over-delayed-prevent-review#top

Index on Censorship's Head of Advocacy Joy Hyvarinen said that, "The Counter-Terrorism and Border Security Act crosses a line that takes the law very close to prohibiting opinions... The act criminalises expressing an opinion or belief that is 'supportive' of a proscribed (terrorist) organisation if done in a way that is 'reckless' as to whether it encourages another person to support a proscribed organisation". He called it a "very dangerous legislative step to take in a democratic society".[43]

2. The Online Harms White Paper 2019:

   ARTICLE 19 believes that the proposal will "delegate censorship powers to private companies, and could require the bulk surveillance of what we post online. It will also almost inevitably lead to the removal of legitimate content as companies are likely to err on the side of caution and remove content at scale".[44]

   David Court writes in his opinion piece in stuff.co.nz[45]: "The summary of this paper states that its vision is for a 'free, open and secure internet' that supports 'freedom of expression online'. Yet a few hundred words later it outlines its plans for a 'new regulatory framework for online safety' where it promotes the need for an independent regulator."

FURTHER ATTEMPTS TO SURVEIL

1. MI5 boss Andrew Parker asks tech firms: Create a way to let us read suspects' secret messages to stop UK terror attacks

Protections

1. Harry Miller case:

   The High Court ruled in February 2020 that the police response over allegedly "transphobic" tweets by turning up at an ex-officer Harry Miller's place of work was unlawful[46]. The Court compared police to Stasi and Gestapo as a judge ruled that police interfered in freedom of speech by investigating 'non crime' trans tweet.[47]

---

[43] indexoncensorship.org/2019/02/freedom-of-expression-and-the-counter-terrorism-and-border-security-act/

[44] Freedom of expression in the UK Policy briefing, March 2020 (https://www.article19.org/wp-content/uploads/2020/03/Fex_UK_briefing.pdf)

[45] https://www.stuff.co.nz/business/opinion-analysis/111987212/internet-giants-like-facebook-youtube-and-twitter-are-facing-tougher-regulation

[46] Police compared to Stasi and Gestapo by judge as he rules they interfered in freedom of speech by investigating 'non crime' trans tweet (https://www.telegraph.co.uk/news/2020/02/14/police-compared-stasi-gestapo-judge-rules-interfered-freedom/)

[47] Police compared to Stasi and Gestapo by judge as he rules they interfered in freedom of speech by investigating 'non crime' trans tweet (https://www.telegraph.co.uk/news/2020/02/14/police-compared-stasi-gestapo-judge-rules-interfered-freedom/)

UNITED STATES

Prevailing laws and time of introduction / Process of legislation, consultation, and implementation timeline

A discussion draft has floated to establish a National Commission on Online Child Exploitation Prevention, and for other purposes. Individually the Attorney General, under the draft bill, could command on how online platforms and services should run. If some companies don't follow the rules made by the Attorney Generals, they could be liable for millions of dollars in state criminal penalties and civil damages. This bill is identified as the Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act, Hence the Executive Branch has been given powers through it. Moreover, it also unlocks the entry for the government to require new methods to screen users' speech and backdoors to read private communications—a stated goal of one of the bill's authors.[48]

Encryption:

End-to-end encryption causes a problem for US law enforcement because even if they have the correct legal process (such as a search warrant or subpoena) to "unlock" a phone, encryption might prevent them from doing so, as was seen in the *Apple vs. FBI* case. Therefore, there is a lot of pressure from US politicians to have companies engineer encryption backdoors or store encryption keys locally on devices. There are hearings taking place currently in Congress covering this subject.

What are the views for or against these?

Chairman of the Senate Judiciary Committee Lindsey Graham and Democratic Senator Richard Blumenthal proposed a bill which intends to challenge child pornography on platforms like Alphabet's Google and Facebook by making them accountable for civil lawsuits and state prosecution. It would do this by threatening a key immunity from liability which the companies have under the federal law called Section 230 of the Communications Decency Act (CDA) of 1996 which states that no user of an interactive computer service will be dealing as the publisher or speaker of any data provided by another data content provider. However, a discussion draft of the EARN IT Act has been criticized by technology corporations."”[49]

Protections

The United States Constitution forbids laws that prohibit the free exercise of religion or curtail the freedom of speech, the right to assemble peacefully, the freedom of the press or the right to petition the government for a redress of grievances, protected by The First Amendment (Amendment I) that was passed on December 15, 1791.

In Packingham v. North Carolina (2017), the Supreme Court held that a North Carolina law prohibiting registered sex offenders from accessing different websites was inadmissible as it restricted lawful speech in violation of the First Amendment. The Court held that "a fundamental principle of the First Amendment

[48] https://www.eff.org/deeplinks/2020/01/congress-must-stop-graham-blumenthal-anti-security-bill
[49] https://www.itnews.com.au/news/encryption-on-facebook-google-others-threatened-by-planned-new-bill-538458

is that all persons have access to places where they can speak and listen, and then, after reflection, speak and listen once more". ".[5051]

Section 230 of the Communications Decency Act:

The initial purpose of the legislation was to restrict free speech on the Internet. The Communications Decency Act (CDA) was objected strongly by the whole Internet community, and the anti-free speech provisions were struck down by the Supreme Court. However, Section 230 declares that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.".[52]

Putting it differently, any online service that publishes third-party content has been secured from legal liability for what others do and say.[53]

Section 230 of CDA provides legal cover to bloggers from liability for comments left by their readers, the work of guest bloggers, tips sent via email, or information received through RSS feeds. Even if one blogger is aware of the "objectionable content" or makes editorial judgments will not be held liable.[54]

The Washington Privacy Act

The three bills were introduced by Washington state lawmakers and were targeted at a collection of consumer privacy issues in 2020. "The first bill, SB 6281, also known as the Washington Privacy Act, was announced in the House on 14 January. It is an inclusive privacy bill demonstrated after the European Union's General Data Protection Regulation (GDPR) with features of the California Consumer Privacy Act (CCPA). The second bill, HB 2485, announced on 15 January in the House, which would use practices of consumer genetic-testing companies and regulate data collection. HB 2644, was announced the next day in the House. Moreover, It pursues to limit the use of artificial intelligence-enabled profiling. Whereas HB 2644 and HB 2485 aim to separate privacy concerns, SB 6281 efforts to set general guardrails for the permissible use, collection, and disclosure of Washington residents' personal data."[55]

EU-US Privacy Shield - Cross border data transfers:

The EU–US Privacy Shield is a structure for governing transatlantic exchanges of personal data for commercial purposes amongst the United States and the European Union. One of its objectives is to permit US companies to obtain personal data more easily from EU entities under EU privacy laws meant to guard European Union citizens.

[50] https://www.oyez.org/cases/2016/15-1194
[51] https://www.supremecourt.gov/opinions/16pdf/15-1194_08l1.pdf
[52] https://www.law.cornell.edu/uscode/text/47/230
[53] https://www.eff.org/issues/cda230
[54] https://www.eff.org/issues/cda230
[55] The Washington Privacy Act Is Back (https://www.jdsupra.com/legalnews/the-washington-privacy-act-is-back-57678/)

The US recently passed something called the CLOUD act 2018 which governs Mutual Legal Assistance Treaties, or MLATs, which cover the relationships between the US and other countries when the US is requesting data that is stored in another jurisdiction and vice versa.

Further reading material:

1. Data Nationalism[56]
2. Googling Freedom[57]
3. Free Speech - Anupam Chander * & Uyên P. Lê **100 Iowa L. Rev. 501 (2015)[58]
4. White paper on the CLOUD act, which focuses on responding to international processes for access to data.[59]

[56] https://law.emory.edu/elj/content/volume-64/issue-3/articles/data-nationalism.html
[57] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1616313
[58] https://ilr.law.uiowa.edu/print/volume-100-issue-2/free-speech/
[59] https://www.justice.gov/opa/press-release/file/1153446/download

INDIA

Prevailing laws and time of introduction

1. Section 66A of the Information Technology Act, 2000:

   Section 66A of the IT Act 2000, criminalised sending "grossly offensive" information, or information which the person sending it knows to be false, but still sends it "for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will". It also criminalised messages sent "for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages"[60].

   Section 66A of the IT Act 2000 was added to the Act through amendments in 2008.

2. Section 69A of the Information Technology Act, 2000:

   Under Section 69A of the Information Technology Act, 2000[61] (IT Act), the central government has the powers to direct the blocking of public access to any online information. The access can be blocked when the central government is satisfied that blocking access is "necessary or expedient" to do in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States, or public order or for preventing incitement to the commission of any cognizable offence relating to above.

   The process for the blocking under Section 69A of IT Act is governed by Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (IT Rules 2009)[62]. Failure to comply will lead to intermediaries be penalised with an imprisonment for a term which may extend to seven years and fine.

3. Section 79 of the Information Technology Act, 2000:

   Section 79 of the IT Act immunes intermediaries from liability for hosting illegal content posted by third parties subject to certain conditions provided the intermediaries have taken due diligence in ensuring the unlawful content has been taken down. The process for takedown is governed by the Information Technology (Intermediaries Guidelines) Rules, 2011 (IT Rules 2011).

   The Government released the Draft Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 and is currently deliberating on the same.[63] The draft rules have

[60] https://www.thehindu.com/news/national/all-you-need-to-know-about-section-66a-of-the-it-act/article10773220.ece
[61] https://indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf
[62] https://meity.gov.in/sites/upload_files/dit/files/Information%20Technology%20(%20Procedure%20and%20safeguards%20for%20blocking%20for%20access%20of%20information%20by%20public)%20Rules,%202009.pdf
[63] https://inc42.com/resources/decrypting-the-encryption-traceability-conundrum/

introduced a new category of information, i.e., content which threatens 'public health or safety' and requires it to be taken down. It also requires intermediaries having over 5 million users to ensure local presence in India with a permanent registered office[64].

Process of legislation, consultation, and implementation timeline

Sections 66A and 69A in addition to other sections were added to the IT Act 2000 through Information Technology (Amendment) Act, 2008 while amendments were also made to Section 79 of the IT Act. After the 2008 amendment, Section 79 provided safe harbour from liability for any third-party content to a wide range of intermediaries.

The Government released the Draft Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018. The rules have still not been notified.

Views for or against these

1. Section 66A of the Information Technology Act, 2000:

   The constitutionality of Section 66A was challenged in Shreya Singhal v. Union of India[65]. The Petitioners argued that Section 66A was vague, had a chilling effect on the right to freedom of expression guaranteed under Article 19 of the Constitution of India and also fell outside the reasonable exceptions to the right.

   The Supreme Court, in Shreya Singhal v. Union of India[66], struck down Section 66A of the IT Act in its entirety holding that it was unconstitutional.[67] The Court said that the Section did not fall within any reasonable exceptions to the exercise of the right to freedom of expression.

   There have been media reports of police continuing to register cases under Section 66A of the IT Act[68]. In January 2020, police officers, who registered an FIR under section 66A, were imposed a cost of INR 10,000/- each by the Karnataka High Court, asked to tender unconditional apologies and submit personal affidavits promising the mistake will not repeat[69].

   The judge said, "This is a case in which police have initiated criminal proceedings invoking provisions of law which is not in statute book… This is nothing but a clear abuse of process of law and harassment to the citizen".[70]

2. Section 69A of the Information Technology Act, 2000:

64 https://inc42.com/features/the-proposed-intermediary-guidelines-impact-indias-tech-startups/
65 https://indiankanoon.org/doc/110813550/
66 https://indi nkanoon.org/doc/110813550/
67 Shreya Singhal v. Union of India, (2015) 5 SCC 1
68 https://indianexpress.com/article/opinion/columns/section-66a-information-technology-act-supreme-court-shreya-singhal-judgment-5599263/
69 https://thewire.in/law/karnataka-hc-section-66a-it-act
70 https://thewire.in/law/karnataka-hc-section-66a-it-act

Government issued letters on August 16, 2017, and August 24, 2017 directing Twitter to block Twitter handles, hashtags, and individual tweets mentioned in those letters[71]. Internet Freedom Foundation said that there was a need for "urgent focus" on the "problematic process" of website blocking. It said that the letters were "vague and illegal" as they provided no notice or hearing, no reasons for directions to block access, and were non transparent[72].

In response to a RTI request filed by SFLC.in, the Ministry of Electronics and Information Technology (MeitY) disclosed on 31 December 2018 that they have blocked access to 14221 websites/URLs between 2010 to 2018 using powers provided under Section 69A of the IT Act, 2000.[73]

The Supreme Court upheld the constitutionality of Section 69A in the Shreya Singhal case[74] observing that the safeguards provided in the legislation were proportionate and enough to prevent any arbitrary decisions from being made.

3. Section 79 of the Information Technology Act, 2000:

Internet Democracy Project said that the Information Technology (Intermediaries guidelines) Rules, 2011, governing process for takedown under Section 79, constituted "an important and worrying move towards the privatisation of censorship in India"[75].

The Supreme Court in Shreya Singhal Case[76] upheld the constitutionality of Section 79 adding that only a court order or a government direction to the intermediary can amount to the intermediary having 'actual knowledge' of the unlawful content.

Indus Law said regarding the use of automated tools to identify and remove unlawful content as required by the Draft Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 that "the use of such automated tools may arbitrarily, excessively and disproportionately pre-censor information and content, having a detrimental effect on an individual's right to free speech, defeating the intention behind the Supreme Court's judgment in Shreya Singhal vs. Union of India"[77].

71 https://internetfreedom.in/blocking-orders-to-twitter-illustrate-a-worrying-process-goiblocks/
72 https://internetfreedom.in/blocking-orders-to-twitter-illustrate-a-worrying-process-goiblocks/
73 https://sflc.in/over-14000-websites-blocked-meity#:~:text=Section%2069A%20of%20the%20Information,agency%20of%20government%20or%20intermediary.
74 https://indiankanoon.org/doc/110813550/
75 https://internetdemocracy.in/laws/the-information-technology-amendment-act-2008/section-79-and-the-it-rules/
76 https://indiankanoon.org/doc/110813550/
77 https://www.mondaq.com/india/it-and-internet/783268/the-draft-information-technology-intermediaries-guidelines-amendment-rules-2018

TURKEY

Prevailing laws

Turkey's amendments to the law on internet crimes 2020:

The amendments force social media platforms to open an office or appoint a Turkish citizen as their representative in Turkey to ensure compliance with Turkey's local laws and court decisions[78]. Under the law, the companies will face fines, the blocking of advertisements or bandwidth reductions in case of non-compliance[79].

The law further requires that the servers with Turkish users' data must be stored in Turkey[80].

Process of legislation, consultation, and implementation timeline

The plans to bring new social media regulations were disclosed during a speech by President Erdoğan on 01 July 2020[81]. The bill was submitted before the parliament on 21 July 2020[82] and was passed by the parliament on 29 July 2020[83].

Views for or against these

Ruling party lawmaker Rumeysa Kadak argued that the legislation was needed to combat cyber-crime against women[84]. However, opposition lawmakers criticised the law arguing that it amounts to a limitation on the right to freedom of expression in a country where the media and journalists are under government control and face criminal charges for their work[85]. The opposition called the bill the "censorship law"[86].

Reporters Without Borders (RSF) condemned the bill arguing that the law aims to silence "mounting online criticism". It said that "the government's goal is to control social media, the only remaining refuge for critical journalists in Turkey"[87].

78 https://rsf.org/en/news/turkey-tightens-grip-social-media-platforms
79 https://www.aljazeera.com/news/2020/07/turkey-passes-controversial-bill-tightening-grip-social-media-200729061612677.html
80 https://www.aljazeera.com/news/2020/07/turkey-passes-controversial-bill-tightening-grip-social-media-200729061612677.html
81 https://dokuz8haber.net/english/science-technology/turkey-data-localization-bill-in-aims-of-total-control-over-social-media/
82 https://rsf.org/en/news/turkey-tightens-grip-social-media-platforms
83 https://www.hurriyetdailynews.com/turkish-parliament-passes-law-to-regulate-social-media-content-156957
84 https://gadgets.ndtv.com/social-networking/news/turkey-social-media-law-content-regulation-2270651
85 https://gadgets.ndtv.com/social-networking/news/turkey-social-media-law-content-regulation-2270651
86 https://gadgets.ndtv.com/social-networking/news/turkey-social-media-law-content-regulation-2270651
87 https://rsf.org/en/news/turkey-tightens-grip-social-media-platforms

Amnesty International's Turkey Researcher Andrew Gardner said, "If passed, these amendments would significantly increase the government's powers to censor online content and prosecute social media users. This is a clear violation of the right to freedom of expression online and contravenes international human rights law and standards"[88].

Deputy program director at Human Rights Watch, Tom Porteous said, "If passed, the new law will enable the government to control social media, to get content removed at will, and to arbitrarily target individual users"[89]. He further said that "...this law signals a new dark era of online censorship"[90].

[88] https://www.amnesty.org/en/latest/news/2020/07/turkey-draconian-social-media-law-poses-grave-threat-to-freedom-of-expression/
[89] https://www.hrw.org/news/2020/07/27/turkey-social-media-law-will-increase-censorship
[90] https://www.hrw.org/news/2020/07/27/turkey-social-media-law-will-increase-censorship

FRANCE

Prevailing laws

The Law on Countering Online Hatred, or bill 'Loi Avia', was introduced to fight different forms of online hate speech, terrorist speech and child pornography. The Bill instructed that after a user is flagged, within 24 hours, platforms should take down certain types of illegal content. However, if companies failed to fulfil, then they would pay both administrative and criminal high-dollar fines[91]. The bill was said to be aimed to strengthen the contribution of digital operators to combat hateful online content[92].

"Our message must be clear: what isn't tolerated in public spaces mustn't either on the internet, no more than we can let racist, anti-Semitic, LGBT-phobic, sexist comments proliferate online with impunity," Ms. Avia, the sponsor of the bill, said in her statement[93].

Process of legislation, consultation, and implementation timeline

Loi Avia law was drafted by Laetitia Avia in March 2019, for regulating hateful content on websites and social media. The Bill was passed by the National Assembly in July 2019, to limit hateful content online. These rules may apply to all offensive content, not just extremism. There is a fine of 4% of global turnover for those who fail to comply.[94]

However, the majority of the law was declared unconstitutional by the French Constitutional Court, rendering key provisions of the law invalid.

Views for or against these

The French Constitutional Council declared the main provisions of the Loi Avia law unconstitutional on 18 June, 2020. The European Commission, digital rights organisations and LBGTQI+, feminist and antiracist organisations opposed to the main measures throughout the legislative process. As soon as it was adopted, the French Senate brought the law before the Constitutional Council[95].

[91] https://www.lawfareblog.com/whats-going-frances-online-hate-speech-law
[92] http://www.assemblee-nationale.fr/dyn/actualites-accueil-hub/ppl-visant-a-lutter-contre-les-contenus-haineux-sur-internet-adoption-en-lecture-definitive
[93] https://www.nytimes.com/2020/06/18/world/europe/france-internet-hate-speech-regulation.html
[94] https://www.article19.org/resources/france-the-online-hate-speech-law-is-a-serious-setback-for-freedom-of-expression/
[95] https://edri.org/french-avia-law-declared-unconstitutional-what-does-this-teach-us-at-eu-level/

"The Avia Bill would have forced social media platforms to single-handedly make an immediate determination as to the legal nature of the content," said Thomas Vandenabeele and Pierre Ciric, president and vice president, respectively, at FABA. "We are pleased that the French Supreme Court adopted the position expressed in our joint June 1 amicus brief, whereby those take down timing requirements will cause over-censorship of perfectly legal speech, and are therefore unconstitutional."[96]

[96] https://www.eff.org/press/releases/victory-french-high-court-rules-most-hate-speech-bill-would-undermine-free-expression