ActiveWatch

FreeEx Digest

- No. 2

Control and censorship of digital communications

Kingdom of the Netherlands

The FreeEx Digest project is funded by the Embassy of the Kingdom of the Netherlands. The views and information presented in this project do not represent the position of the Embassy of the Kingdom of the Netherlands. Responsibility for the accuracy of information and editorial decisions rests solely with ActiveWatch.

FreeEx Digest is an editorial project of the ActiveWatch Association, produced by the ActiveWatch team and its collaborators and financially supported by the Embassy of the Kingdom of the Netherlands.

In the upcoming months we will regularly produce summaries of the main issues that can negatively influence the right to correct information and freedom of expression in Romania.

We will talk about cases of journalists who are not allowed to work in the public interest, expose practices and institutions that restrict freedom of expression and try to offer recommendations and solutions for citizens overwhelmed by the huge flow of contradictory or misleading information that fuels our anxiety and prevents us from making informed decisions.

The FreeEx Digest project is inspired by more than 20 years of work in monitoring freedom of the media and contained in the annual reports on freedom of expression in Romania.

FreeEx Digest no. 1 "Safety of Journalists. Public Lynching and Kompromat" can be read here.

FreeEx Digest n0. 2 was developed in collaboration with Asociația pentru Tehnologie și Internet - Association for Technology and Internet (ApTI).

Prime Minister Nicolae Ciucă on banning TikTok on Romanian institutions' phones:

“(...) through this channel a whole series of elements are delivered, messages that do not always have the content we want."

(March 2023)

TABLE OF CONTENTS

FreeEx 2022 - 2023 // Control and censorship of digital communications

Last week, on 28 February 2023, the Constitutional Court rejected the complaints of unconstitutionality filed by the opposition parties and the Ombudsman on the cyber security law. The law had been criticised by several non-governmental organisations, including for introducing "propaganda and disinformation" on the list of threats to national security and imposing security obligations on all " individuals and legal entities providing public services or services of public interest", which in theory could easily include any online mass-media.

In the context of the recent decision of the Constitutional Court, we believe it is worth summarising the main events and legislative initiatives in the field of digital communications, adopted or discussed by the authorities over the past year and a half, which may have an impact on the work of journalists. The safety of journalists also includes the confidentiality of communications and the protection of online privacy, with the European Commission calling on Member States to ensure that journalists and other media professionals are not subject to unlawful online tracking or surveillance, including in the context of police investigations that may compromise the protection of journalistic sources (see also the February 2023 issue of FreeEx Digest No 1: "Safety of journalists. Public lynching and kompromat").

The war in Ukraine has been used over the past year by state authorities to restrict fundamental rights, including freedom of expression. Thus, in 2022, several laws were passed targeting digital communications and giving to intelligence services increased powers to access non-public data, as well as the right to interfere with freedom of expression. When viewed from the specific situation of a journalist or newsroom, these legislative changes are all the more worrying. Criticisms from organisations with expertise in digital rights, fundamental rights and good governance, opposition politicians and European institutions, have been largely ignored, with the government and parliament giving the impression that they are responding without much critical analysis to the demands made by the intelligence services. The overwhelming majority of the new legal provisions have unfortunately passed the constitutionality test.

The war in Ukraine has also intensified government censorship and cyber-attacks, including on media websites. This has been compounded by social networks censoring or limiting content in a non-transparent way and based on unclear algorithms. In this way, the state, together with private actors, have restricted the public's right to information.

Main events and actions impacting digital freedom in 2022 - 2023:

Intelligence services write their own laws

Authorities in Bucharest sparked strong public controversy in June 2022, when information leaked to the press about a package of national security laws, allegedly drafted not in the offices of the Romanian government, as would have been expected, but rather in those of the intelligence services. The main problem with this package of national security laws was that it gave increased powers to the intelligence services, while control over these services was diminished.

Cyber security law: more “Securitate”, less security

Under the new cyber security and defence law, declared constitutional by the Romanian Constitutional Court on 28 February 2023, natural and legal persons providing public services or services of public interest (so, potentially, mass-media included) have extended obligations, including to report cyber security incidents affecting their systems within 48 hours of their occurrence, or risk a hefty fine (1-3% of their turnover). Cyber security service providers are also obliged to provide security information about their clients (so including the media) without a court order, and even if the information requested is protected by a confidentiality agreement.

One of the most serious provisions is the new law's addition of provisions from the existing National Security Law. Thus, campaigns of "propaganda or disinformation likely to affect the constitutional order" are added to the list of threats to national security, which gives unjustified powers to the Romanian Intelligence Service (SRI) to limit the right to freedom of expression, by unilaterally determining the actions that fall into this category, as well as collecting information and carrying out specific surveillance measures in such cases. Basically an entire newsroom can be prosecuted by the SRI, only if it is suspected of being responsible for actions that fall into this category (legally, prosecution can only be done with a warrant from a judge, but let's not forget that de facto this filter does not exist - over 99% of national security surveillance warrants are approved).

Broadening the interception of electronic communications

The amendments to the communications code adopted in 2022 also sparked strong public controversy, because they unduly broadened the possibility of interception of electronic communications by criminal investigation bodies and the Romanian Intelligence Service (SRI), imposing excessive obligations on providers, including a new category of electronic hosting service providers. In the case of mass-media, this would mean that any data (evidence from investigations, unpublished articles, information sent by whistleblowers, etc.) that would be on a server could be obtained directly from the host, following a warrant sent to it.

Government censorship - websites arbitrarily blocked

The National Cyber Security Directorate (DNSC) is requesting that websites are blocked without a clear legal basis, without an appeal procedure and without meeting the necessary criteria of institutional independence. The blocking of a journalistic website (aktual24.ro) as well as a book review blog and shops websites, including IP addresses owned by Google, gives a measure of the arbitrariness of this type of action, initiated as an extension of the blocking of official Russian websites, requested by the European Union.

Private censorship

Blocking, limiting or deleting Romanian-language media accounts from social media - without explanation or any legal reason, often followed by the impossibility of resuming them and recovering the audience they had - has been a common practice of Facebook and/or Google for many years. The measures seem to be taken either by automated systems or by people who do not understand Romanian at a basic level. Such measures have, in recent years, affected the pages of several online publications, such as HotNews, G4Media, profit.ro, Aktual24.ro, Dela0, Investigatoria, descopera.ro. The Facebook page of the satire publication Times New Roman has been deleted. Journalists have also been affected by Facebook's arbitrary decisions. For example, as recently as January 2023, Cătălin Tolontan's page suddenly lost its reach after publishing a link to a Libertatea investigation into a sex offender.

Cyber attacks on the media

In the context of the war in Ukraine, the number of cyber-attacks has increased, with many of the targets being newsroom websites. Digi24, Hotnews and G4Media have been hit by such attacks.

The intelligence services began 2023 with increased powers, to the detriment of protecting the fundamental rights of citizens and the balance of power in the state. We can expect this trend to continue, as civilian control over the intelligence services is of real concern only to a handful of politicians, usually from the opposition, and a few civil society organisations, and judicial control is de facto non-existent. Under the security package of laws mentioned at the beginning, parliamentary control over the intelligence services could be significantly reduced. The wider scope of action of the intelligence services also has a potential impact on freedom of expression and freedom of the press, because the safety of journalists' communications is diminished, along with that of every citizen. Add to this the fact that it has only been six years since the Romanian Intelligence Service (SRI) admitted to having agents infiltrating the press, information reinforced by a former SRI director.

Security Laws

At the end of May 2022, G4Media made public that a set of ten draft security laws was on the table of the governing coalition. The need to modernise legislation in this area is unquestionable, but the package of laws presented by G4Media revealed the ruling coalition's endorsement of significantly reducing civilian control over intelligence services. They (notably the Romanian Intelligence Service - SRI and the Foreign Intelligence Service - SIE), under the draft laws, would receive expanded rights. The publication of the drafts triggered a public outcry, although many newsrooms ignored it completely or even raised suspicions of censorship. So, according to the drafts leaked to the press:

- SRI can ask citizens for help whenever it feels it needs it, and they would be obliged to help. No exceptions. Including, therefore, journalists.

- Prosecutors would be able to search SRI and SIE premises only with the approval of the Supreme Council of National Defence (CSAT) chairman (who is the President of Romania) and only if the director of the service was notified beforehand. Moreover, only certain designated prosecutors could investigate intelligence officers.

- The list of areas constituting threats to national security would be extended to include organised crime, critical communication and information technology infrastructures, Romania's scientific and research interests, the public administration system, health, education and cultural heritage. By expanding the list of areas of national security so broadly, SRI would be able to apply for national security warrants for virtually any reason. These warrants could be requested directly from the Supreme Court (ICCJ), without having to go through the General Prosecutor's Office.

- Parliament's control over the services would decrease. The Director of SRI could only be dismissed by the President of Romania for political involvement. The Parliament would no longer be able to ask for the Director's dismissal, but only vote on the appointment. The service would also enjoy more freedom in its covert activities. At present, companies opened by the SRI are under parliamentary control, which this bill would remove. The director would also no longer have to submit an annual report to parliament.

These are not the only problems with the package of laws unveiled by the press. There are numerous articles in the ten draft laws contained in the package - not formally adopted by the government - that directly infringe fundamental rights such as freedom of expression or the right to privacy. Moreover, the drafts seek to recover powers of the SRI that have been lost or called into question by the Constitutional Court decisions.

No person or institution has taken responsibility for writing these draft bills. Prime Minister Ciucă vaguely stated that "the laws were drafted at the level of each

institution responsible". Marcel Ciolacu also said that he was aware of the existence of the laws. President Klaus Iohannis denied that he had seen the drafts, despite the fact that the Foreign Intelligence Service (SIE) said that "the working versions of the national security laws are the result of consultations with the Presidential Administration and the General Secretariat of the Government". Several MPs accused the secret services of writing the package of laws.

In his first reaction, President Klaus Iohannis was more concerned about the way the drafts became public than their content. Moreover, he made veiled threats against the whistleblower who leaked the documents to the press.

45 NGOs, including the Association for Technology and the Internet and ActiveWatch, criticised both the president's statement and the package of laws. Reporters Without Borders also condemned the head of state's reaction, which threatened G4Media journalists and their source.

Although the package of laws was supposed to be on the government's agenda in the summer of 2022, the public outcry surrounding them has led to their adoption being postponed. Parliament has adopted one of the ten bills, the cyber security and defence law, by the end of 2022.

Cybersecurity law

The Ministry of Research, Innovation and Digitisation initiated in early November 2022 a draft law on Romania's cyber security and defence. It is part of the unofficial package of national security laws, and is almost identical to the one presented by G4Media in the summer of 2022. The version adopted by the government has been modified from the one presented for public debate, becoming tougher (a whole chapter of sanctions has been introduced - with fines of up to 10% of the turnover) and more extensive (the paragraph on propaganda and disinformation was only included in the law when it was adopted by the government).

Subsequently, the bill was adopted by Parliament in December 2022, passing through both chambers in just nine days. The Romanian Constitutional Court (CCR) ruled on the constitutionality of the draft law on 28 February 2023, following complaints of unconstitutionality by the Ombudsman and USR and Forța Dreptei political parties, respectively.

According to the law on cyber security and defence, the National Cyber Security System (SNSC) is to be set up under the management of the Cyber Security Operational Council (COSC). The SNSC is a framework for cooperation between 12 institutions: the Supreme Council of National Defense (CSAT), the Ministry of Research, Innovation and Digitisation (MCID), the National Cyber Security Directorate (DNSC), ANCOM (the telecom regulator), the Ministry of National Defense (MApN), the Ministry of Internal Affairs (MAI), the Foreign Affairs Ministry (MAE), the National Registry Office for Classified Information (ORNISS), the Romanian Intelligence Service (SRI), the Foreign Intelligence Service (SIE), the Special Telecommunications Service (STS) and the Protection and Guard Service (SPP). The COSC is a consultative body, with the Chairman being the Presidential Adviser on National Security Matters. SRI is responsible for the technical secretariat.

Both the Association for Technology and the Internet (ApTI) and APADOR-CH have criticised some of the provisions of the law, a criticism echoed by several organisations. The NGOs said the new law would unduly extend responsibilities for protecting cyber security to broad categories of companies and individuals. The services would be able to arbitrarily, and therefore potentially abusively, restrict fundamental rights such as privacy and freedom of expression.

Under the new law, natural and legal persons providing public services or services of public interest are compelled to report cyber security incidents within 48 hours of their occurrence through the National Platform for Cyber Security Incident Reporting (PNRISC), to which 11 of the above institutions have access. According to ApTI, this goes beyond the European legal framework. Basically, any internet provider and owner of any private network or computer system considered to be of public interest, so potentially any media institution, NGO or private entity providing public services or services of public interest, could fall under the law. The terms used are not defined in the law (despite comments to this effect by several organisations), so it will be up to the authorities to decide, through subsequent secondary legislation (and therefore potentially to be amended by any government), who these

"public service or public interest providers" will be. ApTI and APADOR-CH have pointed out that it will be impossible for many small companies to meet the 48-hour deadline, as well as other obligations for these providers, such as supply chain risk analysis. The fines imposed by the new law are disproportionately high - from 1% of the turnover for the first offence (!) to 3% of the turnover for the second offence.

Another problem is the obligation imposed on cyber security service providers to provide security information about their clients to 11 institutions without a court warrant, and only on the basis of a "reasoned request". For example, an institution such as the National Registry Office for Classified Information (ORNISS) or the Ministry of National Defense (MApN) or the Ministry of Research, Innovation and Digitisation (MCID) has the right to receive answers to any questions it makes to a cybersecurity provider, even if the data requested is protected by a confidentiality agreement. As ApTI has explained, this obligation is a breach of contractual confidentiality similar in concept to that in which a lawyer would be obliged to provide information about what his client is doing, a journalist about his sources or an auditor about his clients.

One of the most serious provisions is the new law's addition of provisions to the existing national security law. Thus, campaigns of "propaganda or disinformation likely to affect the constitutional order" are added to the list of threats to national security, which gives unjustified powers to SRI in limiting the right to freedom of expression. As the NGOs' analysis shows, since "propaganda or disinformation" campaigns are not sufficiently defined by law, it is up to an authority such as SRI to decide what falls within the definition in the law. With this legislative amendment, the organisations point out, it could also become an offence to express opinions contrary to an official state policy (e.g. vaccination policy). Thus, the authors of such critical positions, directed against official policy, or, in general, any person responsible for any campaign that SRI would consider "propaganda or disinformation, likely to affect the constitutional order", can be prosecuted, applying Article 404 of the Criminal Code: "Communicating or disseminating, by any means, false news, data or information or false documents, knowing their false nature, if this endangers national security, is punishable by imprisonment from one to five years." In addition, by including campaigns of "propaganda or disinformation likely to affect the constitutional order" in the list of threats to national security, the SRI may request surveillance warrants on national security for any technical surveillance measure they find appropriate to detect or analyse such cases.

Communications Code

The European Communications Code is a 2018 European directive, which was ready for implementation in Romania as early as November 2020, but was adopted a year later, three days before the Cîțu government was dismissed.

The law, in the form proposed by the Government, came with a problematic article, in addition to the European text, and which had not existed in the draft when it was in public debate: Art. 10^2. This article widened the scope of interception of electronic communications, including the content of encrypted communications.

The draft would have affected two types of providers:

- providers of "electronic hosting with IP resources" (those who provide access services to content stored on a web address - basically everything on the web),
- providers of number-independent interpersonal communications services (e.g. apps like WhatsApp, Messenger, Signal or Telegram).

Following criticism from the opposition political parties and NGOs (mainly ApTI), the second category was removed before the Senate vote in early 2022 (the Chamber of Deputies had voted on the draft at the end of 2021). Thus, only e-hosting providers with IP resources remain affected.

According to Art. 10^2, such providers must assist state bodies in the technical monitoring of their customers and users. Specifically, the obligations are detailed in four areas, vaguely explained:

- a) to enable lawful interception of communications, including bearing the costs thereof;
- b) to grant access to the content of encrypted communications transmitted over their networks;
- c) to provide retained or stored information on traffic data, subscriber or customer identification data, payment methods and access history with related timestamps; (this point was declared unconstitutional, and removed from the final form of the law - see below)
- d) allow, in the case of electronic hosting service providers with IP resources, access to their own computer systems, in order to copy or extract existing data.

Another problem created by the draft in Art. 10^2 letter a) is that providers, and not the state, are responsible for building and maintaining the interception infrastructure. Also, all hosting providers are obliged to register with ANCOM. According to ApTI, this contradicts European legislation, namely the e-commerce directive.

The draft has passed the Parliament and has been challenged at the Constitutional Court by the Ombudsman and USR political party. The CCR declared only letter c) unconstitutional. On 6 July 2022, the President of Romania promulgated the amended law, after it passed the Parliament.

Nearly nine months after the adoption of the law and ANCOM has no procedure and no public register where hosting providers can notify themselves and no public project to do so (unlike other providers already regulated).

Government censorship - websites arbitrarily blocked

The Russian military invasion of Ukraine has provided Internet security authorities with a new pretext to take arbitrary decisions to block websites under a non-existent legal framework. Moreover, the authorities do not seem to have learned the lessons of the pandemic, when, in the name of fighting disinformation, they took controversial decisions that further fuelled public distrust and legitimised precisely those voices that adhere to conspiracy theories, to the detriment of transparent and open debate.

Blocking a website, which is a means of public communication, is a sensitive decision because it is tantamount to suppressing a publication from appearing, thus violating a fundamental and constitutional right. In a democratic state, such an action can only be acceptable as an extreme solution. Such a decision must be taken transparently, with information for those affected and on a clear legal basis, allowing access to independent review bodies. In any case, the requirements of the ECHR, which has extensive case law on the subject, must be followed.

On 28 February 2022, several sources accused of Russian propaganda were blocked, including Sputnik and Russia Today. The decision to stop the two media channels was taken at European level (by a decision of the European Council) and later extended to four other Russian websites.

On the same day, the National Cyber Security Directorate (DNSC) published a list of "fake news" sites and IP addresses used in cyber attacks. In a press release the same day, the institution admitted that "the issue of <<fake news>> is not within the Directorate's remit". In fact, legally speaking, the DNSC cannot decide on blocking a website. In Romania, the blocking of websites is done through internet providers, which are regulated by ANCOM.

On 3 March 2022, the Association for Technology and the Internet (ApTI), along with several other organisations, sent a non-public letter to the DNSC and ANCOM, calling for more measures to prevent abuse. The letter went unanswered. Moreover, also on 3 March, the aforementioned list was extended by two domains, one of which was aktual24.ro, an online publication launched in 2015 by journalist Ovidiu Albu. The blocking of the site took place without the journalist being warned in any way by the authorities of this decision. Albu denied on his personal Facebook page the accusations of pro-Russian propaganda and stressed that, on the contrary, aktual24.ro's position had been critical of Russia's invasion of Ukraine.

It was only a day later, on 4 March, amid the public outcry over the blocking of the site, that aktual24.ro started working again. However, no institution has explained the decision to include the site in the blocked list. Moreover, the DNSC said in a press release that the decision to block was not its own, as the lists published daily

and sent to the state authorities were a coordinated collaborative effort between several state institutions with competences in the field.

On 15 March 2022, information appeared in the public space that illegal website blocking continued. Among the dozens of domains affected were: bookblog.ro, a book review blog; doilupi.ro, a shop in Beiuș; enterieur.ro, a furniture website; two subdomains firebaseio.com, owned by Google. Under pressure from civil society, the DNSC justified its actions by citing an international alert that these sites were involved in DDoS attacks on EU institutions.

The DNSC's last updated list in September 2022 contained over 36,000 IPs, most of which were from the US. A significant proportion of these are TOR exit nodes, used including by journalists and activists from countries where the Internet is censored (e.g. Belarus, Russia, China) to access content blocked in their country.

Private censorship

Another issue that continued into 2022 was the restrictions placed on journalists by social media companies.

The Times New Roman satire publication's Facebook page, which had been in existence for 13 years, and had 650,000 followers and over 30,000 posts, was deleted.

The Facebook page of the website Investigatoria was reported en masse, resulting in the deletion of several posts. According to Investigatoria, this allegedly happened after the publication of an article that led to the arrest of a county councillor on suspicion of paedophilia. The profit.ro page was also restricted so that posts could no longer be suggested to users, a situation Aktual24 also faced in 2022. Facebook has also restricted the pages of several publications in the past, including G4Media, HotNews, Dela0, descopera.ro (a history magazine) and accounts of journalists, public figures and politicians.

In early 2023, journalist Cătălin Tolontan announced that his Facebook page had decreased its reach after he published links to Libertatea newspaper's investigations into a sex offender. The journalist reported that this happened because the algorithms do not distinguish between exposing an aggressor and promoting an aggression.

Cyber attacks

In the context of the war in Ukraine, 2022 saw an increase in the number of cyber attacks, most of which were DDoS cyber attacks. This type of operation targets websites and servers and aims to deplete resources, with very many hits in a short time.

In the case of Romania, most of the attacks came from an independent but pro-Russian group - Killnet - with attacks being more intense at the beginning of the invasion. The pro-Russian group threatened to attack 300 sites, many of them media sites. In Romania, Killnet has claimed DDoS attacks both on the websites of news outlets such as Digi24 and on the websites of state institutions: the Romanian government, the Ministry of Defence, DNSC, The Romanian Railway (CFR), the police, etc. HotNews was the victim of a DDoS attack in May 2022. Although no group claimed responsibility, KillNet was still the main suspect. The G4Media website suffered a DDoS attack in September 2022. G4Media linked this incident to the publication of an article related to the plagiarism of Prime Minister Nicolae Ciucă. At the time, the Prime Minister publicly called for an investigation into the event.

Team

Andrei Boloș / ActiveWatch

Ionuț Codreanu / ActiveWatch

Liana Ganea / ActiveWatch

Ioana Popa / ActiveWatch

Bogdan Manolea / ApTI

Bucharest,
March 2023