

INTERNET FREEDOM REPORT 2014: SLOVAKIA

Overall Internet freedom score: **33/50**
 Gross domestic product per capita: €18,940 per annum¹
 Population: 5.4 million
 Percent of individuals using the Internet in 2013: 77.88²
 Facebook subscribers: 2,032,200³
 Average broadband speed: 25.06 Mbps (36th out of 192 countries)⁴

Freedom of Expression	10
Maximum potential score	15
Big Brother	10
Maximum potential score	15
Legal Maze	7
Maximum potential score	10
Open Government	6
Maximum potential score	10
Total Score	33
Maximum potential score	50

Free for All, but Someone is Watching

Slovakia has a dynamic, uncensored Internet market, but there are gaps in legislation and the regulatory framework that need to be remedied. Web content is subject to court rulings that tend to favor political actors, and out-of-control surveillance undermines the rule of law and right to privacy.

by Miroslav Kollár*

The Internet in Slovakia remains largely free of direct regulation and state censorship, but informal avenues and the lack of a legal framework for the Internet do pose challenges for freedom of expression and for privacy rights. Fortunately, there are few instances where websites are taken down or specific online content is banned, and the government rarely seeks to block a website.

The country has a freedom of information law, and legislation requires that some types of information should be posted online on a regular basis. Former Prime Minister Iveta Radičová pushed to have government contracts posted online, and a range of nongovernmental organizations have worked to make the public information that is online more accessible and searchable.

Almost 80 percent of people in Slovakia are online in a marketplace that offers plenty of competition among service and content providers.

But Slovakia's online world is constrained in informal ways.

1 Organisation for Economic Co-operation and Development (OECD), converted from USD at European Central Bank exchange rate, December 31, 2013. See: <http://stats.oecd.org/index.aspx?queryid=558>

2 International Telecommunication Union statistics, http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Individuals_Internet_2000-2013.xls

3 Internet World Stats, December 31, 2012, <http://www.internetworldstats.com/stats4.htm>

4 Ookla Net Index Explorer, accessed October 8, 2014, <http://explorer.netindex.com/>

* The author is Executive Director of the Institute for Public Affairs (IVO), Slovakia.

© Institute for Public Affairs (IVO), Transitions (TOL), and PASOS (Policy Association for an Open Society), March 2015
 ISBN 978-80-87804-14-8

This study was written as part of the project, **Internet Freedom Report 2014: Visegrad Four**, a project of Transitions (TOL) and PASOS (Policy Association for an Open Society). The preparation of the reports was supported by Google. The reports were prepared with full research independence and the views expressed herein are views of the authors only (and not of Google).

On the one hand, online media is not subject to regulation. On the other hand, online journalists are not protected by the same laws as print journalists, even when they write for both the print and online editions of the same titles.

The Slovak blogging world provides a rich array of commentary and investigative reporting, including investigative blogs from journalist Tom Nicholson in cooperation with Aliancia Fair-Play,⁵ and the investigative blogspot of Milan Krajniak.⁶ Nevertheless, the future of independent news coverage is now uncertain since the largest daily newspaper SME (www.sme.sk) was taken over by investment group Penta in October 2014, prompting the resignation of the newspaper's core editorial team.⁷ Penta is one of two Slovak financial groups (the other is J&T) that have acquired major holdings in Slovak media, drawing criticism (which Penta refutes) that they are buying influence and preventing independent media investigation of their business activities.⁸

Despite the absence of formal censorship, would-be censors of any stripe can pressure online content providers to remove or alter content with the threat of prohibitively expensive legal action.

No law spells out who is responsible for third-party content on websites, such as comments, although a recent court ruling did determine that website hosts were not responsible for anonymous posts. Regulators have also ducked the issue of net neutrality. In a recent dispute between two providers, the telecoms regulator claimed to have no competence on the question, and cable operators feel free to block third-party hardware and content if they feel the potential exists to affect their own businesses.

⁵ <http://fairplay.blog.sme.sk/>

⁶ <http://www.poslednykraziak.sk/>

⁷ *Investorom v Sme bude Penta, vedenie denníka odchádza (Penta will be investor in SME, the daily's management prepares to leave)*, *Pravda*, October 14, 2014, <http://spravy.pravda.sk/ekonomika/clanok/333096-penta-definitivne-kupuje-polovicu-petit-pressu/>

⁸ Rick Lyman, "Oligarchs of Eastern Europe Scoop Up Stakes in Media Companies", *New York Times*, November 26, 2014, www.nytimes.com/2014/11/27/world/oligarchs-of-eastern-europe-scoop-up-stakes-in-media-companies.html?_r=0

While law enforcement and security agencies are required to get a court order before conducting online or other surveillance, the recent publication of telephone and email transcripts of journalists surveilled for questionable reasons raises doubts about how well the system works. Virtually all requests by police and security agencies to conduct surveillance were granted by the courts in 2012-2013.

CONCLUSIONS AND RECOMMENDATIONS

Several of the current problems and omissions can be solved by the introduction of updated legislation, for instance on prohibition of defamatory content and protection of journalists' sources. Others require more careful oversight, for instance of police surveillance, and strengthened independence of the judiciary to inspire confidence and clarity in the legal framework and the rule of law.

FREEDOM OF EXPRESSION

- Legislation should be updated to stipulate that online journalists have the right to protect their sources, and to give the public recourse to respond to, or demand correction of, factual errors published in online media.
- Strengthened independence of the judiciary from political interference should be a priority so that judgments are based on the facts of the case and impartial interpretation of the law in libel cases.
- Laws prohibiting defamatory content based on race, nationality, or political or religious beliefs, should be extended to cover online content.

BIG BROTHER

- More careful oversight is needed in the area of surveillance, especially when the targets are journalists.
- Legislation is needed to stipulate whether telecommunications and Internet service providers can impede access to content from competing companies; and to close loopholes that allow police to freely obtain certain information on Internet users.

LEGAL MAZE

- Censorship is prohibited by the constitution, but a regulatory framework is needed, backed up by a definition of censorship applicable to the online world.

OPEN GOVERNMENT

- Public authorities should be required to respond more promptly and fully to access-to-information requests.
- The law requiring publicly funded contracts to become valid only after being published online, introduced in 2010, marked a big step toward transparency in the use of public money, but should be strengthened by requirements that documents online are searchable, and include all pricing and budget details, with exceptions only where grounds have been clearly established that certain information comprises a trade secret as defined by law.

FREEDOM OF EXPRESSION

4/5: *The legal framework and instances of prosecutions entailing denial of freedom of expression.*

3/5: *Legal rights and protections for online expression and their status compared with print and broadcast rights.*

3/5: *Cases of bloggers or online journalists being prosecuted, fined, or jailed for defamation or libel.*

Free, but Lack of Explicit Internet Legislation

Freedom of expression on the Internet is not explicitly covered by legislation, and it can come under threat in the courts or in decisions on news objectivity by the politically appointed Council for Broadcasting and Retransmission.

Neither the Press Act of 2008 nor an amendment to it in 2011 addressed online journalism. As a result, journalists for online media do not have the same rights as print journalists, such as protection of sources. At the same time, unlike in the case of print media, the public does not have recourse to the same legal means to respond to, or demand correction of, factual errors published in online media.

Under European Union (EU) law, online audiovisual media (such as on-demand service providers and Internet broadcasters) are regulated somewhat similarly to traditional broadcasters. This includes the obligation to place viewer age advisories on videos and to make a clear distinction between advertising and content. However, the regulation does not include provisions on "news objectivity," which apply to traditional broadcasters. The responsible regulator is the Council for Broadcasting and Retransmission, whose nine members are elected by the Parliament.

Self-regulation to Dowse Controversy

There are no clear definitions of incitement to violence or of hate speech on the Internet in Slovakia. Discussion forums are subject to self-regulation, and some national media outlets prohibit forums in the case of “provocative” topics that would likely elicit controversial and racist comments.

Laws do not explicitly regulate online expression of issues surrounding race, religion, national security, and other topics. Only audiovisual media are specifically prohibited from broadcasting programs containing defamatory content based on race, nationality, or political or religious beliefs, with the threat of license revocation. Such content, when posted online, can be subject to lawsuits or investigations based on standard legislation, such as the criminal or civil code.

There are no restrictions on the acceptance of advertising or investment by online media, whether from government or private sources, foreign or domestic.

A more serious problem is posed by court rulings in libel cases that are often in favor of political figures, most of which concern content published in print media that has also been published in the digital versions of these media outlets.

One such recent ruling against the *Nový Čas* newspaper and website has been criticized by international press-freedom groups. A Bratislava court in June 2014 ordered the media organization to apologize to a judge after it published photos (and posted a video online) of him at a party seemingly mimicking a mass murderer who had killed eight people, including himself, two months earlier. The judge held a fake assault rifle and, like the murderer, wore blue ear protectors.⁹ *Nový Čas* owner

⁹ Michaela Terenzani-Stankova, *The Slovak Spectator*, Bonanno case sees first verdict, June 23, 2014. http://spectator.sme.sk/articles/view/54388/2/bonanno_case_sees_first_verdict.html
 Kauza Bonanno pokračuje, znalci sa na súde opäť sporili o pravosť fotky (Bonanno Case Continues, Experts in Court Again Disagreed Over Authenticity of Photo), *Mediálne.sk*, October 11, 2014
<http://medialne.etrend.sk/tlac/kaucha-bonanno-pokracuje-znalci-sa-na-sude-opat-sporili-o-pravost-fotky.html>

Ringier Axel Springer faces a series of ongoing lawsuits in connection with the article.

The most common way of pressuring bloggers and online media outlets is to threaten legal action if content is not removed.

Hunting for the Truth

One of the most highly publicized cases of a blogger facing legal charges was that of politician Juraj Poláček of the liberal *Sloboda a solidarita* (Freedom and Solidarity) party. In an early 2013 post, *Vrahovia medzi nami* (Murderers Among Us), he paraphrased information from *Plus 7 dní* magazine to imply that then President Ivan Gašparovič was somehow involved in the death of Michal Bobák, a forester who used to go hunting with the president and was shot dead in 2009.¹

The article (and Poláček’s subsequent blog post) implied that the president was in the woods around the time Bobák was shot (another person, Štefan Drozd, was later charged with the killing, although the article in *Plus 7 dní* wrote about rumors that Drozd might have taken the blame for an “eminent person”). The police investigated after the president’s office accused Poláček of libel. After the police did not bring criminal charges, the case was moved to a lower court. Poláček was never charged, suggesting that the case had been dropped. According to *SME* newspaper, the authorities refused to disclose the official results of the investigation.²

¹ Juraj Poláček, *Vrahovia medzi nami* (Murderers Among Us), January 1, 2013. <http://www.blogovisko.sk/vrahovia-medzi-nami.html>
 Ľudmila Lacková, *Prezidentov poľovník utŕžil ranu rovno do hrude* (President’s huntsman shot in the chest), *Plus 7 dní*, August 14, 2009.
<http://www.pluska.sk/plus-7-dni/archiv/vsimli-sme-si/prezidentov-polovnik-utrzil-ranu-rovno-do-hrude.html>

² *Za blog o poľovačke prezidenta nedostal pokutu* (No Fine for Blog about President’s Hunting), *SME*, January 10, 2014. <http://www.sme.sk/c/7063148/za-blog-o-polovacke-prezidenta-nedostal-pokutu.html>

For example, in 2007, university teacher Andrej Školkay threatened to sue former student Michaela Stanková over a blog post criticizing his publications and work at the university. Subsequently, SME newspaper (which published Stanková's blog post on its website) stopped cooperating with Školkay, who had written columns for the newspaper. Školkay requested a formal apology and €500 in damages. Stanková refused to comply. After the case was made public, Školkay did not follow through with the lawsuit.¹⁰

¹⁰ Tomáš Czwitkovics, *SME ukončilo spoluprácu s Andrejom Školkayom (SME stopped cooperation with Andrej Školkay)*, Mediálne.sk, February 6, 2007. <http://medialne.etrend.sk/internet/sme-ukoncilo-spolupracu-s-andrej-školkayom.html>

Responsible for Comments?

The question of who is responsible for actionable online content was addressed in a potentially precedent-setting court decision in 2012. A court in Trenčín County ordered the Strážov civic organization to delete an anonymous comment in a discussion forum that called a local businessman "a thief and a conman." The court also ordered Strážov to pay €5,000 to the businessman. However, the ruling was overturned by a higher court, which said that websites are not responsible for anonymous posts by users.¹

¹ Michal Piško, *Diskusie na webe súd neobmedzil (Court did not constrain discussions on the web)*, SME, April 26, 2012. <http://www.sme.sk/c/6354674/diskusie-na-webe-sud-neobmedzil.html>

BIG BROTHER

4/5: *Censorship – laws and implementation, and pressure-group activity, including requests to remove material.*

4/5: *Filtering and blocking of Internet content by state and other actors.*

2/5: *Published information on government surveillance/tapping – by government and by private companies.*

Censorship Forbidden, Surveillance Out of Control

Censorship per se is mentioned only in the constitution, which forbids it. Other laws, such as the Press Act, do not offer a definition of it or possible regulation.

Pressure groups usually do not focus on the removal of content. In rare instances, they focus on vulgar or sexual TV programming, which is regulated by the media regulator and subject to steep fines. Police or courts can order hosting services to remove content if the content is deemed illegal (such as child pornography or material that violates copyrights) or violates the rights of plaintiffs in libel cases. (See "Gorilla Tactics".)

Between July 2009 and December 2013, Google has received only two take-down requests from authorities in Slovakia: in the first half of 2012 it was asked to remove two items of blog content for reasons of privacy and security; then again it was asked to removed three items of content of an undisclosed nature for reasons of privacy and security in the second half of 2013. The company complied in both cases.¹¹

¹¹ Google Transparency Report, <http://www.google.com/transparencyreport/removals/government/SK/?hl=sk>

In its reports on government information requests covering the whole of 2013 and the first half of 2014, Apple listed only one request from Slovak authorities for customer information (the request was for device-specific information, and no data was provided by Apple).¹²

Until April 2014, providers of electronic communication services were obliged by EU law to archive certain user data for 12 months, except for Internet service providers, which were to keep it for six months. This information mainly included the user's name, address, telephone numbers, username, time of phone calls or Internet sessions, duration, and location. Companies that did not collect and provide the data to authorities could be fined up to €300,000.

Prosecutors, police, or other investigators in probes of serious crimes, corruption, or possible terrorist activities, could obtain access to the data with a court order.

The requirement to collect the information was suspended in April 2014 following a ruling by the European Court of Justice striking down the EU directive. The Justice Ministry has proposed changes to make the law comply with the European Court's ruling. These changes are under review by the country's Constitutional Court.¹³

¹² Report on Government Information Requests, January 1 - June 30, 2013, https://www.apple.com/pr/pdf/131105r_eportongovinforequests3.pdf
Report on Government Information Requests, July 1 - December 31, 2013
<https://www.apple.com/privacy/docs/government-information-requests-20131231.pdf>
Report on Government Information Requests, January 1 - June 30, 2014,
<https://www.apple.com/privacy/docs/government-information-requests-20140630.pdf>

¹³ Ivan Kvasnica, Ústavný súd: Operátori nesmú uchovávať údaje o hovoroch či navštívených weboch (Constitutional Court: Operators must not archive data about phone calls or visited websites), *Živé.sk*, April 25, 2014 <http://www.zive.sk/clanok/95139/ustavny-sud-operatori-nesmu-uchovavat-udaje-o-hovoroch-ci-navstivenych-weboch>
Court of Justice of the European Union, The Court of Justice declares the Data Retention Directive invalid. April 8, 2014. <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>

Police can request location data in missing persons and car theft cases upon authorization by family members or vehicle owners. In 2013, *SME* newspaper reported that police sometimes obtain private data without court permission thanks to loopholes in the law. For example, in 2010 police requested, without court permission, the name of an ISP's client who was allegedly using someone else's name in a discussion forum, the newspaper reported. The ISP provided the information even though it was clear that this case was not among the types listed in legislation in which private data can be provided to the police.¹⁴

In the past three years, there have been two major instances when information leaked that journalists' communications had been under surveillance, but the monitored content reportedly consisted of phone calls.

In one case, a report leaked in 2011 that military intelligence tracked phone calls of journalists working for the *Pravda* daily and the director of news TV broadcaster TA3. Accusations were made in the press that the surveillance was meant to gather information on the government's opponents. In 2013, *SME* published phonecall transcripts and recordings showing that investigative journalist Tom Nicholson was also under surveillance. Police later confirmed that they requested a court order to put Nicholson under surveillance as part of an investigation into the 2010 murder of prominent lawyer Ernest Valko.¹⁵ The British-born Canadian Nicholson had given Valko English lessons. Nicholson had also been instrumental in bringing the "Gorilla" corruption case to light.

A May 2014 blog post that appeared on the website of the *Pravda* newspaper, as well as off-the-record conversations with some investigative

¹⁴ Adam Valček, Štát špehuje ľudí aj bez súhlasu súdu (State spying on people without court's permission), *Sme.sk*, April 2, 2013. <http://tech.sme.sk/c/6754647/stat-spehuje-ludi-aj-bez-suhlasu-sudu.html>

¹⁵ Monika Tódová, Nicholsona policajti odpočúvali pre Valka. Zavraždeného učil angličtinu (Nicholson was under surveillance because of Valko. He taught the murder victim English), *sme.sk*, October 30, 2013. <http://www.sme.sk/c/6989646/nicholsona-policajti-odpocuvali-pre-valka-zavrazdeneho-ucil-anglictinu.html>

journalists, suggest that e-mail surveillance of journalists has also been conducted by unidentified individuals or bodies.

In the post, a blogger, Adam Kemény, published what he said were transcripts of an e-mail exchange between a journalist for the competing *SME* newspaper and two individuals – an actor and the spokesperson for the Nova political party.¹⁶

Tó Neutralita novinárov alebo čo má spoločné NOVA a SME (II. časť) (Neutrality of journalists or what links NOVA to SME? (Part II)) <http://adamkemeny.blog.pravda.sk/2014/05/22/neutralita-novinarov-alebo-co-ma-spolocne-nova-a-sme/>

Gorilla Tactics

Pressure to take down information from websites usually comes in the form of legal threats. Most notoriously, in the “Gorilla” case in 2011, a number of websites were threatened with lawsuits after posting alleged transcripts of phone surveillance conducted by the Slovak security services. The transcripts dealt with, among other things, alleged secret meetings between government ministers and Jaroslav Haščák, a representative of the influential Penta financial group. The documents, from 2005 and 2006, suggested close ties between representatives of several political parties and the business sphere. Haščák threatened legal action against the websites, many of which removed the transcripts as a result.¹

Though the documents spurred police to launch a corruption probe, including into the privatization of Bratislava airport and Slovenské elektrárne energy company, no findings have been released.

¹ *Matúš Burčík, TASR, Vargovo podanie na Facebook súd zamietol, Haščák svoje stiahne (The court dismissed Varga’s complaint on Facebook, Haščák will withdraw his complaint), March 2, 2012.* <http://www.sme.sk/c/6283446/vargovo-podanie-na-facebook-sud-zamietol-hascak-svoje-stiahne.html>

The alleged e-mails revealed an inappropriate and compromising closeness between *SME* and the party. The blogger had published several posts criticizing the Nova party and said he had “personal issues” with party leader Daniel Lipšic. The intelligence service denied that it had requested surveillance in this case. The Interior Ministry refused to comment.

As they do to obtain data, law-enforcement agencies must get a court order to conduct surveillance, or in urgent cases it can be granted by a prosecutor.

According to a parliamentary report for 2012, the latest available, police made 1,551 requests to conduct surveillance, of which 1,489 were granted, 62 dismissed. The information obtained was used in a trial in only 59 instances. Slovak intelligence agencies made 218 requests, with only two rejected. Military intelligence made 38 requests, all of them granted.

Cyberattacks are relatively rare in Slovakia. After the “Gorilla” case was made public, hacker groups allying themselves to the Anonymous movement attacked websites of political parties and of some business activities of the Penta group. No laws specifically target cyberterrorism.

The telecommunications infrastructure is not governed by a monopoly. Mobile, Internet, cable television, satellite, and radio broadcast services are provided by several usually private companies (the government holds 49 percent of the largest fixed-line and DSL operator, Slovak Telekom, but has virtually no influence on the company, which is controlled by majority shareholder Deutsche Telekom).

The state owns the frequency spectrum, which the media regulator awards to radio broadcasters in “beauty contests” based on criteria, such as media diversity, weighed by a jury, rather than competitive bids. Frequencies for digital terrestrial television (DTT), mobile, and other telecommunications are handed out by the Office for the Regulation of Electronic Communication and Postal Services. The only market ruled by a *de facto* monopoly is that for

DTT, where the telecoms regulator awarded all national frequencies to one player, Towercom. As DTT is used by about only 10 percent of households for TV reception, this cannot be considered a threat to the control of content.

State authorities do not have a policy on filtering or blocking online content.

In 2013, regulatory bodies and courts dealt with the issue of net neutrality. Local cable TV provider Antik Telecom launched SmartTVbox, a TV set-top box that uses a broadband connection (of any Internet service provider) to give access to real-time programming or on-demand services. Slovakia's largest cable operator, UPC, blocked Internet access for SmartTVbox, meaning that Internet users with a connection by UPC could not use the product. The telecoms regulatory body did not make a decision in the case, claiming the issue was outside its competence. Following an interim court ruling, UPC stopped blocking the set-top boxes in October 2013. A final court decision was still pending at the end of 2014.¹⁷

The case raised complex legal questions that have not been addressed by the law, among them the definition of Antik Telecom's service. The broadcasting council recognizes two types of Internet broadcasting – IPTV (for which the customer does not need Internet access) and Internet retransmission (which requires an Internet connection). The media regulator ruled that Antik's service did not fall under the IPTV category and was in fact Internet retransmission without a proper license – the operator had permission to provide TV programs only via traditional channels (i.e., cable, IPTV). Antik appealed this decision in court and was still waiting for a ruling at the end of 2014.¹⁸

Another question concerns the relationship between cable operators, their customers, and net neutrality, and whether operators can

legally block third-party hardware if it competes with their own services. UPC claimed that it blocked access to the SmartTVbox because it might limit the quality of service for other users, as online streaming is a data-heavy service. However, Antik's hardware works in a way that differs little from standard online streaming through websites or on-demand services such as YouTube.

The government of Slovakia has not weighed in on the debate spurred by the U.S. Department of Commerce's announcement this year that it would transfer key Internet domain name functions from the nonprofit Internet Corporation for Assigned Names and Numbers (ICANN) to some other organization or organizations, yet to be determined.

Nor is the government preparing for possible changes in Internet governance as ICANN's contract comes up for renewal next year. (As one of ICANN's fundamental missions has been to maintain the openness of the Internet, a possible transition to, for instance, a government-based model could have profound implications for Internet freedom.)

But the Slovak government has taken no stance on the Internet's future governance, as ICANN's contract could be renewed, and it believes the organization is not likely to be dissolved in any event. In a statement, the country's Finance Ministry was wary of pressure from states "outside Europe" to shift competencies from ICANN, and said governments should not have a more prominent voice in the Internet's administration than other interested parties. Any changes should serve primarily to "ensure the security of citizens and prevent or constrain illegal activities."

¹⁷ Martin Poláš, *UPC už prestal blokovať set-top boxy Antiku* (UPC stopped blocking Antik's set-top boxes), October 30, 2013. <http://medialne.etrend.sk/televizia/upc-uz-prestal-blokovat-set-top-boxy-antiku.html>

¹⁸ Rada pre vysielanie a retransmisiu, *Retransmisia cez internet a prostredníctvom IPTV* (Retransmission over Internet and IPTV), 2013. <http://www.rvr.sk/sk/spravy/?aktualitaId=2138>

LEGAL MAZE

3/5: *Transparency of legal procedures and appeals mechanisms*

4/5: *Copyright laws, fair use – laws and practice*

News, Commentary, and Copyright

Protection against Internet censorship is not covered by any regulatory body. Censorship per se is legally covered only by the constitution, which prohibits it. Audiovisual content that is broadcast online is subject to a certain extent to the same legal regulations as traditional broadcasting (especially age-restriction labeling and rules on differentiating between content and advertising). On-demand service providers and Internet broadcasters (including live streams of traditional broadcasters or online-only programming) do not need a license, but they must report basic information about their services to the regulatory body before launching the service.

Provisions concerning news objectivity and distinguishing between reporting and opinion that apply to traditional broadcasters do not apply to online audiovisual media. All these regulations are enforced by the Council for Broadcasting and Retransmission, whose nine members are elected by parliament, increasing the risk of politically biased decision-making.

Online content is legally protected the same way as any other creative content distributed by any other channel. Until 2013, one problem had been the exclusion of protection for “daily news” in copyright law. As a result, some companies providing online news monitoring services had been collecting content from print and online sources without paying the publishers and reselling that content to third parties. In 2013, the Copyright Act was changed to grant news and media outlets (in digital or printed form) standard copyright protection.

Online media have also been dealing with the problematic use of their photographs by Google. The search engine altered its image search interface to provide thumbnails of these images and direct links, allowing users to display or download the photographs without knowing who originally published them or what copyright restrictions apply (though a link to the original website is also provided in the search results). In Germany and France, Google has changed the image search interface so that users also see a preview of the website where the image originated. Google has been approached about this problem by the Internet Advertising Bureau in Slovakia. The company has since added a disclaimer to the search results informing users that copyright restrictions may apply.¹⁹

OPEN GOVERNMENT

3/5: *Quality of access to information legislation and Internet provisions.*

3/5: *Access on Internet to government and parliament decisions, court cases and decisions; right and speed of access to data through requests, and capacity of authorities to answer complex information requests.*

Tender Transparency

Slovakia’s Free Access to Information Act, passed in 2000, requires public institutions to provide requested information in written or digital form within eight working days (with a possible extension in certain “severe cases” of another eight work days). The act also requires various institutions to post online certain data, such as decisions, protocols, strategic documents of the parliament and government, and publicly funded contracts and related orders.

¹⁹ Tomáš Czwikovics, *Google z webov vyciava fotky. Proti sa ozvali už aj slovenské médiá (Google sucking photos from websites. Slovak media have raised their voice)*, *medialne.etrend.sk*, September 27, 2013. <http://medialne.etrend.sk/internet/google-z-webov-vyciava-fotky-proti-sa-ozvali-uz-aj-slovenske-media.html>

Political parties are required to post their annual reports on parliament's website and reports on their election spending on the Finance Ministry's website.

There has been no comprehensive analysis of public officials' responsiveness to freedom of information requests, but journalists and nongovernmental organizations face frequent denials when seeking access to information. Among the largest contracts to which Slovakia's government has denied access are those concerning the privatization of the former government-owned Slovak Telekom and those with PSA Peugeot Citroën, KIA Motors, and Hyundai Mobis, which included details about state subsidies. In all of these cases, courts later decided that the government was obliged to provide the requested documents (although not in their entirety).²⁰

Since May 2013, top officials have been discussing changes to give institutions more discretion in refusing requests in order to avoid what Prime Minister Robert Fico has termed the "bullying" of public institutions, and to clarify who is required to provide data, but no proposals have been released.²¹

The Open Data Index created by the Open Knowledge Foundation ranks Slovakia 61st out of 97 countries in 2014, with a below-average score of 345 out of 1,000. That rather negative assessment is questionable. For example, a category evaluating the availability of information on postcodes received a score of 20 percent on the grounds that the data are not publicly available, free of charge, machine readable, or available in bulk, none of which is true. The government spending category received a 10 percent score, although government spending is to a certain degree tracked by the Institute of Economic and Social

²⁰ Štát podľa súdu musí zverejniť privatizačnú zmluvu s Deutsche Telekom (The state must publish the privatization contract with Deutsche Telekom, says court), *SME*, December 10, 2005. <http://tech.sme.sk/c/2504524/stat-podla-sudu-musi-zverejnit-privatizacnu-zmluvu-s-deutsche-telecom.html#ixzz32AvT7doc>

²¹ Fico chce odstaviť infozákon (Fico wants to block the information act), *SITA/eTRENDSK*, May 29, 2013, <http://ekonomika.etrend.sk/ekonomika-slovensko/fico-chce-odstavit-infozakon.html>

Studies' *Cena štátu* (Price of the State) project, using publicly available data.²²

Standard government-run databases available online include the company register (incorporating a new register of financial statements); a cadastral map and land register; legislation (including the record of changes, official consultations, legal proposals, etc.); weather data; government and parliament agendas and decisions, including voting results and legislators' voting records (parliamentary debates are streamed live); and basic economic data provided by the statistics office (GDP, unemployment, etc.). The vast majority of the data are available online for free (including the company register, unlike in many countries).

Accessibility and usability of this data varies, with most restrictions linked to operating system or browser requirements. For instance, the cadastral map is accessible only on Microsoft's Internet Explorer.

Data are usually not available in bulk for third parties, though nongovernmental organizations have launched several online projects that gather publicly available information and make it accessible, for instance, with more advanced search features. They include *otvorenezmluvy.sk* (Open Contracts – a database of publicly funded contracts); *otvorenesudy.sk* (Open Courts – a database of court decisions); *Transparentní lekári* (Transparent Doctors – a database of marketing activities aimed at doctors); and others.

In 2010, the government of then Prime Minister Iveta Radičová passed a law that decrees that publicly funded contracts can become valid only after being published online. While the measure was a big step toward transparency in the use of public money, many documents are available in only scanned form, and are therefore not searchable. In many cases, institutions do not include certain details of the contracts, claiming they would disclose confidential trade information, although the law specifically defines which type of information can be considered a trade secret. Examples

²² <http://index.okfn.org/place/slovakia/>

of the kind of information that agencies controversially withhold include prices for TV broadcasting rights (such as for sporting events or foreign program licenses) and detailed budgets, listing instead only the overall price.

Interviews:

Peter Blaas, Business Development Director at Antik Technology
Press Bureau of the Department of the Interior of the Slovak Republic

Legislation cited:

Act on Broadcasting and Retransmission (Act no. 308/2000 Coll.)
Code of Criminal Procedure (Act no. 166/2003 Coll.)
Act of the National Council of the Slovak Republic (Act no. 171/1993 Coll.)
Act on Electronic Communications (Act no. 351/2011 Coll.)

NOTE ON METHODOLOGY:

The four country reports were drawn up based on a common methodology, with a set of questions for each section. The research teams' scores were drawn up by the analysts in the respective countries, peer-reviewed in-country, reviewed by Transitions Online and PASOS, then subject to a final comparative peer-review across the four countries.

The scale for each question is from 0 to 5, where 0 indicates no openness/freedom at all, and 5 indicates maximum degree of openness. For each score, researchers were asked the following questions:

- *Is the body of laws/regulations/practice optimal/not needing any reforms to protect freedoms on the internet?*
- *Is the body of laws/regulations/practice generally adequate to protect freedoms on the internet?*
- *Are there significant gaps in the given area, where it is necessary to introduce and implement changes/statutory reforms to sustain*

open government/protection of freedoms/protection of privacy/clarity and transparency of legal framework?

- *Is there a serious lapse in open government/protection of freedoms/protection of privacy/clarity and transparency of legal framework?*

The score (0-5) was assessed for each of the following questions within the four main chapters:

Section 1: Freedom of Expression

Freedom of expression on the Internet – laws, definitions, and de facto regulation

- *The legal framework and instances of prosecutions entailing denial of freedom of expression.*
- *Legal rights and protections for online expression and their status compared with print and broadcast rights.*
- *Cases of bloggers or online journalists being prosecuted, fined, or jailed for defamation or libel.*

Section 2: Big Brother

- *Censorship – laws and implementation, and pressure-group activity, including requests to remove material.*
- *Filtering and blocking of Internet content by state and other actors.*
- *Published information on government surveillance/tapping – by government and by private companies.*

Section 3: Legal Maze

- *Transparency of legal procedures and appeals mechanisms*
- *Copyright laws, fair use – laws and practice*

Section 4: Open Government

- *Quality of access to information legislation and Internet provisions.*
- *Access on Internet to government and parliament decisions, court cases, and decisions; right and speed of access to data through requests, and capacity of authorities to answer complex information requests.*

This study was written as part of the project, **Internet Freedom Report 2014: Visegrad Four**, a project of Transitions (TOL) and PASOS (Policy Association for an Open Society). The preparation of the reports was supported by Google. The reports were prepared with full research independence and the views expressed herein are views of the authors only (and not of Google).

The research is based on detailed analysis of the current situation - in law and in practice - using a methodology that examines Internet Freedom by looking into four main areas, namely *Freedom of Expression*, *Big Brother* (surveillance, regulation, and interference by the state), the *Legal Maze* (the clarity of the legal framework in terms of its letter and practice), and *Open Government* (transparency and online disclosure by government of its functioning and decisions, such as budget information and tender contracts).

The study, **Internet Freedom 2014: Visegrad Four**, was conceived with a view to raising the public profile of Internet freedom and censorship issues in the Visegrad countries within the region and internationally. Further objectives included the aim of addressing governments in the four countries to persuade them to take a consistent, open approach to Internet freedoms and transparency of government on the Internet, and the generation of empirical-based input to consultations in the European Union on digital rights and Internet freedom. The project also provides a template for evaluating and monitoring Internet freedom over time.

Internet Freedom 2014: Visegrad Four, compiled by independent think-tanks in the four countries, is the result of a project led by Transitions (TOL) to a methodology designed by PASOS (Policy Association for an Open Society). The participating think-tanks were the Association for International Affairs (AMO), Czech Republic, the Center for Media & Communication Studies, School of Public Policy, Central European University, Hungary, the Institute of Public Affairs (IPA), Poland, and the Institute for Public Affairs (IVO), Slovakia.

This publication has been peer-reviewed, but the final text is the responsibility of the authors. The publisher confirms that this policy analysis has been prepared in accordance with the PASOS principles for effective quality controls in the work of independent think-tanks.



The Institute for Public Affairs (IVO), Bratislava, is a leading independent think-tank in Slovakia.

Institute for Public Affairs (IVO)
Baštová 5, 811 03 Bratislava, Slovak Republic
Tel + 421-2-54 43 40 30/31
Email: ipa@ivo.sk
www.ivo.sk

PASOS (Policy Association for an Open Society) is a network of independent think-tanks working to strengthen participatory policymaking at the local, national, and international level.

PASOS
Těšnov 3, 110 00 Praha 1, Czech Republic
Tel: +420 2223 13644
Email: info@pasos.org
www.pasos.org

Transitions (TOL) is a publishing and training organization with a mission of strengthening the professionalism, independence, and impact of the news media in the post-communist countries of Europe and the former Soviet Union.

Transitions
Baranova 33, 130 00 Praha 3, Czech Republic
Tel: +420 222 780 805
Email: info@tol.org
www.tol.org