Responsibility of Tech Companies
Operating in Authoritarian Regimes: Belarus

Analytical paper by Human Constanta
December 2022

Contents:

Introduction

As the practices of digital authoritarianism are spreading and autocrats are attempting to hold an even tighter grip on Internet freedoms, it is crucial that tech companies, especially tech giants who are widespread across autocracies and democracies alike, are not using a "one fits all approach" to the countries they are operating in. It is essential that businesses are sensitive to the political environment they are choosing to operate in and the malicious ways the governments may be seeking to exploit them.

It is not uncommon for state propaganda to create its Youtube channels, Instagram pages, or Telegram bots. Such outlets were then used to spread disinformation or intimidate civil society. The activity of citizens using social media accounts on big tech platforms is often monitored, while the companies may be pressured to share the data about its users with the state.

Belarus is notorious for its repressive digital practices. Since the Belarusian presidential election in 2020, Belarus has been experiencing the largest political and human rights crisis in its modern history. The election itself was manifestly fraudulent – with opponents of Alexander Lukashenko, who has been *de facto* in power for almost 28 years, being imprisoned and forced out of the country. Peaceful protests that followed were violently dispersed – tens of thousands of people were arrested and detained, thousands sentenced to real prison terms, and more having to leave the country and seek refuge. The number of political prisoners in Belarus continues to grow daily and amounts to 1447 people as of December 2022.

Civil society has been hit hard by the wave of political repressions. At least 667 civil society organizations are in the process of liquidation (disbandment) by the authorities as of October 2022. The newly amended Criminal Code made "working on behalf of an unregistered or liquidated organization" a criminal offense, punishable by up to 2 years of imprisonment.

Since the Russian invasion of Ukraine on 24 February 2022, escalating the ongoing armed conflict, digital space has been increasingly used to spread propaganda and silence anti-war voices.

The trends towards not just "analogue," but digital authoritarianism are vivid and increasingly more dangerous in Belarus. The regime does not shy away from resorting to Internet shutdowns, censorship, spreading disinformation and propaganda, hacking into accounts of activists, monitoring and persecuting online speech. The civil society is forced to navigate the shrinking space it operates in. A better understanding of such context by the platforms would help formulate a more tailored approach to the challenges of Belarus and the region, in line with the companies' obligations in the field of business and human rights.

In the wake of the protests, the authorities used imported DPI equipment to implement Internet shutdowns, as well as software to identify protestors. Belarusian authorities used to be able to disseminate forced confession videos of arrested activists, clearly filmed under pressure, as Youtube ads. The practice of disseminating such videos continues on Telegram channels, even as repeated attempts to delete such channels are made. The newly adopted laws oblige online service providers, such as messengers, taxi apps, or marketplaces, to retain data about their users and share it at the state's request.

While some businesses successfully resist the state pressure, others are yet to figure out the strategies of operating in authoritarian regimes, while complying with their human rights obligations and not enabling the dictators in their pursuits to control online spaces.

The present paper seeks to identify the problems associated with tech companies functioning in authoritarian regimes – specifically, in Belarus, as well as to put it in the framework of existing human rights obligations of businesses. By drawing a general picture of the digital rights landscape we hope to inform relevant stakeholders – tech companies and corporations, digital rights activists, and international organizations – and inspire advocacy on the matter. The contributors to the ideas laid out in this paper include Access Now, Belarusian Helsinki Committee, Press Club Belarus, Reform.by.

1. Problems identified

A. Human rights violations committed via resources of platforms

Since the beginning of post-electoral 2020 political and human crisis in Belarus the main forms of human rights violations committed via resources of platforms are so-called "confession videos" – that is, footage of detainees, forced to confess crimes against the regime, which they did not commit. Often people are forced to record such videos under pressure or following torture and other inhumane and degrading treatment. Such videos violate the right to be free from torture, the right to privacy, the freedom of expression, and constitute discrimination on political grounds. There are cases when such videos feature representatives of vulnerable groups, adding an additional layer of human rights abuse: LGBTQ+ (who, in addition to forced confessions are forced to publicly declare their sexual orientation) and children. Publishing such videos is common practice of Belarusian law enforcement agencies. The videos are distributed via different open Telegram and Youtube channels of state's media, pro-state bloggers and are an inalienable part of Belarusian propaganda.

In January 2022, Belarusian Helsinki Committee sent a letter to Telegram as well as to Apple and Google (as Telegram in their supply chain) in respect to such videos, recorded with

LGBTQ+ people with detailed description and the list of channels, where the videos were posted. In May 2022, Belarusian Helsinki Committee applied to the same platforms in respect to such videos, recorded with children.

B. Safety of users in Belarus

Along with general cyber threats and privacy concerns which are relevant to the majority of users worldwide there are risks and incident patterns specific for authoritarian regimes and particularly for Belarus. Vague 'anti-extremist' regulation is being used to ban not only activities of independent media and civil society initiatives but it is also widely used to prosecute their supporters and contributors. Sharing, likes, commenting and other interactions with extremist-labeled accounts can be considered as a criminal offense. Unfortunately, even the unique high-tech privacy and security settings of popular social networks and messengers do not meet the conditions of a full-scale online prosecution of dissenters by the Belarusian regime.

During detentions and searches, personal electronic devices are routinely confiscated by the security forces and disconnected from the Internet connection, which allows the security forces to get long-term access to personal correspondence, even if the user has set a timer for automatic deletion of messages. Some messengers do not provide a message deletion function for all chat participants, others have implemented the function of canceling the sending of a message only for a short period of time after sending – this does not allow users to delete sensitive messages in case of detention of one of the conversation participants. The privacy settings of some messengers, such as Signal, do not allow the user to hide the phone number to which the account was registered, which allows the security forces to identify the user even though there is no access to any other personal data. Many applications, such as Slack, leave sensitive information in the form of a cache or other residual files with unprotected access, even if the user has logged out of the application's account, and sometimes even if the application has been deleted. Some messengers, such as Telegram, leave traces of registration in chatbots, even after the bot is stopped. The situation with digital security is seriously aggravated by the widespread practice of law enforcement agencies of using psychological and physical violence in order to force a person under duress to give out all passwords or log into applications of interest to law enforcement agencies.

It is crucial that the companies' approach to security takes into account risks specific to authoritarian context. The ability to quickly delete and conceal data at the time of politically motivated prosecution is often the question of dissenters' liberty.

C. Equal approach to civil society oriented services

Google for Nonprofits is a service that allows non-profit organizations to collaborate more effectively through the coordinated use of apps like Gmail, Docs, Calendar, Drive, and

Google Meet at no cost. Using Google for Nonprofits allows grassroots initiatives, as well as local and regional civil society organizations to operate in a more professional and structured way. Google for Nonprofits is launched in 68 countries, including all immediate neighbors of Belarus. No specific reasons are indicated for not offering the service in Belarus. One may argue that the pressure exerted on the civil society in Belarus may be one of the reasons for not launching Google for Nonprofits. At the same time, the service remains available in Russia – Belarusian neighbor, notorious for pressuring civil society organizations, including through the use of its "foreign agents" law. It is important that there is dialogue on specific ways to support civil society in Belarus and which technical solutions can build resilience in countries with shrinking civil society space.

D. Propaganda, censorship and downrating of independent Belarusian media websites

Since Russia started war in Ukraine, Belarus has been used as a proxy to promote Russian disinformation. Whilst in response to Russian military aggression in Ukraine, many Russian online outlets (websites, social media accounts, Youtube channels) were marked by the platforms as state-owned and controlled to make sure the audience is able to distinguish between independent and non-independent sources of information, no similar approach was taken in case of Belarusian state media. For example, a news report by Belarusian State TV company about events in Bucha, Ukraine, has around two million views on Youtube and targeted Russian speakers in Ukraine, Belarus, Russia and other post-Soviet states. *Marking state-owned and controlled media, including not just major ones, but regional ones, would allow Belarusian audiences to filter through layers of propaganda and receive verified information from trusted sources.*

In the aftermath of the 2020 presidential campaign, many independent media outlets in Belarus are blocked by the authorities, including being arbitrarily designated as "extremist", creating criminal liability for those who share or repost content. Blocked websites are accessible through VPNs or have mirror services. However, unsuccessful attempts by users to reach the blocked websites lead to their automatic downrating by the Google search engine algorithms or services like Google News and Google Discover. Hence, state-owned and controlled outlets or foreign (e.g. Russian) outlets, commenting on the same news piece are being promoted automatically. *We believe, perhaps, this problem could be partially resolved by "allow lists", which would include the independent media outlets blocked inside the country.*

Another serious concern is linked to content localisation. Google News and GoogleDiscovery could consider the option to prioritize Belarusian news resources, including in Belarusian, for those who search for news inside Belarus. That is, so that Belarusian media competed among each other, but not with the Russian media. This could help fight the systemic dissemination of Russian manipulative narratives among Belarusian audiences. The problem of localizing Belarusian-made content for Belarusian has been regularly raised with Google by the

Belarusian independent media sector since 2019. *It is vital that algorithms help promote outlets created by Belarusians for Belarusians.*

E. Dialogue between platforms and Belarusian civil society

While the present opportunity of voicing concerns of Belarusian civil society to online platforms is valuable, there is no sustainable platform on which similar concerns can be regularly brought up and acted upon. Belarusian digital landscape is highly affected by the repressive politics of the regime and such practices pose a challenge to Internet freedoms in the region and in the world. Making sure that Belarusian digital rights watchdogs and other human rights organizations have a chance to regularly inform platforms of the new challenges and discuss possible solutions beyond *ad hoc* events would help companies keep an eye on the tightening grip of digital dictatorship in the region and reply accordingly, in line with applicable human rights obligations of all actors involved. It's also important to say they big tech companies may also benefit from collaborations with Belarussian human rights organizations and civil society representatives. As big tech employees are not located on Belarus and not aware of exact circumstances in the country, they might be lacking local contexts. Building ongoing dialogue, and consequently, trust between big tech companies teams and local human rights organizations might lead to better and more efficient results.

F. Bridging local legal compliance and human rights centered approach

While it is reasonable to expect companies to comply with local laws of the states they are working in, there is a challenge when it comes to companies' operating in authoritarian states with repressive laws and policies. For civil societies of such countries, including Belarus, it is crucial to know the platforms' strategies and stance on cooperating with the authorities and the level of compromise the platforms may be willing to take to remain active in such jurisdiction. Given the amount of users' data shared on the platforms, it is also crucial to know how secure such data is, if companies are faced with pressure from authoritarian governments.

G. Belarusian-language content and its moderation

Belarus is a country with two equally official languages – Russian and Belarusian. However, for the purposes of Google services' reach, Belarus is sometimes regarded as part of the Russian-language segment of the digital market rather than a separate country. Such *status quo* renders it impossible for Belarusian-language Youtube content to get properly moderated and prevents content-creators from benefiting from Google Ads services, making it harder to grow an audience for creators, who speak Belarusian, and disincentivizing them from creating content.

The question of lack of rationale for gatekeeping Belarusian content has been raised by Belarusian activists:

- The petition to add the Belarusian language to Google Ads has collected more than 21 000 signatures.
- The Declaration on the Need for Geographical Localization of Internet Services and Recognition of the Belarusian Segment of the Internet as a Separate Market was signed by 16 key representatives of the media community in Belarus, some of whom are now political prisoners. The Declaration states, *inter alia*, that "Internet corporations' unwillingness to offer services localized for Belarus … has a direct impact on Belarus' information sector and violates our country's information sovereignty."
- The Assembly of Delegates of PEN International, meeting at its 85th annual Congress in Manila, Philippines have mentioned in their Resolution on the Belarusian Language that "Belsat TV, the first and only independent [TV] channel in Belarus, currently plays a key role in popularizing Belarusian and offering alternative content. Yet Belsat TV is unable to place advertisements promoting videos in Belarusian on its YouTube channels, as Google Ads does not support the Belarusian language. This greatly affects Belsat TV's attempts to expand its audience and disseminate independent and reliable news in the Belarusian language."

When the issues of the impossibility of moderating Belarusian language content or placing Belarsuian-language adds with Google were brought before Google representatives by a Belarusian-language activist and now a foreign policy advisor to Sviatlana Tsikhanouskaya Franak Viacorka, Google Moscow employee responded that "all videos in Belarusian, Tatar, Kazakh, and other "indigineous" or "small" languages are limited for the purposes of paid promotion" since "the company cannot afford to promote them." When Viacorka asked the Google representative about what he was supposed to do in such a case, the latter recommended Viacorka "to create content in Russian." Such situation demonstrates a borderline "neocolonial" attitude to content created in languages other than those dominant in the region, despite the needs of millions of people who speak, create, and consume content in Belarusian, Tatar, and Kazakh languages, summarily swiped under "indigenous" label by the Google employee, let alone other languages. At the same time, no problems with content moderation in national language is reported by countries with a far smaller population than that in Belarus or Kazakhstan – *e.g.*, Georgia, Lithuania, Latvia, or Estonia.

2. Notable cases

Kipod

"Kipod" facial recognition software developed by Synesis company and operated in Belarus by "24x7 Panoptes" is a recent example of the tool adapted by the Belarusian authorities to track dissidents. The algorithm became integrated into the Republican Public Safety

Monitoring System after winning the tender for the selection of the technical operator for this national system. “Kipod” technology became infamous due to its use for the prosecution of dissenters (for instance, to arrest a popular opposition activist Nikolai Dedok).

Abovementioned company is a subsidiary of Synesis — a notorious Belarusian software developer, which was included in the European Union, United Kingdom and the United States sanctions lists for providing Belarusian authorities with the video surveillance platform and aiding therewith the state in repressing the civil society and democratic opposition.

Sandvine

During the rigged elections in Belarus on 9 August 2022, as well as during the peaceful protests that followed them, the government of Belarus regularly restricted access to most of the Internet traffic throughout all the territory of Belarus. According to the Bloomberg investigation, the Belarusian regime used equipment manufactured by the U.S.-based company Sandvine to conduct Internet shutdowns. The company specializes in the production of deep packet inspection (DPI) equipment, which is used to monitor and filter network traffic. Citizen Lab in its report stated that the company's technologies are used around the world not only for legitimate purposes (for example, detecting spam and other malicious activities), but also for blocking political, human rights and news content, for example, by the government of Turkey and Egypt. Such equipment was obtained by Belarus’s National Traffic Exchange Center as well.

After the Bloomberg investigation as well as after advocacy of Access Now, Belarusian diaspora, and U.S. Senators condemning the use of Sandvine’s equipment to implement shutdowns, the company announced the termination of the deal with Belarus. The representative of Sandvine stated that the reason for the termination is the fact that the Belarusian regime used the company’s products to obstruct the free flow of information during the elections in Belarus and in general to violate human rights. With the withdrawal from the agreement, the company would stop providing software updates and technical assistance for its hardware.

A1

Belarusian Internet provider A1, a subsidiary of the Austrian company A1 Telekom Austria Group, regularly reduced the capacity of the 3G network in Minsk during all mass protest marches held in the city in 2020. According to the company's reports, access to the Internet actually was completely restricted “at the request of state bodies in connection with ensuring national security.” On 16 March 2022, the Open Society Justice Initiative submitted a complaint before the Organization for Economic Co-operation and Development (OECD) concerning Telekom Austria’s contribution to Belarus’ internet shutdowns, which contravened its responsibilities under the OECD Guidelines for Multinational Enterprises, particularly concerning human rights due diligence. The legal initiative in its appeal proposed a number of measures to remedy the situation that can be taken by Telekom Austria in connection with the Internet outage in Belarus in 2020. In particular, the initiative requested the “establishing a network and fund of technology companies to promote internet freedom and address the challenges emerging in authoritarian systems;" the creation of an operational system for filing complaints for legal remedies for affected people and relevant stakeholders; the creation of a fund for the work of the Belarusian diaspora to monitor and promote Internet freedom and other measures.

Forced confessions videos

Since 2020, the practice of publishing "confession videos" on pro-government resources close to law enforcement agencies, in particular to the Main Directorate for Combating Organized Crime and Corruption (GUBOPiK), has been expanding. In these videos, the security forces, using physical and psychological pressure, force the detained people on camera to admit their guilt in committing actions against the Lukashenka regime, as well as to declare support for the current regime and urge viewers not to participate in opposition activities. The researchers also note the strengthening of discriminatory and hate-fueling narratives in the Belarusian state media as a whole.

In January 2022, the Belarusian Helsinki Committee (BHC) appealed to Telegram, Apple, Google in connection with the dissemination by the Belarusian authorities through Telegram of materials violating human rights and containing radical forms of hate speech. In May 2022, the BHC asked the heads of Telegram, Apple, Google to respond to the facts of violations of children's rights in the Belarusian segment of Telegram: the organization indicated that channels affiliated with the Belarusian regime regularly posted "confession videos," including with the participation of minors. In March 2022, the People's Anti-Crisis Management (NAU) sent to YouTube and Google a list of representatives of Lukashenka's propaganda and the materials they create, as well as a legal justification for blocking their channels. Other civil initiatives content, such as the "Stop Propaganda" community, also involved in efforts to block propaganda by consolidating people to send complaints to the managers of popular social networks about human rights violating content.

On 14 June 2022, as a result of appeals of civil society, Telegram completely removed most popular pro-government channels "Желтые сливы" ("Zheltye slivy") and "Ваши сливы" ("Vashi slivy") involved in human rights violations. Moreover, based on the efforts of activists, in 2022 Telegram blocked more than 20 channels close to GUBOPiK. Facebook and YouTube have blocked the accounts of the most odious propagandist Grigory Azarenok, infamous for his speeches inciting hostility.

3. Obligations of tech companies in the sphere of human rights

In international law there is a clear legal framework of the obligation for business enterprises to tackle adverse impact on human rights. The universally recognized global international standard in the field of human rights and business is the United Nations Guiding Principles on Business and Human Rights (UNGPs), adopted by the UN Human Rights Council in 2011. Principle №17 stipulates that in order to identify, prevent, mitigate and account for how they address their adverse human rights impacts, business enterprises should carry out human rights *due diligence*. The process should include assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed.

Experts emphasize the important role of enterprises in the field of digital technologies in assessment of the impact of their commercial activities on human rights which is recognized as a key component of corporate responsibility in the field of human rights due diligence. In this regard the Danish Institute for Human Rights has developed a practical guide for businesses and other actors on how to assess the impact of digital activities on human rights.

4. Recommendations

- **General recommendations to Big tech as to exercising human rights due diligence and risk assessment in authoritarian regimes (including Belarus):**
    - Pay special attention to the human rights due diligence and conduct more detailed impact assessment in line with obligations in the field of business and human rights taking into consideration specific risks;
    - Consider the possibility to formulate special appropriate strategies of operating in authoritarian environment upon consultation with civil society local actors;
    - Exercising human rights due diligence of activities in/under jurisdiction of the authoritarian regime in Belarus, aggravated by the political and human rights crisis in 2020-2022 it is important to **take into consideration following factors**: dependence of all institutions in the country on the authorities; the absence of the independent court and other elements of the division of powers; using of business (public and private) by the authorities as a tool to achieve political goals; using legislation for achieving political goals and increasing the dependence of a person on the State; constant and large-scale pressure on civil society, including mass media, lack of free access to necessary information (including asses to the texts and justification of draft laws, restricting human rights); lack of possibility for people to participate in public affairs and influence political decisions of authorities; a high degree of personification of power which leads to high extent of unpredictability of state's policy;
    - While conducting human rights risk assessment organize regular communication with local civil society actors and digital rights activists to exchange information on the changing digital rights landscape and ways to minimize risks for the users and for the company;

  - Support civil society by providing tools and solutions to activists on equal basis and supporting local activists in developing local civic tech tools;
  - Prioritize human rights consideration in taking decisions, when working in authoritarian states and inform civil society and general public on the measures taken to preserve users' security and privacy in such contexts;
  - Reflect human rights abuses and violations, conducted by state-owned and controlled accounts in authoritarian regimes in non-financial reporting, as well as the measures taken to overcome such risks and demand the same from your partners.

- **Operational measures platforms can take to better protect rights and freedoms of users in Belarus:**
  - Recognize Belarus as a separate market segment and make sure that independent content in Belarusian is properly moderated and is not perceived as part of the Russian segment of the market;
  - Ensure that content of Belarusian independent media is not pessimized and not overtaken by Belarusian governmental and Russia media, even when such media are blocked or otherwise censored by the regime, by analyzing and working on algorithms;
  - Clearly mark state-owned and controlled accounts and channels as such, making sure the audience can draw a distinction between independent and non-independent sources of information; As well as marking such accounts with a warning of possible human rights violations;
  - Provide additional informing (special notes of warning) users of state-owned and controlled accounts about the unacceptability of using the means of platforms for actions, violating human rights;
  - Take into consideration that "confession videos" and radical forms of hate speech towards opponents of the authorities, disseminated by state-owned and controlled channels, are not rare incidents but purposeful and conscious policy of the state. These channels are created not with the purpose of realizing freedom of expression and/or informing the public about public authorities activities, but with the purpose of intimidation and propaganda. That is why these accounts can not be protected by freedom of speech standart. In this respect the preferred course of actions in respect to such cases is not just blocking some materials, but deleting the accounts themselves.