Committee: Special Conference on Cyber Governance

Issue: The rise of digital authoritarianism

Student Officer: Ariadne Lampropoulou

Position: President

INTRODUCTION

Nowadays, governments all over the world enact personal data protection laws and make use of "fake news" claims in order to control people's views and opinions, but to also limit citizens' trust in the internet. The limitation of internet freedom has a severe impact on our democracies that face many challenges in the digital era.

A recent research showed that many governments worldwide have been troubled by fake news. In an attempt to deal with this problem, they have passed legislation to fight propaganda. Although, at first, this may appear to be an effort to the right direction, most of these governments are authoritarian. In addition to the above, certain governments have their own trolls that feed social media with the news that support or promote said government.

Moreover, the fact that people in countries are made to believe they are under constant threat by terrorists and extremists minimizes their resistance to state control and gives their government the power to use technology, such as facial recognition, to gather information and use it for any purpose it deems appropriate, whether it is ethical or not. Authoritarian states may vote laws which "appear" to protect the interest of their people but in reality, they are only passed to limit the freedom or even persecute those that speak against them.

DEFINITION OF KEY TERMS

Fake news

Fake news means that someone intentionally misinforms the public through all forms of traditional mass media (e.g. newspapers, radio, television), as well as social media. Those feeding the media with fake news are sometimes paid to act this way by third parties.

Data protection laws

Data protection laws means all laws enacted, in order to protect the sensitive data of individuals. In particular all EU countries have harmonised their legislation with Directive 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free [1]movement of such data with the aim to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

Authoritarian state

Authoritarian state is a state where the power is held by the leader (e.g. prime minister, president, etc) and a small group of people who enjoy his trust and support. The citizens are expected to follow, without questioning, their orders.

Propaganda

Dissemination of information, news, etc., that are not objective or true but aim at influencing the public, in order to promote certain policies, politics or achieve certain goals. Propaganda is a word with negative connotation.

Troll

A person who purposefully disseminates information on social media that is not true or is upsetting with the aim to create controversy.[2]

BACKGROUND INFORMATION

How has the internet worked so far?

The internet is comparatively recent. Most users had been brought up in an era where information was disseminated by newspapers, television and the radio. Said media had a very clear political standview so everybody knew, when getting a piece of information from a specific source, how biased it was. And then came the internet. In the beginning people treated it the same way as the traditional media. They thought that whatever they read on a website was objective and true. However, being completely free and open to all people the

[1] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32001R0045
[2] https://dictionary.cambridge.org/dictionary/english/troll

internet started to be used for uploading fake information. Unlike newspapers where all articles are signed the internet was full of news feeded by people who couldn't be traced. Anyone could write anything without being held responsible for it because most of the times that person couldn't be located. Soon, governments realised what a powerful weapon they had available. Thus they started to use social media to influence the public into supporting their policies, blindly following their proposals and reelecting them. For example, a policy posted by a member of a government on Facebook would be liked and commented on by trolls employed by the government itself. This way, the public was influenced and people were made to think that a vast majority of the population supported the government's policies. Certain governments even use trolls who attack those who question their policies and create animosity amongst people.

The internet nowadays

Concerning the internet nowadays, a big debate has started about how the internet is manipulated by governments. In the 2016 US Presidential Election, the Kremlin tried to influence the vote of the American people. In its effort to do so, the Russian intelligence used trolls who tarnished the image of Hillary Clinton, by spreading the fake news that she had connections with Islamic extremists and that her health as well as her mental capacities were not in a good state.

Another example that clearly manifests the problem is the Cambridge Analytica Scandal, where Mark Zuckerberg of Facebook sold the personal data of millions of users, to Cambridge Analytica, a company that worked on the Trump Campaign.

Western countries, including the European Union have passed personal data protection laws in an attempt to regulate the framework for the collection, processing and distribution of information collected by companies in their everyday cooperation with individuals. According to the GDPR all companies that have access to personal information need to keep records of their processing and need to ensure that the information they hold is not transferred to other organisations. People whose data have been collected have the right

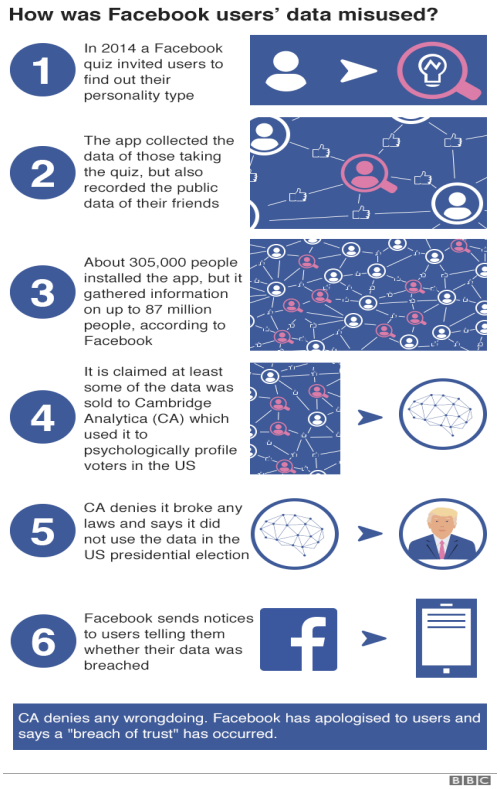

Figure 1: How Facebook users' data was misapplied

to receive a copy thereof. Companies need to collect data in a lawful and transparent manner after receiving explicit consent (in the case of children under the age of 16 the relevant consent needs to be given by the parent or guardian) from the individual whose personal information they request and have to make sure that said information is not kept for longer than it is absolutely necessary. Said consent can, at any time, be revoked. A member or members of the staff have to receive appropriate training on the handling of personal data and big companies appoint a GDPR manager who is responsible for the day-to-day handing of personal. People need to be assured that their personal information shared with a specific company for a specific cause (e.g. passport details disclosed to an airline or airport) will not be disclosed or sold to any other company, organization or country for whatever reason. For example, someone's hospital record should never be shared with insurance companies because that would give the latter a benefit when drafting a contract or proposing a policy to that specific individual.

What is yet to come?

If strict observance of very specific rules is not guaranteed things might get out of hand in the very near future. Citizens need to be assured that whatever information they upload from their eye retina scanned at airports to their political views shared on social platforms, such as facebook, will be protected. If an organisation or a nation can get hold of all of this their power over people's lives will be uncontrollable.

Furthermore, the information uploaded needs to be somehow controlled. This is very sensitive and difficult because we must, at all expense, avoid censorship. But letting manipulated or biased or bogus information to be shared may very easily provoked hostilities amongst different religious, racial and other groups of people causing uprising and wars.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

China

In 2018 China has been found to be the greatest abuser of internet freedom. It has come in contact with governments in countries where human rights are not properly observed and has used technology to exploit information. Moreover, media officials have been held from a multitude of countries for fortnite seminars on its sprawling system of suppression and surveillance.

Bangladesh, India, Sri Lanka, Myanmar

The past year there were damaging outbreaks of roughness opposed to ethnic and religious minorities due to fake rumors and detestable propaganda. These breaches usually benefit anti-democratic forces in the government and society, which, through manipulation, actively uplifted them.

Russia

As well as more repressive states expect all of their citizens' information to be stored inside their borders, so all data can be available to be found by security agencies.

Egypt and Iran

Egypt and Iran enacted media laws with the aim to restrict social media, imprison individuals who opposed their policies and disrupt communication and connection with social media of other countries.

TIMELINE OF EVENTS

Date	Description of Event
24 October 1995	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[3]
14 April 2016	The General Data Protection Regulation (GDPR) is approved by the EU Parliament.
2016	Kremlin tries to interfere with the US election.
March 2018	Christopher Wylie, employee of Cambridge Analytica came forward and disclosed information relating to the scandal.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en

25 May 2018	The General Data Protection Regulation (GDPR) is enforced and organization in breach could be fined.
July 2018	Cambodia arrests and imprisons a number of citizens for online speech.
2018	China was found to be the worst abuser of internet freedom.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

The rise of digital authoritarianism is one topic of great importance which asks for quick and immediate response. Therefore, numerous measures have taken place. Primarily, once China had been found to be "the worst abusers of internet freedom" throughout 2018, its government responded by choosing to host fortnite long seminars on its sprawling system of suppression and surveillance from a multitude of countries. Moreover, democracies had been recognized as slow when it came to responding to crises. This meant that their systems of balances as well as checks and public engagement were not conducive to quick decision-making. However, a built-in caution has allowed some semi-democratic countries to fend off authoritarian-style internet controls. Lastly, it must be remembered that over 500 million citizens in the European Union obtained more rights in May 25 for their personal data as part of the GDPR (General Data Protection Regulation).

POSSIBLE SOLUTIONS

Despite solutions having taken place already concerning the issue of the rise of digital authoritarianism there are, a number of possible solutions. In order for democracy to be kept safe from harm, making sure that internet freedom against the rise of digital authoritarianism is secured, is vital. All citizens must be authorized by technology, in order to be able to make their own economic, political but also social decisions. This of course, must be done without any sort of manipulation from anyone. This must be ensured as the web is now known as a modern public sphere, and both social media and search engines have huge power and responsibility to make sure that their platforms only serve good to the public.

Moreover, a secured private sphere is needed for democracy. The unrestrained collection of personal data limits a person's right to a private life which is what democracy is all about. This problem needs to be dealt with jointly, meaning by governments, companies and societies in general. All these stakeholders need to define the framework for proper collection, processing and distribution of personal data. However, the stakeholders must also

put a limit to abuse of social media platforms. Individuals must also have tools in order to be able to protect their lives and personality from the state and enterprises. Digital freedom is and should remain the opposite of digital authoritarianism. All we have to do is find the tools to ensure this.

BIBLIOGRAPHY

General Bibliography

Burkeman, Oliver. "Forty Years of the Internet: How the World Changed for Ever." *The Guardian*, Guardian News and Media, www.theguardian.com/technology/technology+content/interactive.

Shahbaz, Adrian. "The Rise of Digital Authoritarianism (2018) - DME for Peace: Design, Monitoring and Evaluation for Peacebuilding." *DME for Peace | Design, Monitoring and Evaluation for Peacebuilding*, 2018, www.dmeforpeace.org/resource/the-rise-of-digital-authoritarianism-2018/.

"Lex - 31995L0046 - EN." *EUR*, OPOCE, eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A31995L0046%3Aen%3AHTML.

Shahbaz, Adrian. "Freedom on the Net 2018: The Rise of Digital Authoritarianism." *The Rise of Digital Authoritarianism | Freedom House*, 16 Nov. 2018, freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism.

Gent, Edd. "Digital Authoritarianism Is Rising. Here's What That Means." *Singularity Hub*, 16 Nov. 2018, singularityhub.com/2018/11/23/digital-authoritarianism-is-rising-heres-what-that-means/.

"Russia, Trump, and the 2016 U.S. Election." *Council on Foreign Relations*, Council on Foreign Relations, www.cfr.org/backgrounder/russia-trump-and-2016-us-election.

Chang, Alvin. "The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram." *Vox*, Vox, 2 May 2018, www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram.

"GDPR in a Nutshell: Everything You Need to Know." *CFPro Financial & Business Management Services*, cfpro.co.uk/gdpr-in-a-nutshell-everything-you-need-to-know/.

Pictures, graphs, etc.

"Facebook Fined £500,000 for Cambridge Analytica Scandal." *BBC News*, BBC, 25 Oct. 2018, www.bbc.com/news/technology-45976300.