

Estonia

C Violations of User Rights

Freedom of expression online is protected by the constitution and by the country's obligations as an EU member state. However, two journalists were personally held liable for defamation in a novel civil case during the coverage period. Anonymity is unrestricted, as is the use of encryption. The COVID-19 pandemic did not drive an increase in state surveillance.

C1 1.00-6.00 pts 0-6 pts

Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?	6.006 6.006
--	----------------

All citizens have the constitutional rights to freely obtain information and to freely disseminate ideas, beliefs, and facts.⁷⁶ There are no obstacles to people exercising their right to freedom of expression online.

The judiciary in Estonia is independent, and there have not been any instances of political interference with the judiciary. According to a 2019 survey, 55 percent of Estonians trust the judiciary.⁷⁷

Protections for journalists, which include the right to the confidentiality of sources, are strong.⁷⁸

The Ministry of Justice plans to amend the Public Sector Information Act⁷⁹ by July 2021 in line with the EU's revised Public Sector Information Directive,⁸⁰ which governs public access to state data.

C2 1.00-4.00 pts 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities?	3.003 4.004
---	-------------

On paper, there are few limits on freedom of expression online. Speech that publicly incites hatred, violence, or discrimination on the basis of nationality, race, color, gender, language, origin, religion, sexual orientation, political opinion, or financial or social status is punishable by a fine of up to 3,200 euros (\$3,500) under the penal code.⁸¹ Such speech is also punishable by up to three years in prison if it leads to the “death of a person or results in damage to health or other serious consequences.”

Defamation was decriminalized in 2002.⁸² Civil defamation cases can be brought under the Law of Obligations Act,⁸³ though cases are rare and damages are usually moderate (see C3).⁸⁴

In October 2017, the Court of Justice of the European Union (CJEU) sought to clarify EU law in a case on internet jurisdiction at the request of the Estonian Supreme Court.⁸⁵ The ruling considered whether a defamation case can be brought before a court in Estonia if the company affected is based domestically, despite the infringing content being published on a Swedish website. The CJEU clarified that the party affected may sue in the country where its center of interest resides, but noted that it is not possible to bring cases in any country where the online information is accessible.⁸⁶

C3 1.00-6.00 pts0-6 pts

Are individuals penalized for online activities?	6.006 6.006
--	-------------

There were no criminal prosecutions or detentions for online activities during the coverage period.⁸⁷

In November 2018, a court in Tallinn held *Postimees* and two of its reporters liable for a defamatory story about businessman Margo Tomingas (see B2). The two reporters were each ordered to pay 500 euros (\$566) in damages, while *Postimees* was ordered to pay a further 3,000 euros (\$3,400). The defendants also had to cover Tomingas's legal costs. The verdict was upheld in November 2019.⁸⁸ The case made headlines because the two reporters were held personally liable. However, the *Postimees* legal team declined to appeal the decision because, in its view, no precedent had been set in this regard.⁸⁹ Nevertheless, the state Data Protection Inspectorate (AKI), commenting on the case, reminded "all authors operating in the public sphere," including social media users, to abide by journalistic principles "when publishing current, social or other public interest texts."⁹⁰

C4 1.00-4.00 pts0-4 pts

Does the government place restrictions on anonymous communication or encryption?	4.004 4.004
--	-------------

There are no governmental restrictions on anonymous communication or encryption. There are no SIM card registration requirements.⁹¹

Some major news sites have limited anonymous commenting on their articles in reaction to the establishment of intermediary liability for third-party defamatory comments on internet news portals (see B3).

C5 1.00-6.00 pts0-6 pts

Does state surveillance of internet activities infringe on users' right to privacy?	6.006 6.006
---	-------------

Government surveillance is not intrusive, and the constitution guarantees the right to the confidentiality of messages sent or received.[92](#)

Parliament's Security Authorities Surveillance Select Committee oversees surveillance and security agencies. The committee monitors the activities of these bodies to ensure conformity with the constitution, the Security Authorities Act,[93](#) and other regulations, which include necessity and proportionality requirements.

The prosecutor's office monitors surveillance activities and reports regularly to the parliamentary select committee. In its annual report for 2019, the prosecutor's office disclosed that it had granted law enforcement bodies permission to surveil 1,003 times, while the courts had done so 726 times. Surveillance was mainly used in cases concerning organized crime and crimes relating to drugs and taxes.[94](#) While the overall use of surveillance remained stable in 2019, the number of permits for "covert review of possessions" increased by 164 percent and "covert collection of reference materials" increased by 116 percent compared to 2018.[95](#)

In her 2018–19 annual report, the Chancellor of Justice, the state ombudsperson, noted that it reviewed 28 surveillance files, finding that "all had a clearly defined purpose" and that "no surveillance measures carried out without authorisation by a preliminary investigation judge or prosecutor."[96](#)

In response to the COVID-19 pandemic, the government did not release a contact-tracing application until after the coverage period, in August 2020. The app, HOIA, is voluntary. It anonymously logs users' proximity to other users via Bluetooth technology and alerts them when they have been in contact with an individual who has tested positive for COVID-19.[97](#)

In February 2019, Parliament voted to amend the Defence Forces Organisation Act to allow the military to access private data and surveil citizens under certain emergency circumstances.[98](#) However, President Kersti Kaljulaid rejected the measure in March 2019, arguing that it violated basic rights. Parliament passed the amendment again, and Kaljulaid again vetoed it.[99](#) The Supreme Court declared the amendment unconstitutional in December 2019, on the grounds that it would allow individuals to be monitored by the Defence Forces without their knowledge.[100](#)

C6 1.00-6.00 pts0-6 pts

Are service providers and other technology companies required to aid the government in monitoring the communications of their users?	4.004 6.006
--	----------------

Estonia has strong laws protecting citizens' personal information, although service providers are mandated to retain user data. The General Data Protection Regulation (GDPR), which came into force in all EU member states in May 2018,[101](#) puts limits on how interested parties can use and store Estonians' data.

Additionally, the Personal Data Protection Act (PDPA) was amended in 2018 and entered into force in January 2019.[102](#) The law contains the provisions left by the GDPR to EU member states' legislation, which includes certain

exceptions like those identifying instances when the media can use personal data if it is in the public interest. Laws regulating databases and data collection by public and private registries were also updated in the course of this process.

The AKI is the supervisory authority for the PDPA.¹⁰³ In addition, the Chancellor of Justice can make suggestions regarding data protection.

Service providers are required to collect and retain a substantial amount of metadata. These requirements were established under the Electronic Communications Act, which aligned with EU legislation. They were cast into doubt by the CJEU in April 2014, when the court found the European Data Retention Directive (2006/24/EC) to be invalid.¹⁰⁴

Article 111 of the Electronic Communications Act outlines various restrictions on how this data can be stored and used.¹⁰⁵ Data shall be kept for one year, unless there are special circumstances determined by the government that justify keeping it longer, such as maintaining public order and national safety. Article 112 regulates how requests by law enforcement authorities or other agencies can be made in relevant situations, such as criminal investigations, as provided by law. Judicial approval is not always required. These requests for data are kept by the requesting agency for two years. Article 112 also stipulates that operators shall inform the TTJA of requests made and measures undertaken. The Electronic Communications Act has been criticized for allowing requests for metadata in too many situations. While Estonia's Chancellor of Justice has found that the system does not contradict constitutional guarantees, the office has questioned the proportionality of the law.¹⁰⁶ Pursuant to the Electronic Communications Act, the Cybersecurity Act also requires companies to monitor communications, mainly to ensure the security of their own systems; companies are required to inform the RIA of "actions or software compromising the security of the system."¹⁰⁷

In its 2018–19 annual report, the Chancellor of Justice observed that the majority of user data requested by the government in 2017 and 2018 under the Electronic Communications Act was "used in criminal proceedings and in collecting information under the Security Agencies [Authorities] Act," referring to intelligence and law enforcement agencies.¹⁰⁸ The Chancellor of Justice's office randomly reviewed requests from the Police and Border Guard Board, and the MTA, and found that all the requests "had been justified, had been made with the person's prior consent and with authorisation from the head of the institution or the prosecutor's office." Notably, user data was requested in 26 civil proceedings between 2017 and 2018, primarily to identify the authors of anonymous comments in order to lodge defamation claims.

In November 2018, Estonia's Supreme Court made a referral for a preliminary ruling to the CJEU to find out whether EU law, such as the Charter of Fundamental Rights, prevents the state from using people's metadata in the course of investigations into crimes other than serious crimes. The Supreme Court asked for clarification on whether this level of data access is justified and proportional, and whether the process should include judicial review.¹⁰⁹ The case is still pending.

During the state of emergency declared amid the COVID-19 pandemic, the government asked Statistics Estonia to

aggregate anonymized geolocation data from users to inform the state's response to the virus. According to Statistics Estonia's director general, the office worked with telecommunications companies to collate this data. The director general noted that companies were not required to collate the data, and that users' privacy was protected according to data protection rules. The director general stated that the data collection effort was approved by the Data Protection Inspectorate and the Ministry of Justice.[110](#)

C7 1.00-5.00 pts0-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?	5.005 5.005
---	----------------

There have been no registered physical attacks against users or online journalists, though online discussions are sometimes inflammatory. Both critics and supporters of EKRE have faced online harassment, including threats of violence, for their views.[111](#) Online harassment can be reported to the social media administrators or to the police, which has a designated web patrol unit with a presence on Facebook.[112](#)

C8 1.00-3.00 pts0-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?	3.003 3.003
---	----------------

According to the ITU's 2018 Global Cybersecurity Index, Estonia ranks fifth in the world and fourth in Europe in regards to its commitment to ensuring cybersecurity.[113](#) In 2018, the government allocated additional funds to advancing the country's online security and adopted a new Cyber Security Strategy for 2019–22.[114](#) However, the volume of cybercrime increased significantly in 2019, reaching 965 recorded cases. The most typical crime was hijacking a victim's online account. Distributed denial-of-service (DDoS) attacks and other such acts accounted for five percent of all cybercrime.[115](#)

Estonia's cybersecurity strategy is built on strong private-public collaboration and a unique voluntary structure through the National Cyber Defense League.[116](#) With more than 150 experts participating, the league has simulated different security threat scenarios in defense exercises, with the aim of improving the technical resilience of telecommunication networks and other critical infrastructure.[117](#)

As an additional measure to ensure the security of public electronic data, Estonia has established the first of several planned "data embassies." The first embassy, based in Luxembourg, stores public data and information systems critical to the functioning of the state, including its state gazette, land registry, and business register, in the cloud, enabling the Estonian state to function in the event of a cyberattack or other political crisis within the country. The bilateral agreement between the two governments to establish the embassy was signed in June 2017 and it was ratified by both parliaments. The embassy was opened in 2019. The data embassy is granted the same privileges bestowed

upon traditional embassies.[118](#)

The Estonian e-governance infrastructure suffered one of its first major challenges in 2017, when a chip malfunction that could lead to potential security breaches was discovered in government-issued ID cards.[119](#) In response, the government recalled security certificates for more than 760,000 ID cards, which made their electronic use impossible until the certificates were renewed. The issue was apparently discovered before any data was compromised. Despite delays in fixing the issue, the certificates were renewed, and the incident has not significantly affected the public's trust in e-governance. [120](#)

Parliament adopted a new cybersecurity law in May 2018. The law implements EU Directive 2016/1148 on measures for a high common level of security of network and information systems.[121](#) It includes requirements to have a computer security incident response team (CSIRT) and a competent national network and information security (NIS) authority (which Estonia previously had), and strengthens cooperation among EU member states. Businesses identified as operators of essential services are required to take appropriate security measures and to notify serious incidents to the relevant national authority. The supervisory authority under Estonian Cybersecurity Act is the RIA.[122](#)

The North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Center of Excellence is located in Tallinn. Since its founding, the center has supported awareness campaigns and academic research, and hosted several high-profile conferences, among other activities. The center organizes an annual International Conference on Cyber Conflict, or CyCon, bringing together international experts from governments, the private sector, and academia, with the goal of ensuring the development of a free and secure internet.