

THE ONLINE REGULATION SERIES

| EXECUTIVE SUMMARY



BACKGROUND TO TECH AGAINST TERRORISM

Tech Against Terrorism is a public-private partnership supported by the United Nations Counter-Terrorism Executive Directorate (UN CTED). Tech Against Terrorism was launched in April 2017 at the United Nations Headquarters in New York and is implemented by the Online Harms Foundation. As a public-private partnership, the initiative has been supported by the Global Internet Forum to Counter Terrorism (GIFCT) and the governments of UK, Spain, Switzerland, the Republic of Korea, and Canada.

Our research shows that terrorist groups consistently exploit smaller tech platforms when disseminating propaganda. At Tech Against Terrorism, our mission is to support smaller tech companies in tackling this threat whilst respecting human rights, and to provide companies with practical tools to facilitate this process.

We strive to constantly provide tech companies with all the resources they need to counter terrorist use of the internet, and inscribe their efforts into the rule of law.

Our core aim at Tech Against Terrorism is to support the tech industry in building capacity to tackle the use of the internet for terrorist purposes whilst respecting human rights. We work with all types of tech companies, such as social media, pasting, file-storage, messaging, fintech platforms, and web infrastructure providers. Our core mission is providing the global tech industry with the tools needed to effectively tackle terrorist activity on their platforms.


Analysis of the threat and outreach

We carry out extensive open-source intelligence analysis to identify platforms at risk and build constructive working relationships with the tech sector, as well as facilitating public-private cooperation.

Knowledge sharing and best practice

We facilitate intra-industry and cross-sector support mechanisms through online tools, guides, and practical datasets to support policy and content moderation decisions. Here we work closely with the GIFCT in organising global workshops and webinars. We also support companies through our [membership and mentorship programmes](#). In July 2021, we launched an updated version of the [Knowledge Sharing Platform](#), which collates tools and resources to support tech companies in tackling terrorist use of the internet.

The Online Regulation Series falls within the scope of our knowledge-sharing activities, as we strive to constantly provide tech companies with all the resources they need to counter terrorist use of the internet, and inscribe their efforts into the rule of law.



Our mission is to support smaller tech companies in tackling this threat whilst respecting human rights, and to provide companies with practical tools to facilitate this process.

Tech development and operational support

We provide technical support and resources for tech companies to improve their counterterrorism mechanisms, for example through data science or development support. Examples of past work within this workstream includes [our work with Jihadology.net](#) and our current work on the [Terrorist Content Analytics Platform](#).

For more information on our organisation and how we strive to support the global tech sector and in particular smaller platforms, please visit www.techgainstterrorism.org

BACKGROUND TO THE ONLINE REGULATION SERIES

Since 2017 and the passing of the Germany's Network Enforcement Act (NetzDg), there have been many developments in the regulation of online speech and content, in particular in how we counter the spread of terrorist content online. Several new laws have been passed or proposed in jurisdictions such as Australia, Brazil, France, India, the United Kingdom, Morocco, Pakistan, Singapore, Turkey, and the European Union.

Facing this fast-changing landscape, Tech Against Terrorism decided to provide smaller tech companies with a comprehensive overview of global online regulation. We reviewed over 60 pieces of legislation, proposals, and guidelines that aim to regulate the online sphere, and analysed over 100 data sources and civil society reports.

This effort culminated in the Online Regulation Series, where over the course of six weeks, in October and November 2020, Tech Against Terrorism focused its outreach and knowledge-sharing efforts on providing our stakeholders with an update on the state of global online regulation.

We focused on three questions to improve our understanding of online regulation:

- What is the global state of play with regard to online regulation?
- What are some of the recent proposals that aim to regulate online content?
- What are the implications for tech platforms?

Throughout the series, we published 20 blogposts on our website, sharing relevant resources and insights on Twitter as well. The series covered:

- 17 jurisdiction-specific blogposts divided by region: Asia-Pacific, North America, Europe, MENA and Sub-Saharan Africa, South America.
- 3 additional blogposts on tech sector initiatives and expert perspectives to complement our regional focus.

The Online Regulation Series concluded with a webinar entitled The State of Global Online Regulation, bringing together analysis from tech policy and digital rights experts on the key global regulations that are shaping online speech around the world.

Editorial note

The analysis included in this report is based on the blogposts we published on [Tech Against Terrorism's website](#) in October – November 2020, and were updated to reflect changes in the online regulation landscape that took place between October 2020 and June 2021. As the state of global online regulation continues to change, Tech Against Terrorism will strive to provide regular updates on the implications for tech companies, and their efforts in countering terrorist use of the internet whilst respecting human rights.

If you are aware of something that should be included or updated, please get in touch with us at contact@techagainstterrorism.org

THE ONLINE REGULATION SERIES | OVERVIEW

When conducting our research for the Online Regulation Series, we identified three separate regulatory aims used by governments to justify regulating online content:

1. Countering terrorist and violent extremist content, or “harmful” content

These regulations target terrorist use of the internet by compelling tech companies to rapidly remove terrorist and violent extremist content from their platforms, often including short removal deadlines (from 1 to 36 hours) and heavy fines in cases of non-compliance. The German NetzDG (2017) was the first of such regulations and was followed by similar moves in other jurisdictions, including [France](#), [the UK](#), [the EU](#), and more recently [Canada](#). Some of these laws also target “harmful” online content more generally, which can span anything from illegal content and incitement to hatred to suicide-promoting content.

2. Countering the spread of misinformation and disinformation

In some countries, policymakers have focused regulatory proposals on misinformation and disinformation. These proposals often include the power for governments to issue removal or correction orders to platforms, as is the case in [Singapore](#); or the power for platforms to trace the originator of a message, as has been introduced in [India](#) and discussed in [Brazil](#).

3. Adapting to the digital space

These laws are motivated by the idea that existing regulations are no longer adapted to the reality and risks of today's digital world. For instance, the [EU's Digital Services Act](#) has been explicitly framed as a response to how digital changes impact our lives. [Canada's Communications Future: Time to Act](#) report also outlined recommendations for a thorough change to the country's regulation of online platforms and content.



TECH AGAINST TERRORISM | RECOMMENDATIONS FOR GOVERNMENTS

Based on our analysis of existing and upcoming regulations aimed at countering terrorist and other harmful content online, we call on governments to:

1. Safeguard the rule of law

Avoid measures that risk undermining the rule of law and due process. In particular governments should:

- Ensure that definitions of key terms, such as terrorist content, are clear, practical, and have a basis in existing legal frameworks. Governments should also avoid introducing regulation that depends on subjective interpretation of harm, as this is often difficult for tech companies to operationalise at scale without negatively impacting freedom of expression.
- Use legal powers to promote the rule of law through more comprehensive terrorism designation lists (in particular of far-right terrorist groups) to help increase definitional clarity around terms such as terrorism.
- Refrain from making content that is legal online, illegal offline. There should be a clear legal basis to remove online content, including via existing counterterrorism laws and terrorism designation lists, or via existing limitations to freedom of expression.
- Refrain from introducing provisions that infringe on existing due process with regards to limitations to freedom of expression. In line with international human rights standards, limits to freedom of expression should be adjudicated by an independent judiciary body and not delegated to a private entity.
- Provide legal certainty to tech platforms by clarifying how regulatory compliance will be assessed, and by providing guidance on the specific steps companies should take to comply with legal requirements

2. Consider the capacity and resources of smaller platforms and respect the principles of proportional regulations and equality before public charges.

- Ensure obligations for tech companies are proportionate according to size and capacity, and avoid harming competition and innovation by limiting financial penalties for smaller or micro-platforms.
- Increase support for the tech sector, particularly for smaller platforms, in countering terrorist and violent extremist use of the internet, for example through public-private partnership endeavours, and digital literacy programmes. We know from experience that smaller platforms are very receptive to mentoring and any opportunity to learn how to minimise the terrorist and violent extremist threat online. If governments wish to tackle online harms – including terrorist content – effectively, we recommend they invest in similar programmes to support smaller platforms.

3. Provide clarity regarding the safeguards and redress mechanisms

We call on governments to:

- Clarify what safeguards are in place to avoid removal of legal content.
- Clarify what redress mechanisms are in place in case of erroneous removal, in particular regarding content removal following removal requests from a country's judicial or governmental authority.

4. Ensure that human rights – in particular freedom of expression – are safeguarded when implementing online regulations

We call on governments to:

- Provide information on the steps taken by the relevant implementing and supervising authority to ensure that their mandates are carried out with the fullest respect for freedom of expression and human rights, and that they are:
 - Fully aware of risks to human rights and freedom of expression associated with the measures they implement, for example removal orders and requirement to remove content within a specified timeframe.
 - Uniform in their judgement and do not politicise removal orders.
 - Consistent and accurate in issuing penalties to companies.
 - Disincentivised from over-zealous content removal.
 - Held accountable for assessments and judgements made in implementing this regulation.

5. Produce transparency reports on their engagement with tech companies for counterterrorism purposes, in line with the Tech Against Terrorism Guidelines¹

1. Forthcoming 2021

Some of the online regulations that have been passed, or are being discussed at the time of writing, include provisions that Tech Against Terrorism strongly advises against. For governments that decide to pursue these provisions, we recommend the following:

Tech Against Terrorism argues that adjudication of the legality or harmfulness of content should be the role of governments, not tech platforms. For regulations that place the onus of adjudication on tech companies, we recommend governments to:

- Avoid introducing measures that do not allow sufficient time for platforms to adequately assess the legality of content, and provide the necessary practical support for platforms to correctly assess content.

Tech Against Terrorism strongly advises against placing liability for user-generated content on tech companies or their employees. If governments decide to pursue these liability regimes, we urge them to:

- Clarify under what exact circumstances a company's legal representative may be held liable for their company's lack of compliance with the regulation.

Tech Against Terrorism advises against mandating short removal deadlines for terrorist or harmful content, as these deadlines lack consideration for platforms' capacities and encourage overzealous removal of content. For governments that decide to mandate short removal deadlines, we call on them to:

- Consider the increase in resources (financial, human, and technical) these provisions require and small platforms' capacity.

We call on governments to take a holistic approach to countering terrorism and violence extremism. Beyond regulating terrorist and harmful content, governments should ensure that regulatory frameworks address the root causes of radicalisation and hold individuals that engage in terrorist and violent extremism activities accountable, in full respect for international human rights standards.

THE STATE OF ONLINE REGULATION | TECH AGAINST TERRORISM'S CONCERNS

Based on our analysis of online regulation globally and the regulatory key trends we identified, we develop in this section on our main concerns with the new wave of online regulation.

1. Lack of consideration for smaller platforms

Research conducted by Tech Against Terrorism has shown that smaller and newer tech companies are the most at risk of exploitation by terrorists and violent extremists. Most of the small platforms Tech Against Terrorism regularly engages with show willingness in tackling this threat but lack the human, technical, and financial resources required.

Despite this observation, most of the online regulations covered in this handbook apply indiscriminately to platforms of all sizes and resources. This means that small and micro-sized platforms are expected to comply with the same stringent legal requirements as larger and long-established platforms would do.

Such unrealistic expectations of compliance risk penalising small platforms with heavy fines and leaving them behind, instead of offering them the support needed to counter the threat. This also bears the risk of reduced competition in the tech sector if smaller platforms are not able to catch up or are financially compromised by the fines.

Based on our analysis of the regulations covered in this Handbook, we assess that laws in the following jurisdictions do not sufficiently account for smaller platform challenges:



2. Recognising that not all platforms are equal in their capacity to comply

Concerns regarding disparities in resources and how these impact a platform's capacity to comply with legal requirements were also raised by the French Constitutional Council in its censuring of the so-called “CyberHate” law. The Council stressed that some of the provisions in the original version law were impossible to satisfy and broke the principle of equality before public charges – which underlines that legal and administrative requirements should not cause heavy or particular burdens for those having to comply.

With this ruling, the Council recognised that platforms' resources can significantly impede their capacity to comply with legal requirements, and that requirements which are highly resource-demanding should not be included in online regulation.

Tech Against Terrorism urges policymakers to consider the diversity of platforms to ensure that the most demanding legal requirements consider platforms' sizes. In line with this, smaller tech companies should be consulted when new regulations are being drafted and discussed.

Policymakers should also support capacity-building and knowledge-sharing activities to strengthen smaller platforms' capacity to respond to terrorist and violent extremist use of the internet, and to comply with legal requirements.

Tech Against Terrorism works to ensure that smaller platforms are considered and heard. We regularly raise the importance of acknowledging that smaller platforms need additional support, rather than heavy fines, in our policy responses. To do so, we regularly consult with smaller tech companies engaged in our Mentorship and Membership programmes.

3. Lack of definitional clarity and risks for freedom of expression

Many of the regulations analysed for the 2020 Online Regulations Series are impractically broad in their definition of harmful content and circular in their explanation of terrorist content – they rarely indicate how to implement the definition of terrorism or harmful content. This presents serious risks for freedom of expression, as these regulations could be used to pressure tech companies to remove legal or non-violent speech.

With such vague definitions of “legal but harmful” content, countries are introducing mechanisms that risk undermining the rule of law. In a democracy, we cannot make speech that is legal offline illegal in the online space, and private organisations should not be pressured to remove legal content.

4. Online regulation and the risks of “censorship creep”

Danielle Citron (Professor at the University of Virginia School of Law and expert on information privacy and free expression), in her criticisms of the EU regulation of online content and EU Internet Referral Units, has expressed concerns with the risks of “Censorship Creep”: “whereby a wide array of protected speech, including political criticism and newsworthy content, may end up being removed from online platforms on a global scale.”

Citron’s criticisms focus on “definitional ambiguity” around what constitutes harmful content, namely “hateful conduct” and “violent extremism material”, which can be abused to target legitimate speech and political dissent. Combined with pressure on platforms to (rapidly) remove harmful content, this risks the over-removal of content which could have major repercussions on freedom of expression online.

Tech Against Terrorism cautions against vague and circular definitions of terrorist or harmful content in laws, and against governments demanding platforms to remove content that is not clearly prohibited by law. We call on governments to apply the same level of detail and clarity in their legislation that governments expect of tech companies in publishing clear terms of service: clearly delineated and defined prohibitions, that are inscribed in the rule of law by reflecting behaviours and content that is illegal offline, instead of creating a differentiated regime for the online space.



KEY TRENDS |

Overview of jurisdictions aligning with the key trends identified by Tech Against Terrorism

In this table, “Not Applicable” refers to the absence of a passed legislation aimed at regulating terrorist or harmful content online. These jurisdictions are considered in this Handbook due to regulatory discussions and legislative proposals, however, in the absence of a published draft bill, we refrained from classifying them in the below table.

Singapore and Jordan stand out in this table by being the only countries that do not follow any of the key trends Tech Against Terrorism identified. Please see our commentaries of each country to learn more about our analysis and assessments of online regulations in Singapore and Jordan.

KEY TRENDS IN ONLINE REGULATION



Fully in line with the key trends identified



Partially in line with the key trends identified

JURISDICTIONS



Different requirements depending on platform size

Short removal deadlines

Increased reliance on automated moderation

Outsourcing legal adjudication

Platform employees liability or demanding a focal point

Mandating a local presence

Mandating transparency and accountability

Not applicable.

Not applicable.

The Cybercrime Law (2019) also applies online messaging services.

Not applicable.

Not applicable.

The Protection of Online Falsehoods and Manipulation Bill (2019), applies to all type of online platforms including encrypted messaging services.

Not applicable.

1. Short removal deadlines

Requiring smaller tech companies to remove content within short timeframes is a common yet unrealistic expectation being placed on smaller companies in various jurisdictions. A one-hour deadline, for example, would likely require constant monitoring from tech platforms to ensure compliance. It is a difficult endeavour for most medium and large tech platforms and virtually impossible for smaller platforms.

The pressure put on tech companies to quickly respond to alerted content, and to proactively remove or prevent upload of content risks freedom of expression, as tech platforms will not have the time necessary to properly adjudicate on content legality. Instead, there is the risk of an overzealous removal of content, with platforms indiscriminately taking down all content reported for illegality or violation of the content standards, before properly reviewing a report.

The EU Regulation 2021/784 on Addressing the dissemination of terrorist content online, which mandates a one-hour removal for terrorist content for all platforms, has been amended in its final version to acknowledge that not all platforms have the same resources and capacities. Tech companies that cannot comply with a removal order will have to inform the competent authority of this without “undue delay”, and will be excused if they can provide “objectively justifiable technical or operational reasons” as to why they cannot comply. However, this amendment still requires smaller tech platforms to rapidly acknowledge terrorist content alerts to avoid penalties, which does not resolve the issue of platforms having to be almost constantly monitoring alerts received.

In our assessment, the laws discussed or passed in the following jurisdictions align with this trend:



2. Increased reliance on automated moderation

For most platforms, stringent online regulation mandating content to be removed will require a significant increase in resources dedicated to content moderation. For the platforms that have the necessary technical resources, this will most likely mean an increased reliance on automated content moderation tools.

Whilst automated content moderation has its benefits, current solutions are not nuanced enough to correctly assess whether certain pieces of content are in fact terrorist material or harmful. Most automated solutions notably lack the capacity to comprehend context (for example, whether content is journalistic, or shared in order to criticise a specific position) and require human overview to avoid the excessive takedown of content. An increased reliance on automated moderation solutions raises the risk of false positives in taking down content that is legal, and raises questions about accountability in removal decisions. Our greatest concern is the risk that content denouncing human rights violations, including journalistic content that can serve as evidence of such violations, could be automatically removed, more so at a time where constitutional guarantees are weakened in certain countries.

Covid-19 and increased reliance on automated tools

YouTube's increased reliance on automated tools in 2020 demonstrates the risks of over-removing non-violating content. Due to the Covid-19 pandemic and ensuing lockdown measures, YouTube and many other large tech companies increased their use of automated moderation tools considerably. This resulted in more non-violating content being actioned, with the number of user appeals doubling and the number of reinstated content quadrupling.

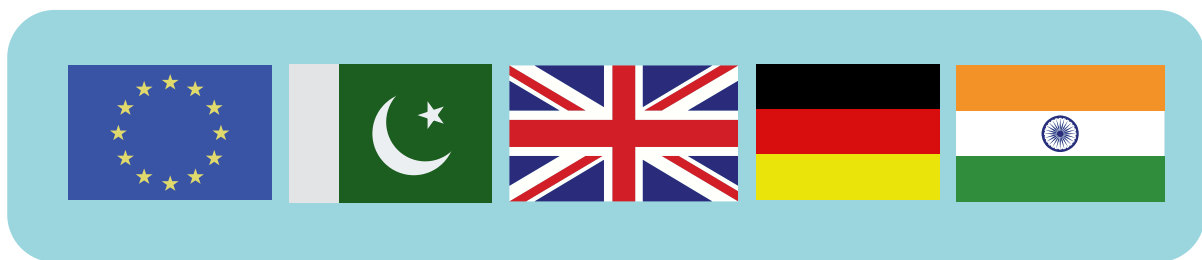
The use of automated solutions to detect and remove terrorist content is also not straightforward. These solutions cannot replace consensus on what constitutes a terrorist organisation, and need to be informed by responsible terrorist designations from governments and intergovernmental organisations. It becomes even more complicated when harmful content originates from users that are not officially affiliated with terrorism or violent extremism, or when the content exists in a legal “grey area”.

3. Leaving smaller platforms behind

Smaller platforms lack the resources necessary to deploy automated moderation tools at scale, which presents a dual risk. On the one hand, smaller platforms risk being left behind and penalised for not being able to comply with provisions where automated technology might be necessary. On the other hand, there is a risk of an uniformisation of the online moderation landscape and the expansion of what Evelyn Douek has labelled “content cartels”, with smaller platforms turning to larger ones for content moderation tools (buying their services or replicating their moderation practices).

Tech Against Terrorism calls for greater support for smaller tech companies, in particular via the development of data-driven moderation tools built with considerations for human rights and transparency on counterterrorism efforts, such as the Terrorist Content Analytics Platform. The development of these tools should be adapted to the needs of smaller platforms and respect their autonomy. Governments and larger platforms should support the development of these tools and facilitate their accessibility to smaller platforms, in respect of accountability and transparency.

In our assessment, the laws discussed or passed in the following jurisdictions align with this trend:



4. Delegation of legal adjudication to tech companies

One key emerging trend is regulation introducing mechanisms that outsource adjudication of illegality from courts and democratically-accountable institutions to private and unaccountable tech companies. This poses severe risks to the rule of law, not to mention that platforms, particularly smaller ones, do not have the legal expertise to adjudicate accurately, especially when they are facing time pressure such as removal deadlines.

International human rights standards underline that limits to freedom of expression should be decided by an independent judiciary body. However, by mandating tech companies to remove content at scale, many online regulations meant to counter online harms instead shift the responsibility of deciding what is harmful and/or illegal content to private tech companies. This is exemplified by the criticism made by David Kaye on the French “cyberhate law”. The law itself did not create a new set of harms (it was based on restrictions to freedom of expression existing in French law); nevertheless Kaye underlined that “censorship measures”, such as those implied by the duty to remove terrorist and hateful content, should not be delegated to private entities.

Tech Against Terrorism calls on governments to provide support mechanisms for tech companies to address terrorist and violent extremist content, and to provide clear legal bases to counter other online harms:

- With regard to terrorist content, we believe that designating terrorist groups in a responsible and accurate manner – whilst respecting human rights and freedom of expression – is an important tool that helps tech companies take appropriate action, whilst inscribing such action in the rule of law.
- Platforms should also be given sufficient time to properly assess the legality and harmfulness of content, and should be practically supported in this endeavour.

All laws that mandate platforms to remove flagged content within a short timeframe, or proactively remove certain types of content, are in effect placing the onus of adjudication of illegality on tech platforms. In our assessment, this includes:



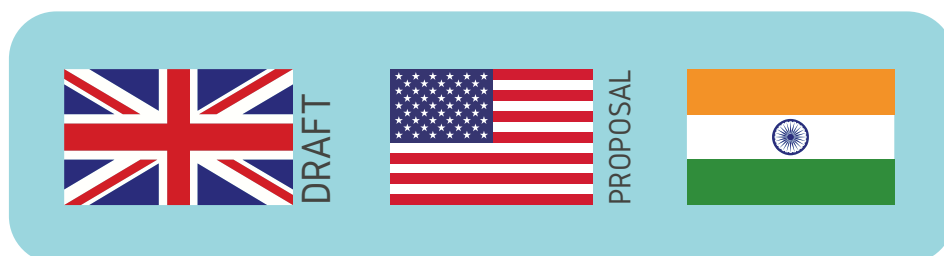
5. Holding platforms liable for user-generated content

The Online Safety Bill draft in the UK, and proposals to reform Section 230 in the US, suggest that platforms are increasingly likely to be held liable for user-generated content. Tech Against Terrorism cautions against holding platforms legally responsible for user content as this would heighten the risks for freedom of expression.

As the [Global Network Initiative](#) has warned, imposing liability on tech companies is likely to lead to the over-removal of content rather than tackling the underlying drivers of terrorist content on the internet.

In addition, many platforms exist only as hosts or mere conduits. Forcing them to undertake moderation and content checks would open them up to potential liability for third party content they have little to no oversight over.

In our assessment, the laws discussed or passed in the following jurisdictions align with this trend:



6. Placing legal liability on platform employees

Certain countries, including [India](#) and [Pakistan](#), require tech companies to designate focal points for handling reports of violating content and user complaints. The [UK draft Online Safety Bill](#) takes this a step further by including a provision on “Senior Manager liability”, which opens the way for senior managers to be held accountable for failing “to take all reasonable steps to prevent [an] offence being committed.”

In some instances, employees of tech platforms have already been held legally liable for their companies' non-compliance with government requests. This goes beyond the usual fines that platforms can face for not abiding with regulations or government requests, with employees jailed or threatened with imprisonment in order to pressure platforms to comply.

Tech Against Terrorism warns against such provisions, which risk criminalising individuals engaged in countering the diffusion of terrorist and violent extremist material, rather than on those responsible for diffusing such content. In non-democratic countries with broad definitions of terrorist and harmful content, this further bears the risks of platforms and their employees becoming the targets of crackdowns on political dissent and non-violent speech.

Instead of holding platforms' employees responsible for terrorist content, there is a need to address the root causes of radicalisation and terrorism, and ensure that counterterrorism frameworks can be used to hold terrorists accountable for their online actions.

In our assessment, the laws discussed or passed in the following jurisdictions align with this trend:



LIABILITY
REGIME
CLEAR



LIABILITY
REGIME
UNCLEAR

7. Local physical presence requirement

A number of regulations passed in 2020 and early 2021 require tech companies to establish a presence within the remit of a territorial jurisdiction – whether that be by appointing a focal point or nominating a legal representative or by establishing a physical office or by a data centre within the country.

Complying with such requirements represents a significant challenge for smaller tech companies, especially as they are replicated throughout multiple countries. Potentially, small and micro-size platforms operated by 1-15 people will have to ensure a legal or physical presence in several countries if they wish to continue to operate there, a requirement that most smaller platforms will not be able to comply with due to the financial cost associated with it and will, as a result, be forced to stop their services in certain countries. Ultimately this is a threat to diversity and innovation in the tech sector.

Depending on the legislation and specific provisions, only larger tech companies have to comply with such requirements. However, these still present increased risks of governmental control over tech companies, such as via the legal liability of a platform's point of contact or user data, as is the case with regulations mandating tech companies to set up data centres within a specific territorial jurisdiction. This risks country's authorities having facilitated access to user data by diminishing the need to send complicated mutual legal assistance treaty requests across jurisdictions to access user data. Law enforcement and judicial authorities, including in non-democratic countries, can thus use such data centre requirements to facilitate information and content removal requests at the expense of users' privacy rights.

Given the global nature of the online space, Tech Against Terrorism warns against the multiplication of legal requirements forcing platforms to have a physical or legal presence in a country. Replicated across jurisdictions, this creates a multiplicity of impossible legal requirements.

In our assessment, the laws discussed or passed in the following jurisdictions align with this trend:



8. Mandating different requirements depending on platforms size

Some online regulations acknowledge that smaller platforms should not be expected to comply with the same level of demanding requirements than larger ones, and include provisions that only larger platforms need to comply with.

India and Turkey, for instance, include specific provisions for large platforms to comply with. However, the definitions or criteria used to define what constitutes a “large” platform are not always clear in these laws, and mandates further clarification from authorities in charge of overseeing the implementation of the laws. The Bill on Separatism in France also requires platforms over a certain user-base size in France to comply with specific requirements on countering the spread of “illegal and hateful content”, including a review of their algorithms.

Tech Against Terrorism welcomes the consideration given to smaller platforms in certain laws and amendments. However, we recommend policymakers to clarify in the regulatory frameworks the categorisation of platform size and to consider not only the user-base but also platform resources (financial, human and technical) in their categorisation process. This would ensure that platforms that lack resources are not misclassified.

In our assessment, the laws discussed or passed in the following jurisdictions align with this trend:



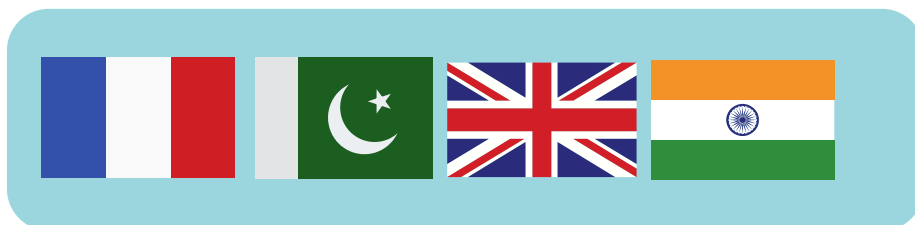
9. Transparency reporting expectations and requirements

Commendably the majority of online regulations introduced in 2019-2021 include provisions that seek to increase transparency and accountability from the tech sector.

Mandating detailed content standards

Some of the regulations analysed in this Handbook state that tech platforms should have clear and detailed content standards for users to understand what is allowed or not on the platform. In certain instances, regulations outline what should be included in the content standards, and mandate or recommend platforms to explicitly prohibit the types of content that are covered in the regulation itself.

The [EU Regulation 2021/784](#) states that platforms should have a clear prohibition of terrorist content in their community guidelines, whereas the EU Digital Service Act and the UK Guidance for Video Sharing Platforms outline what platforms should raise in their content standards. The [2020 Rules in Pakistan](#) and the [2021 Guidelines in India](#) both go a step further and require platforms to add to their content standards the list of content prohibited in the laws. In our assessment, the laws discussed or passed in the following jurisdictions align with this trend:



Increasing transparency reporting

On transparency, the proposed Online Safety Bill in the UK demands that platforms publish transparency reports on their compliance with the Bill. The EU Regulation 2021/784 on Addressing the dissemination of terrorist content online, will require tech companies to publish transparency reports on their efforts to comply with the regulation, and outlines metrics for transparency reporting by governments and competent authorities. France's "cyberhate" law also calls for increased transparency from both the tech and government sectors, and requires the country's audio-visual authority to publish an annual report on the enforcement of the law.

Tech Against Terrorism connects industry, government, and civil society to prevent the terrorist use of the internet whilst respecting human rights.

A project supported by UN CTED under mandate of the United Nations Security Council Counter-Terrorism Committee

Find out more at:

techagainstterrorism.org

[@techvsterrorism](https://twitter.com/techvsterrorism)

contact@techagainstterrorism.org

