

HUMAN RIGHTS,
DEMOCRACY
AND THE RULE OF LAW

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

DROITS DE L'HOMME,
DÉMOCRATIE
ET ÉTAT DE DROIT

Protecting human rights

Information Society developments and challenges

Presentation

May 2021

Patrick Penninckx

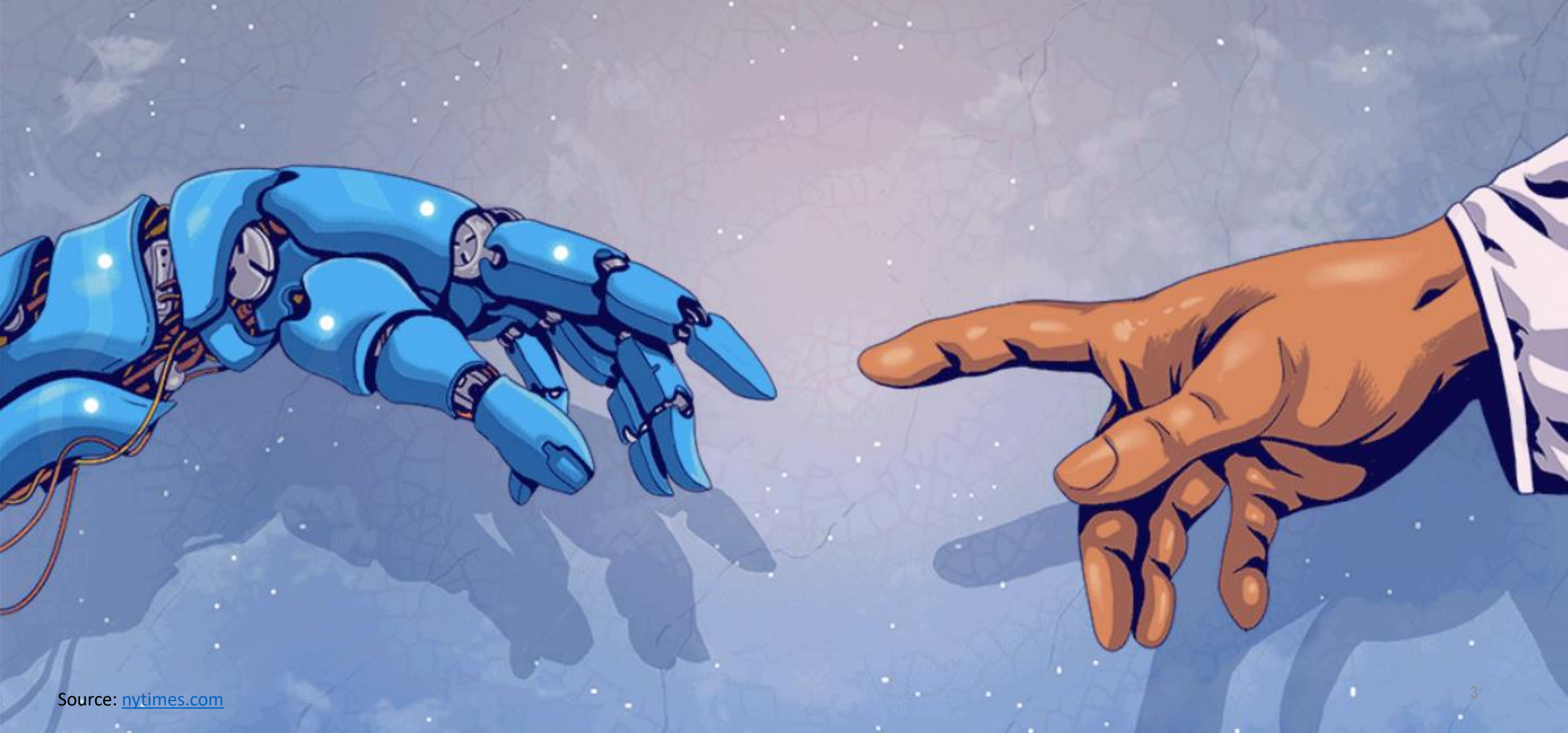
Head of Information Society Department



PRESENTATION TOPICS:

1. Assessing the Impact of the Digital Revolution
2. Managing the Information Society
3. Council of Europe Protecting Human Rights in the digital age

The technological revolution spreads...



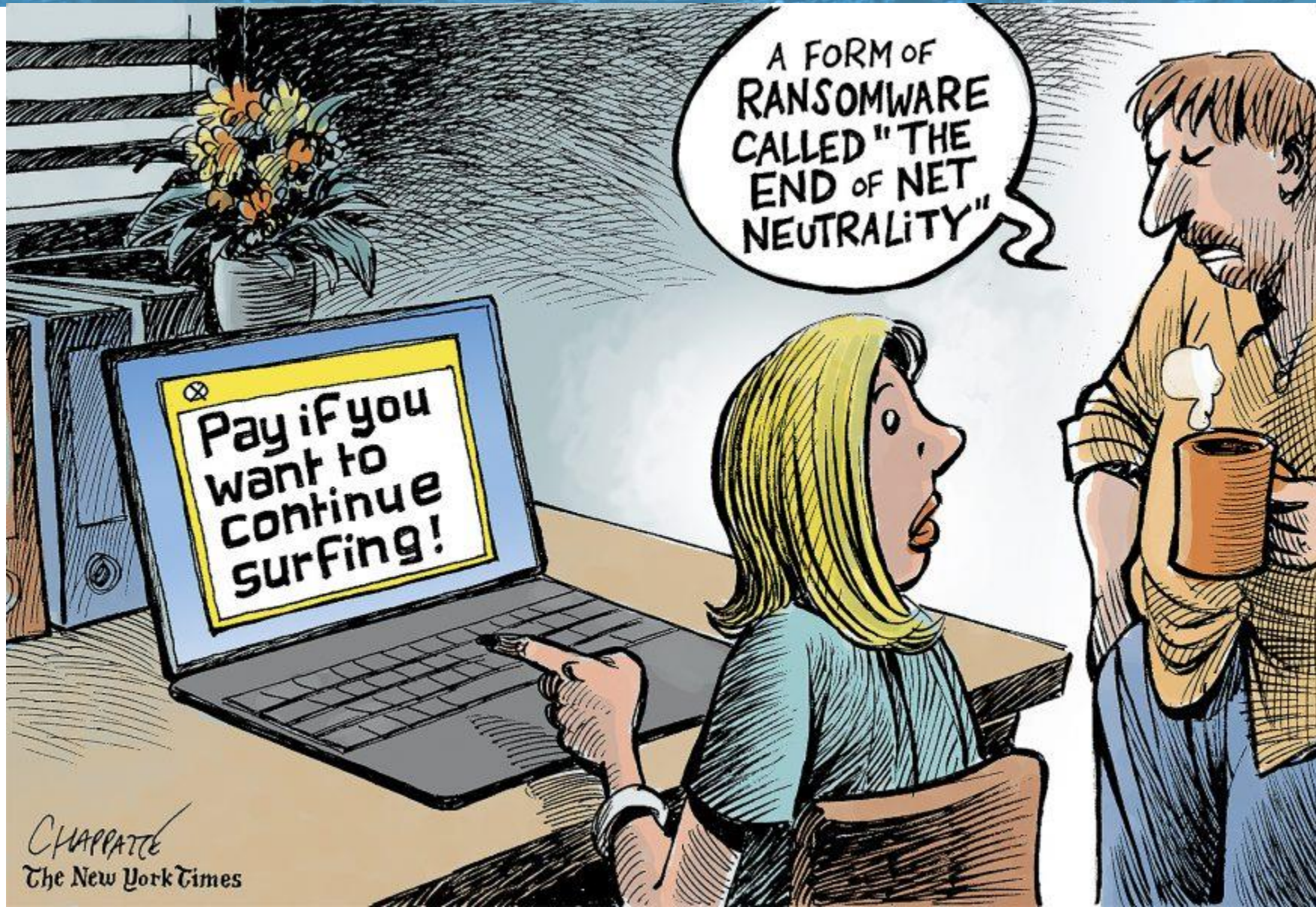
Technology connects more and more



...but technology also divides



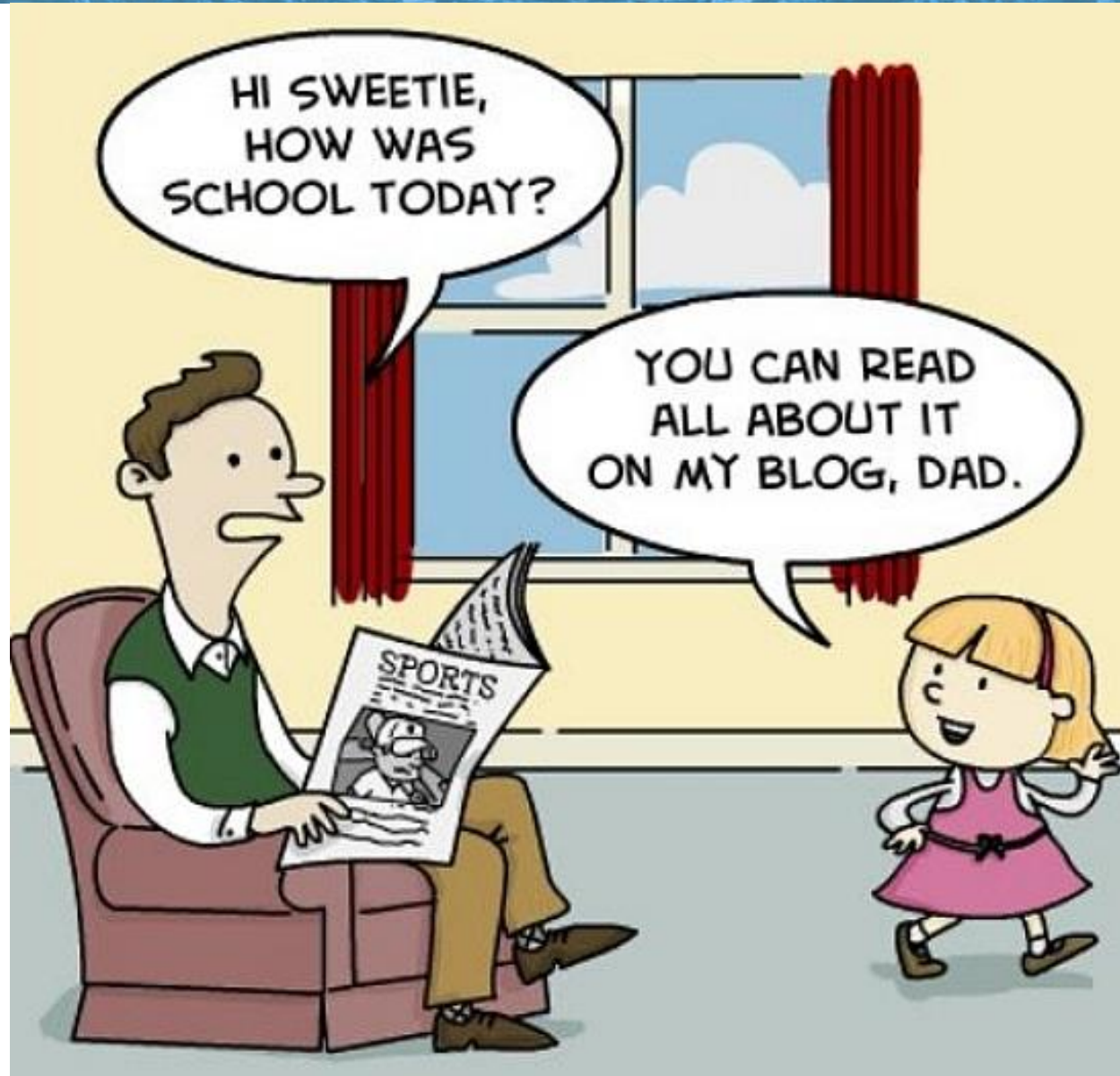
The access to the net is not free



Technology encourages social control



Social media replace socialisation



Platforms manage social contacts

Friends



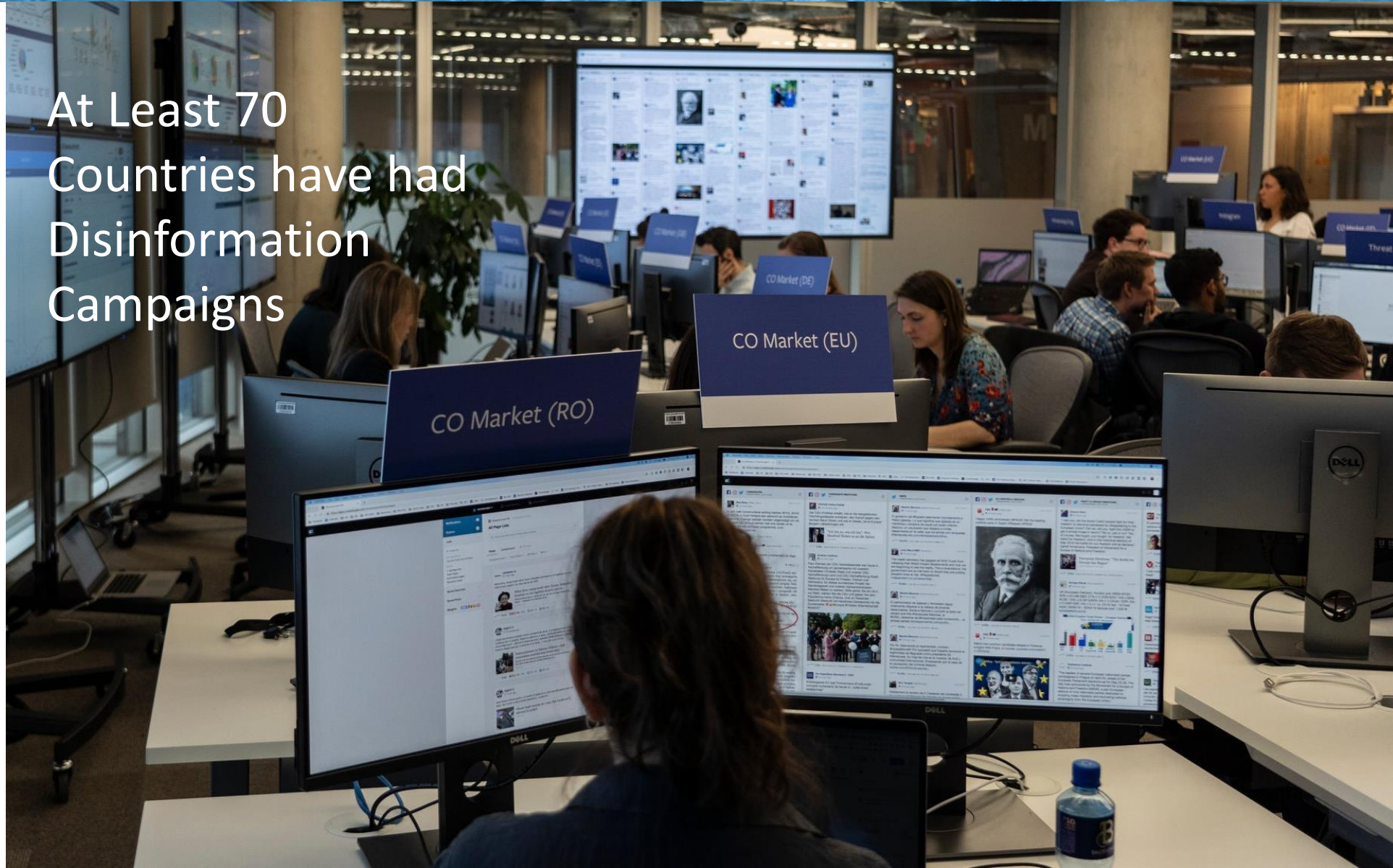
Fake news are spined online



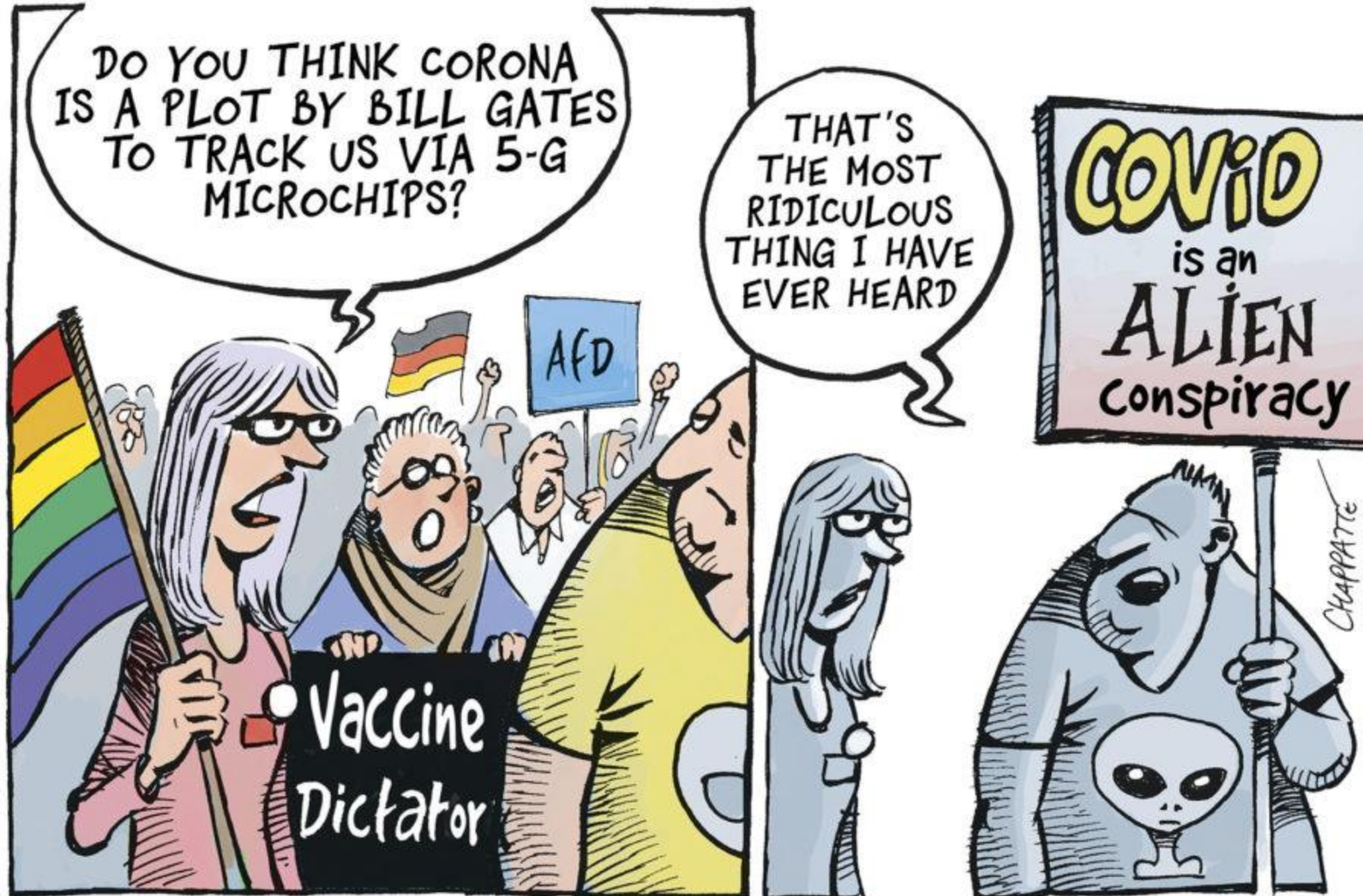
... as well as hate speech



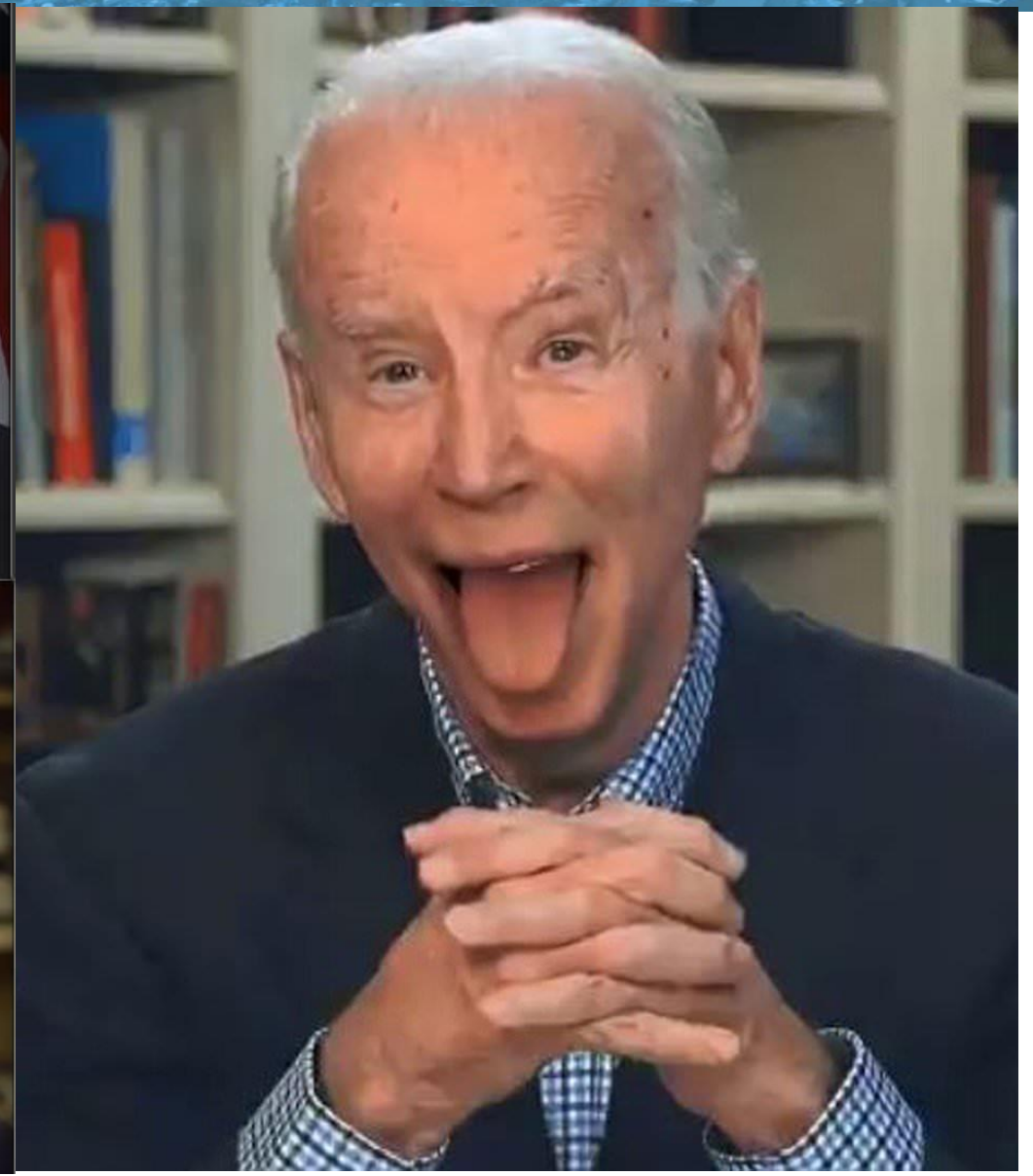
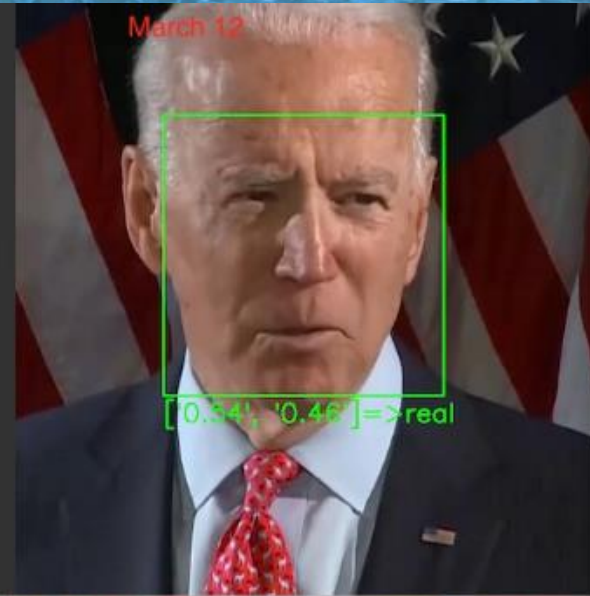
At Least 70
Countries have had
Disinformation
Campaigns



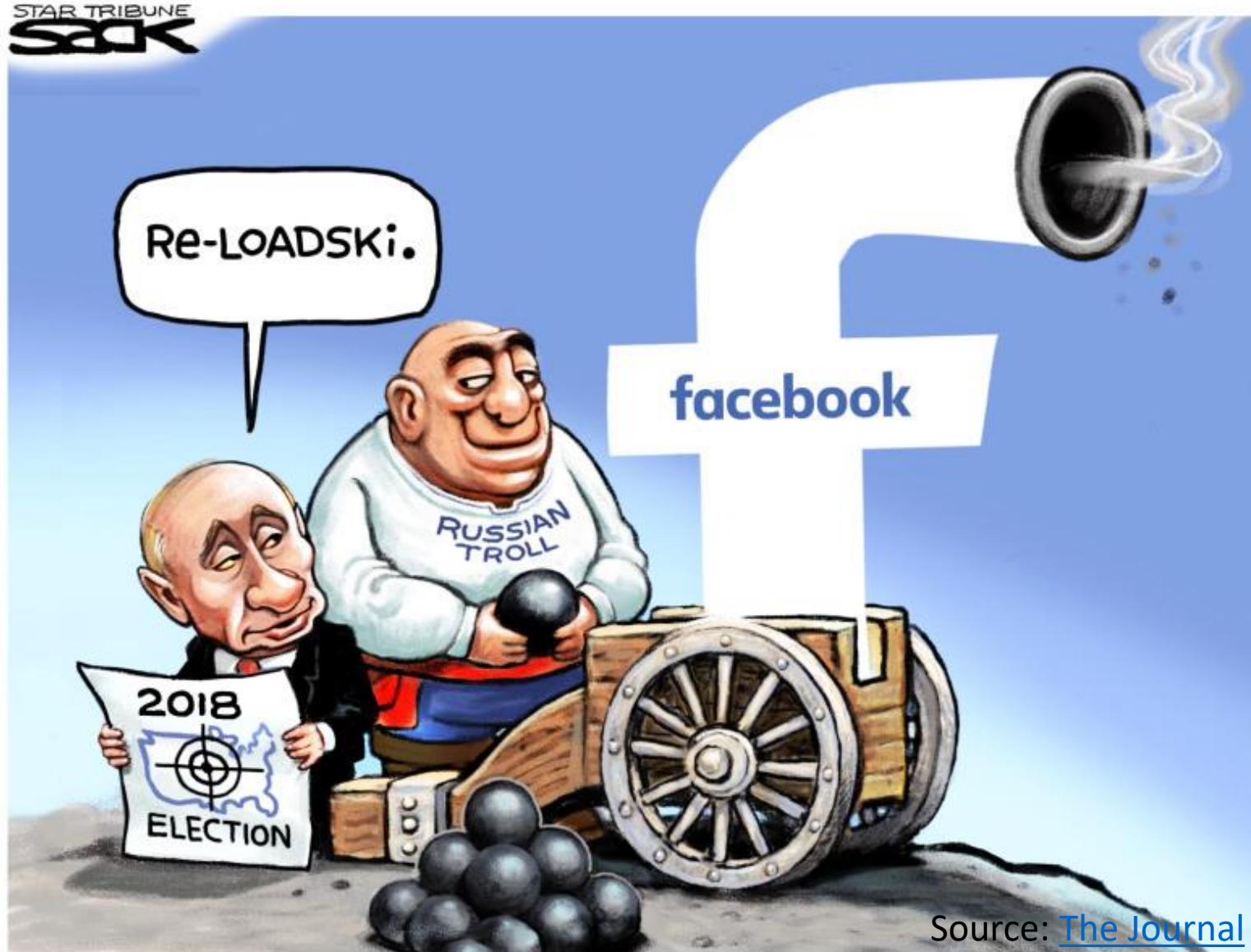
Conspiracies and fake news thrive



Deep fakes distort reality



Disinformation rigs elections

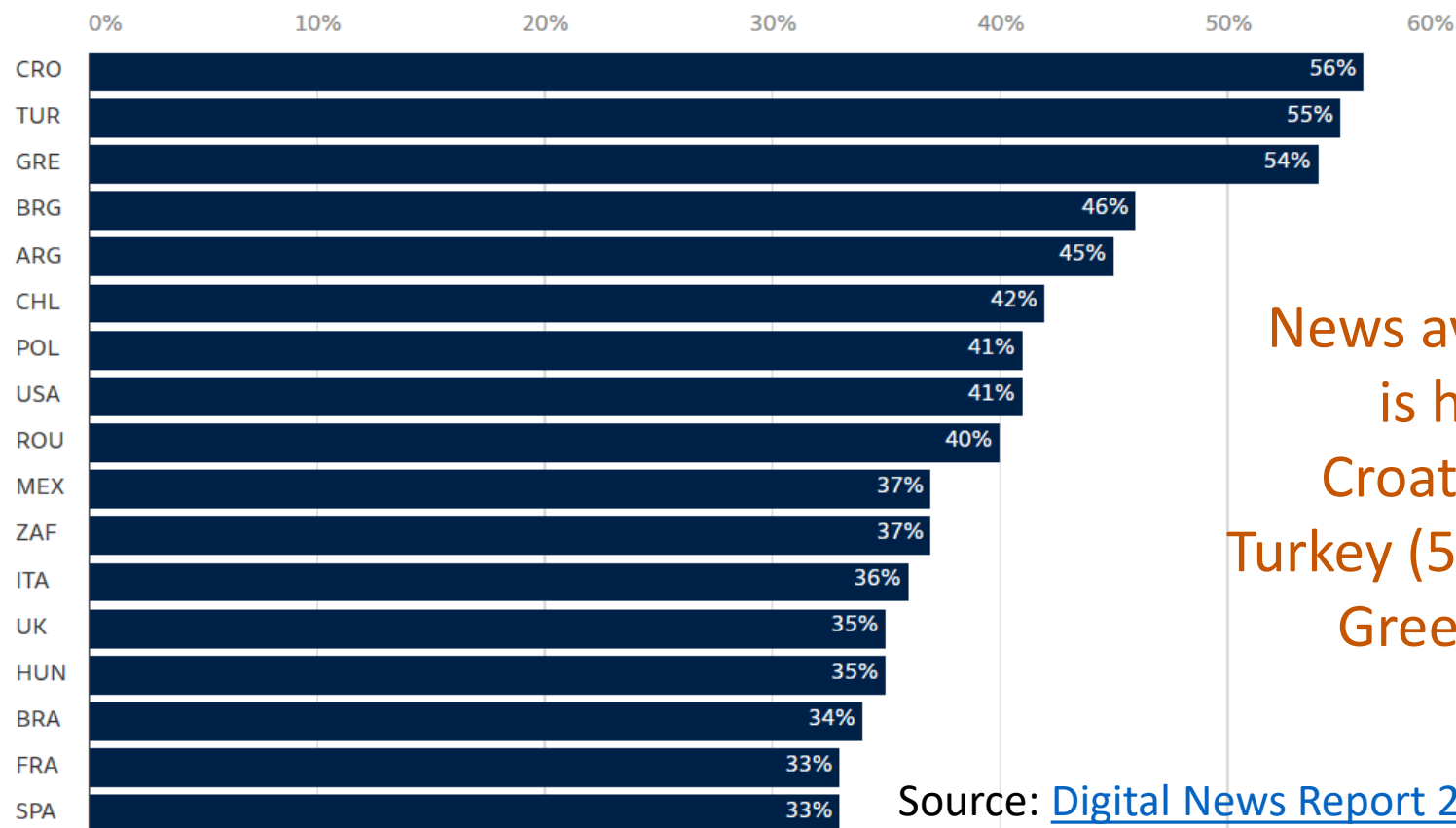


Source: [The Journal](#)

News avoidance extends

PROPORTION THAT OFTEN OR SOMETIMES ACTIVELY AVOIDS THE NEWS

All markets



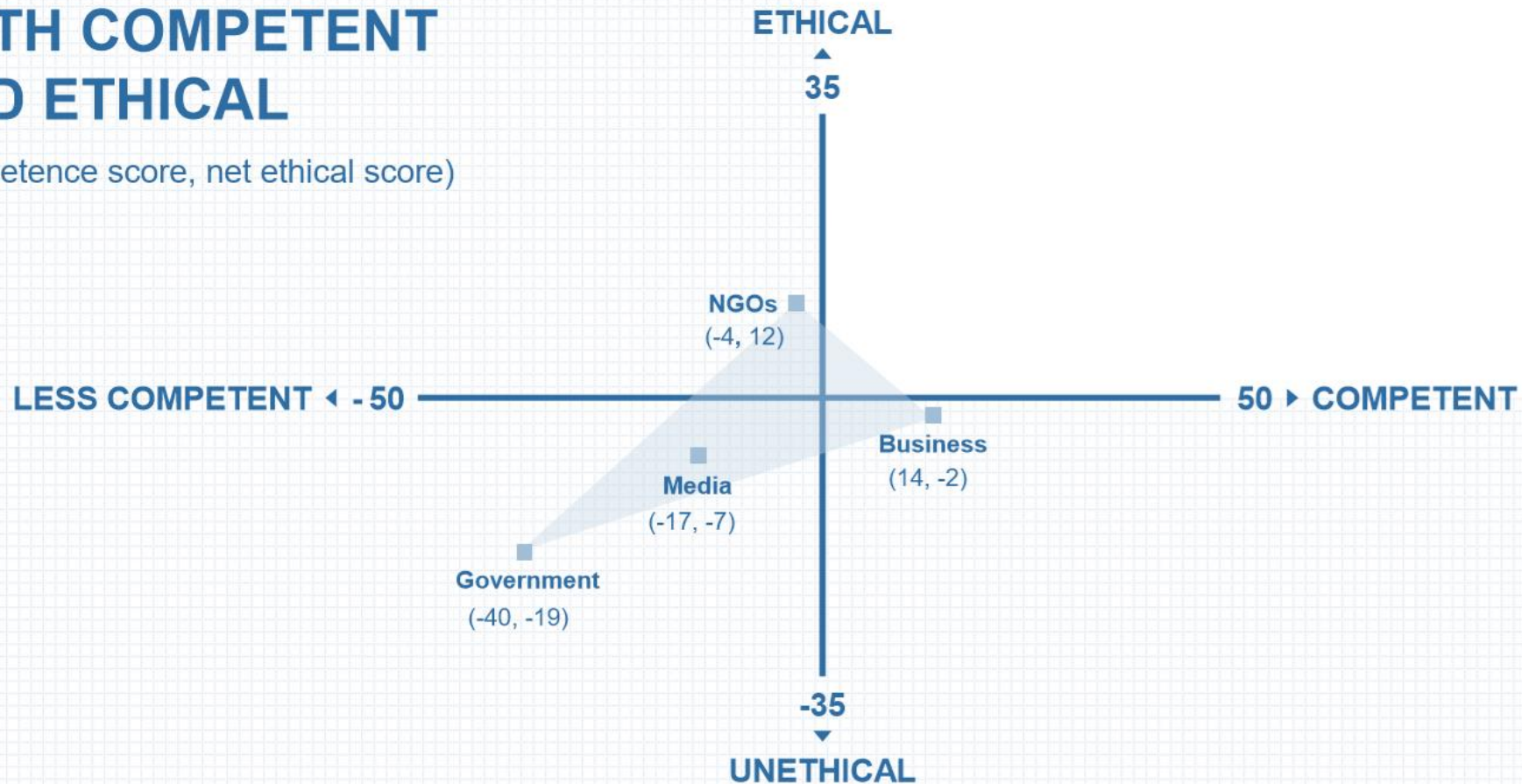
News avoidance
is highest in
Croatia (56%),
Turkey (55%), and
Greece (54%)

Source: [Digital News Report 2020](#), Reuters Institute

Disinformation brings distrust

NO INSTITUTION SEEN AS BOTH COMPETENT AND ETHICAL

(Competence score, net ethical score)



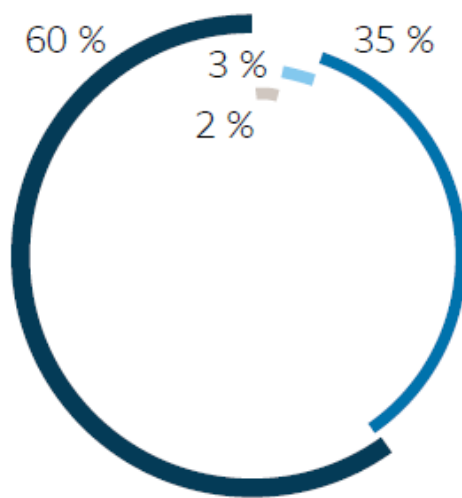
Source: [Edelman Trust Barometer 2020](#)

Distrust in Internet increases

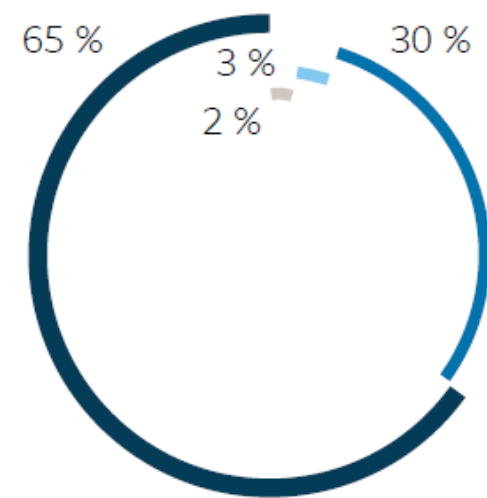
European caution when using the internet,* 2021, percent

● More cautious ● No difference ● Less cautious ● Don't know

Compared to five years ago, are you more or less cautious regarding...



the security of your devices and accounts



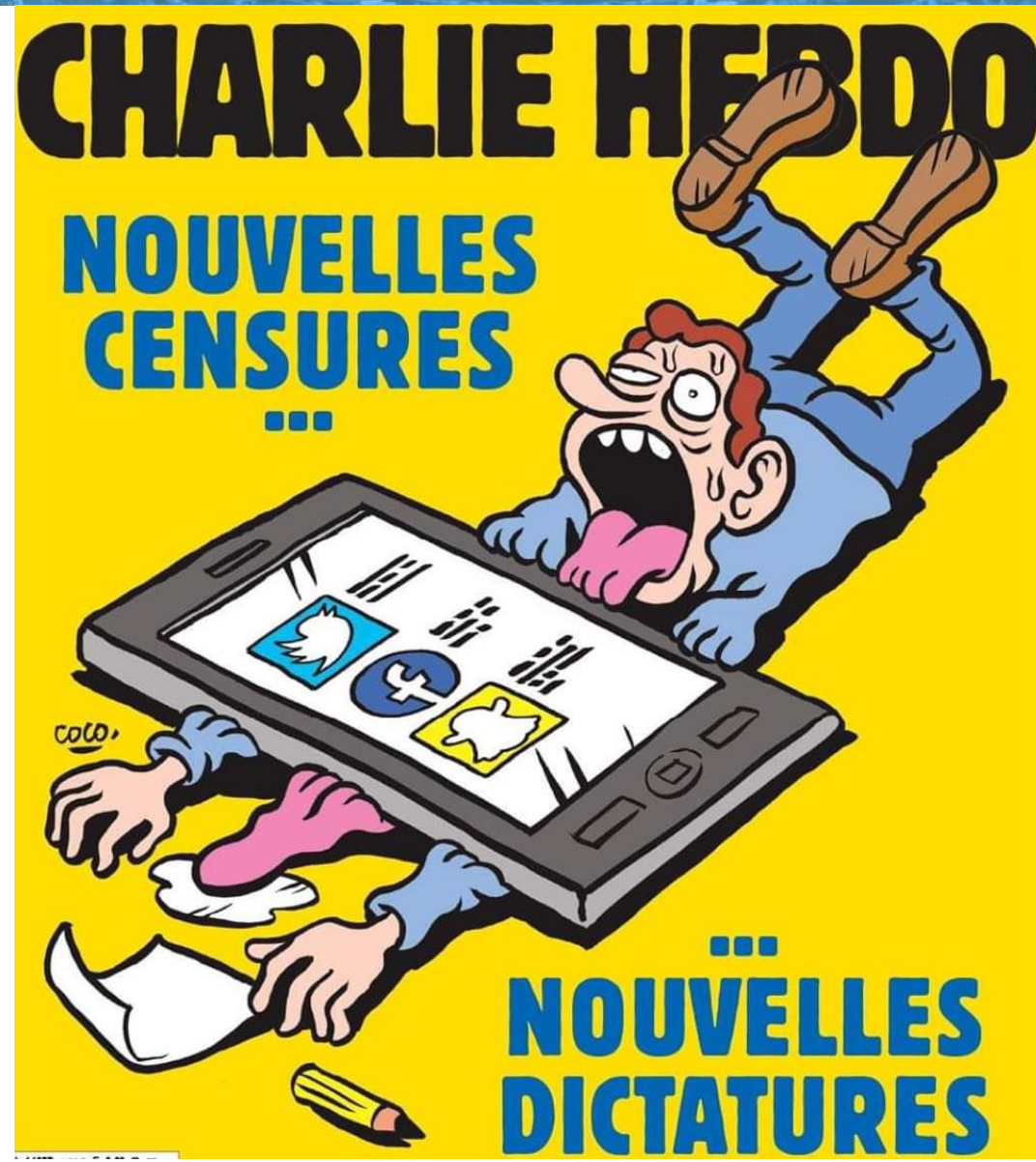
the reliability of information online

Source: [Munich Security Brief](#)

Data: Kekst CNC, commissioned by the Munich Security Conference.

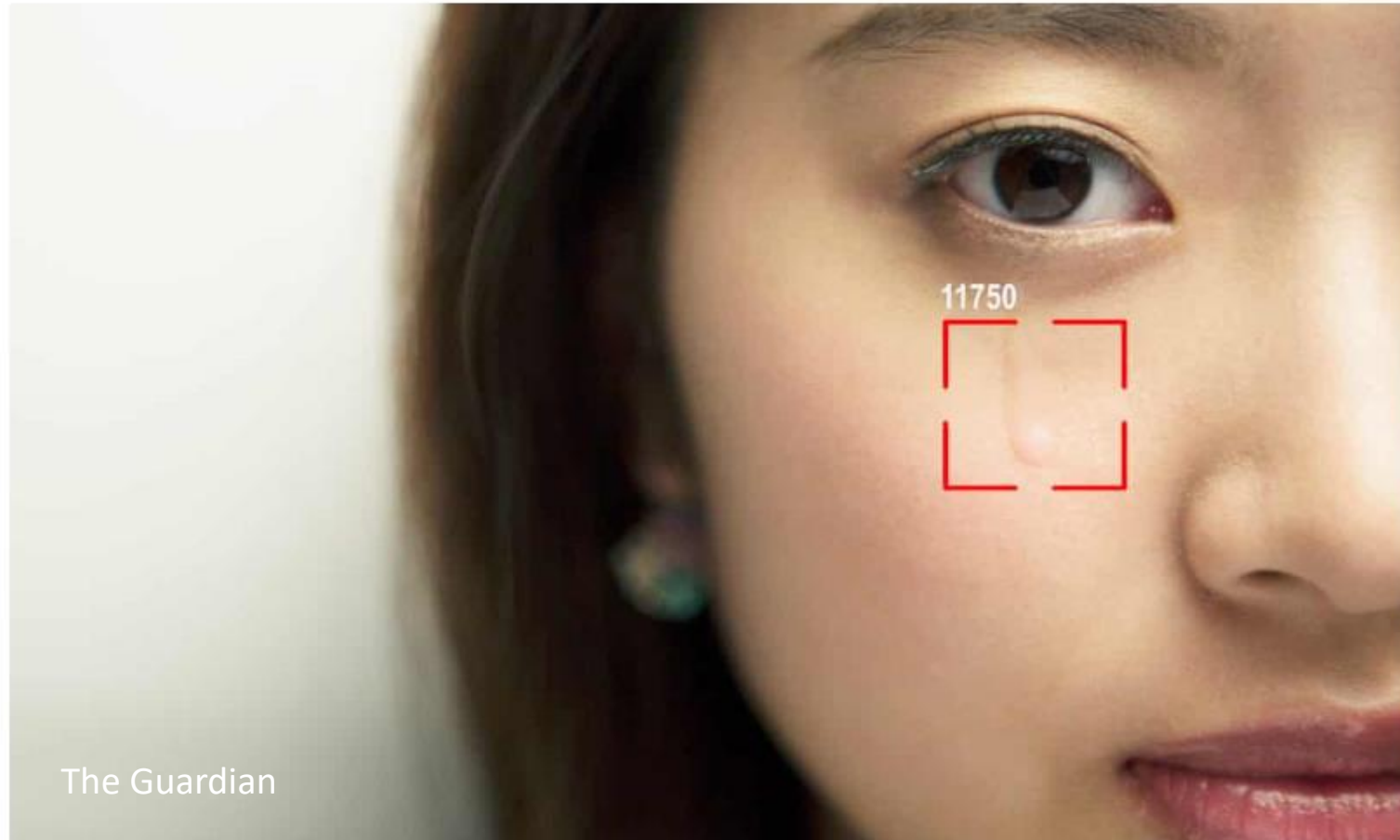
Illustration: Munich Security Conference.

*General population in France, Germany, Italy, Poland, Sweden, and the United Kingdom.



Machines are getting smarter

Machines can now allegedly identify anger, fear, disgust and sadness. 'Emotion detection' has grown from a research project to a \$20bn industry



The Guardian

I am always watched

Your face: a \$20bn industry

The Guardian



▲ Monitors display a video showing facial recognition software in use at the headquarters of the artificial intelligence company Megvii, in Beijing. Photograph: New York Times/eyevine



My personal data are public



AI selects my content



Source: Facebook
Transparency Report

NUDITY
21 million
removals
99,8% by AI

HATE SPEECH
2,5 million
removals
38% by AI

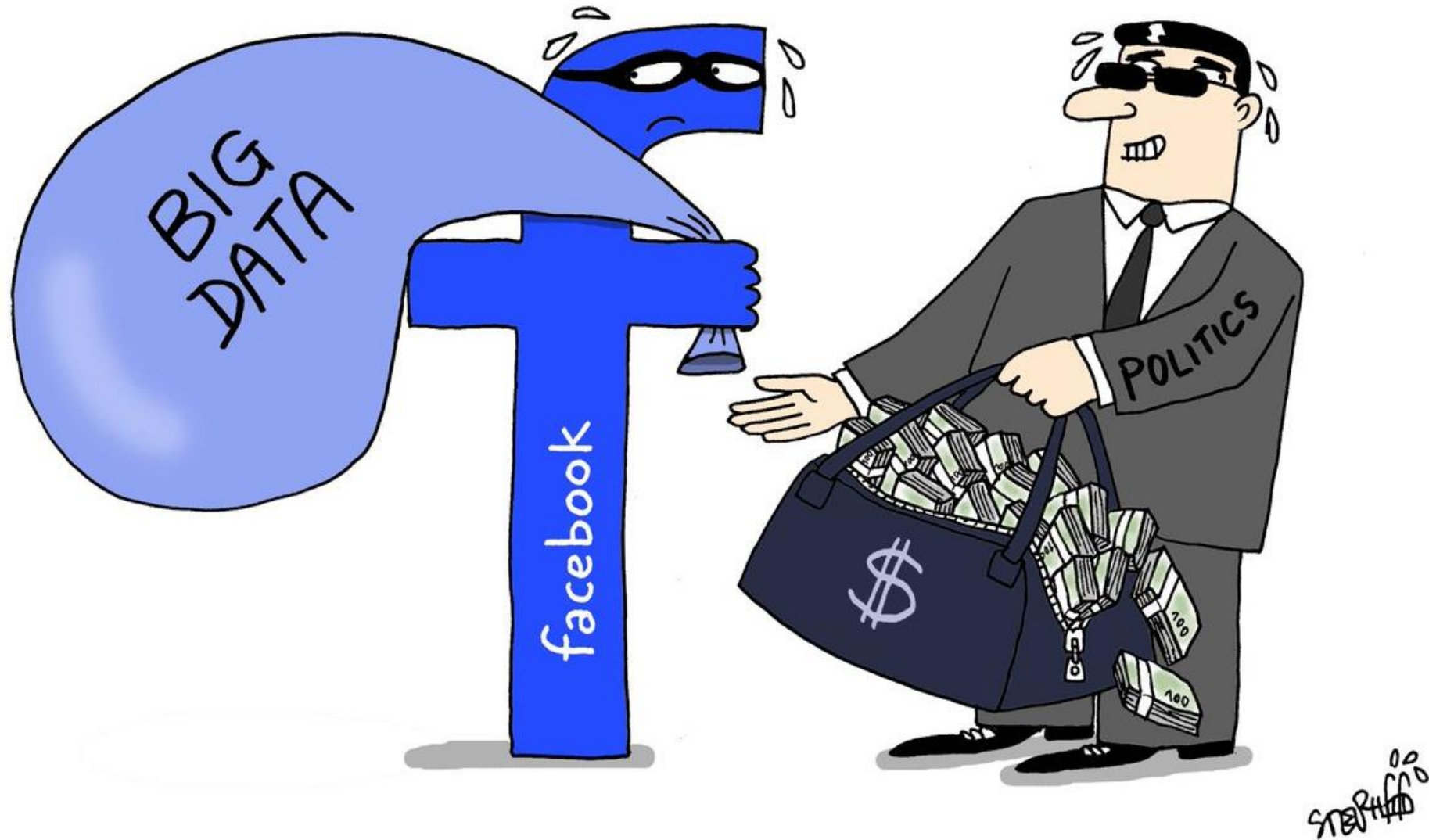
**TERRORIST
CONTENT**
1,9 million
removals
99,5% by AI

**GRAPHIC
VIOLENCE**
3,4 million
removals
85,6% by AI

I feel naked on the net



My data becomes a commodity



Cybercrime proliferates



Fake vaccine certificates are sold online



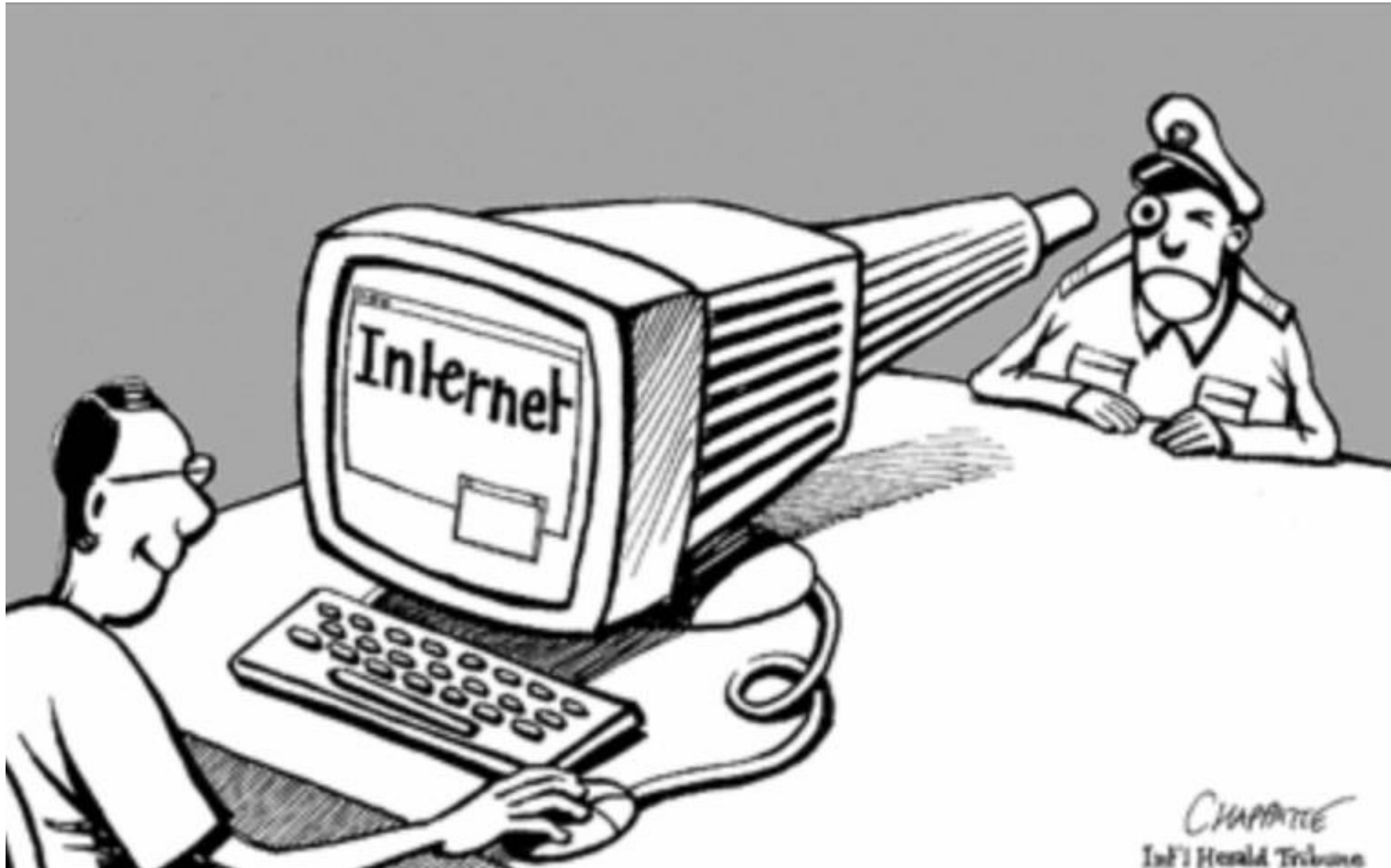
Fraudsters sell forged COVID-19 vaccination certificates on the dark web in a fast-growing pandemic scam, cyber security analysts say

Privacy and public safety collide



Source: Do not let the spies weaken encryption, [FT](#)

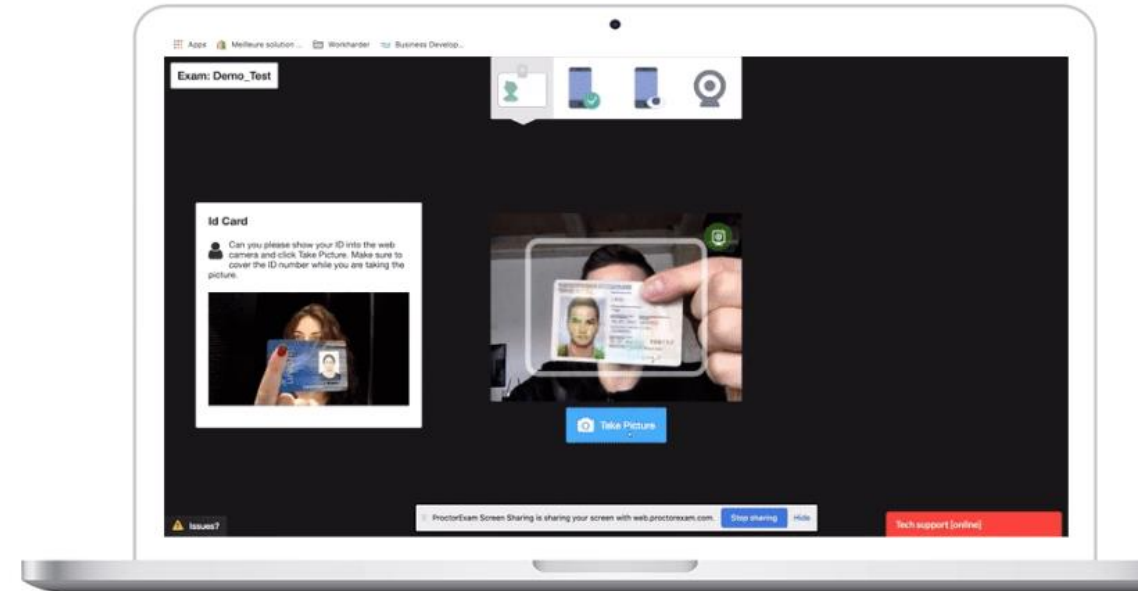
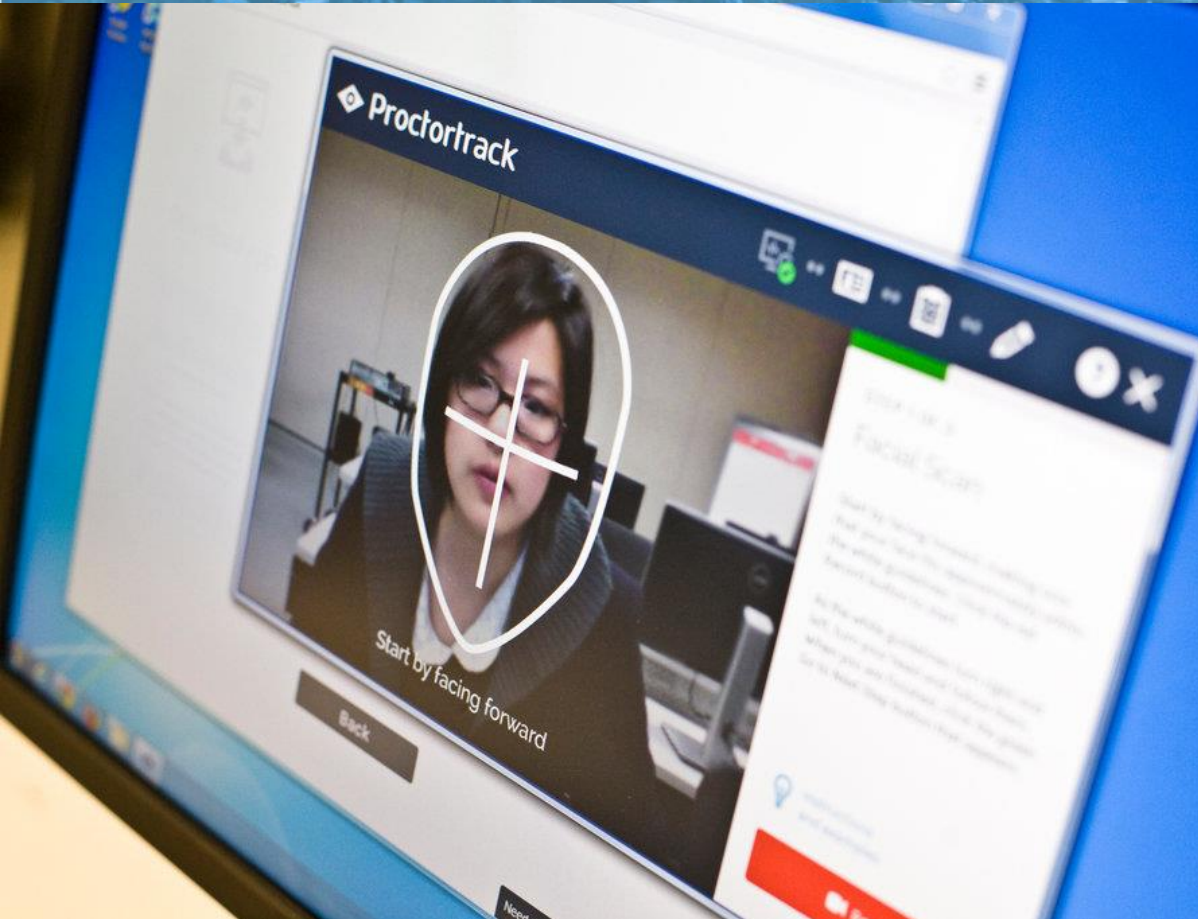
Surveillance becomes widespread



Surveillance hinders transparency



E-proctoring affects students



Concerns

- violations of students' privacy
- impact to students' mental health
- user data from commercial e-proctoring services being hacked

Sources:

globaldomainsnews.com;

wikipedia.org; theverge.com

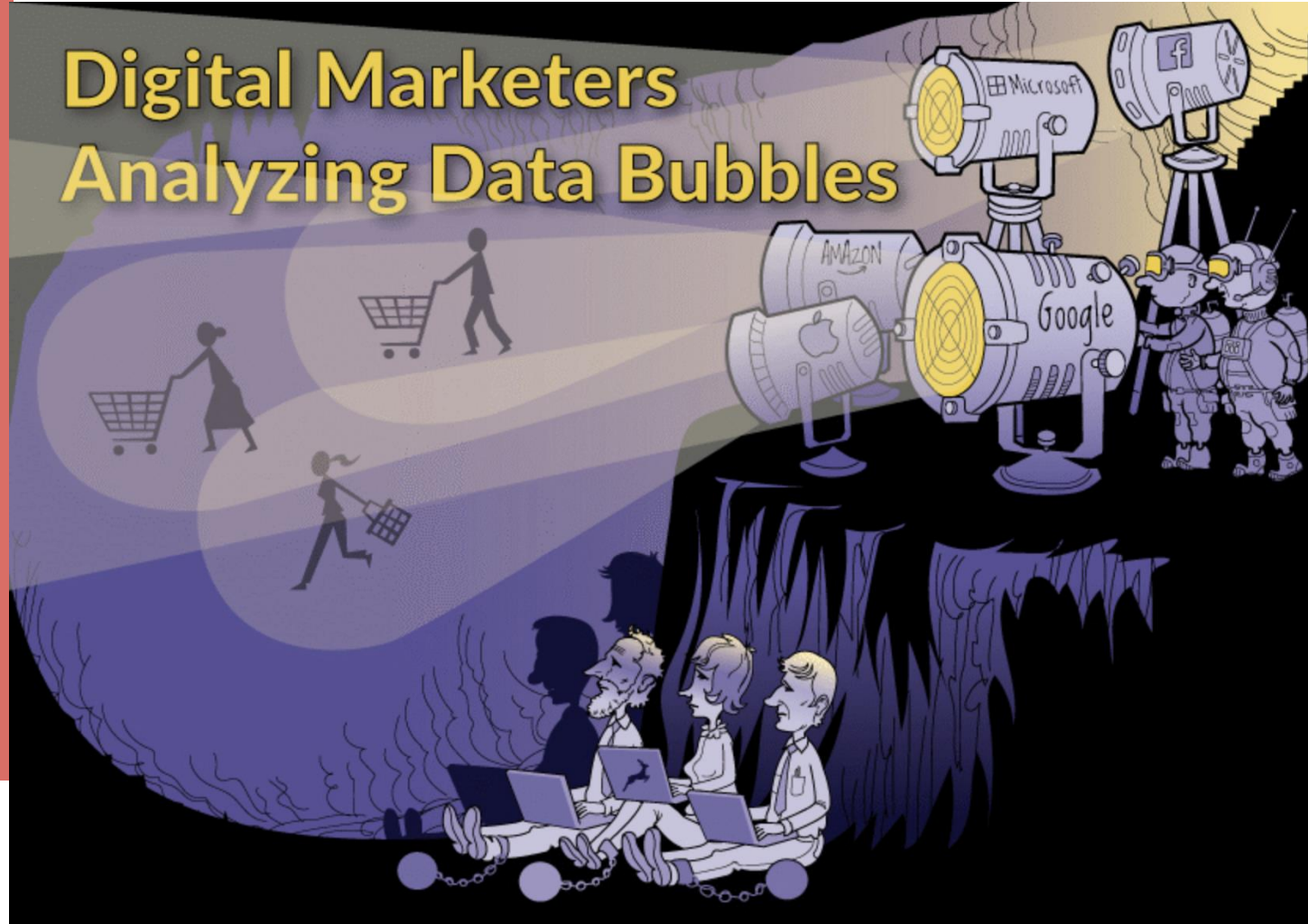
Am I a customer or a product?



Do I still have access to information?



Digital Marketers Analyzing Data Bubbles



Am I free to speak?



Is AI shaping humanity or saving it?



The new world is challenging

Yuval Noah

Harari



21 Lessons
for the
21st Century

**The world has never felt
more unequal.**

Will machine learning and robotics
make humans economically
redundant ?

**Am I moral if I do nothing
when there is a refugee crisis?**

**Algorithms already control
much of our daily lives.**

Volatile societies...

**No one knows what the future
will look like.**

The new world is unstable



The U.S. dollar and the euro will face threats from digital currencies such as Bitcoin.

Source: [livemint.com](https://www.livemint.com)



AI-powered propaganda, by ratcheting up cognitive manipulation and societal polarization, will increase.

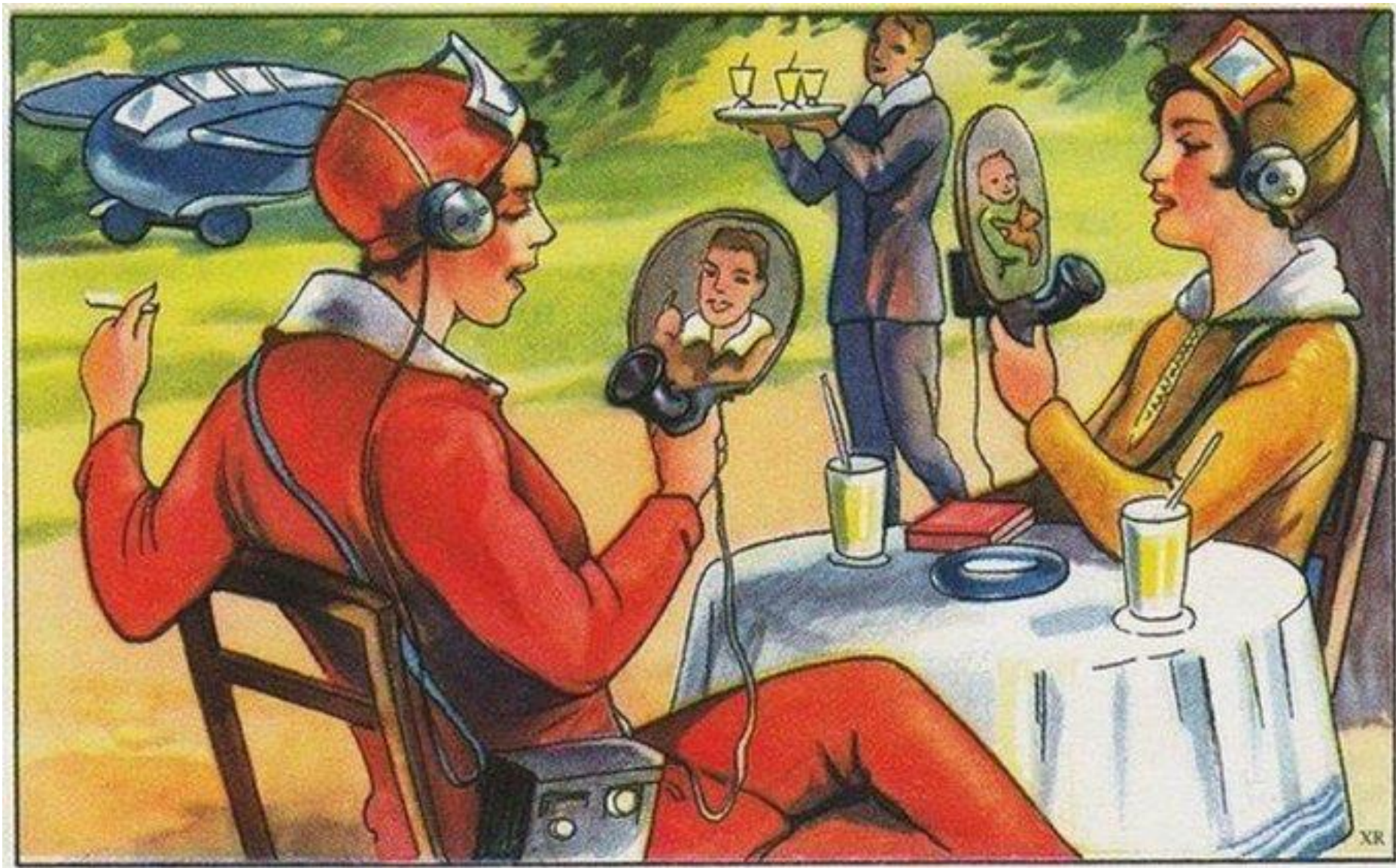
Source: penser-critique.be

Tomorrow will be different...



Artificial intelligence, quantum computing, 5G and the rise of the Internet of Things are just some of the emerging technologies that influence the way our society operates.

1930 vision of the future of communication

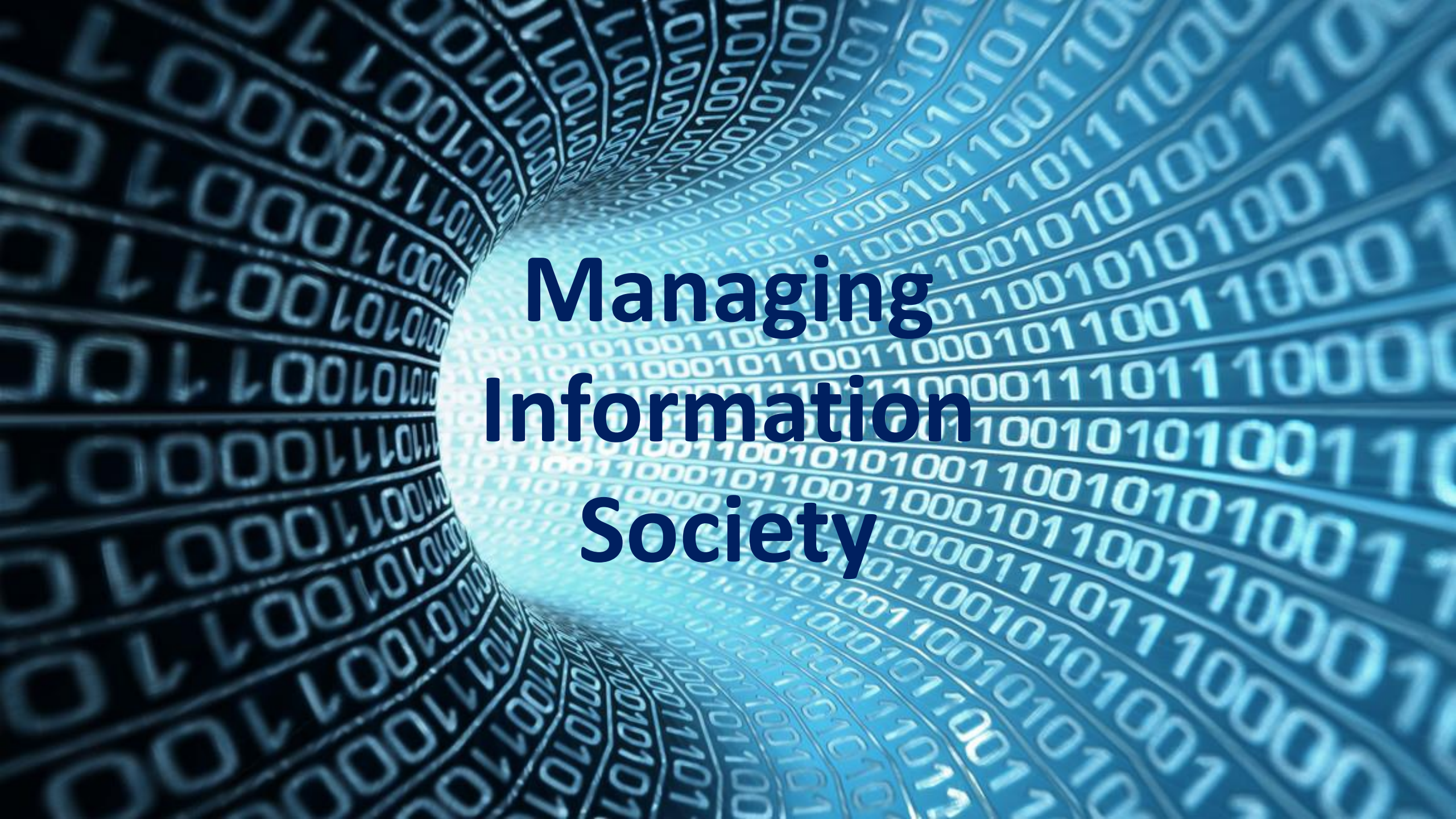


2018 vision of the future humans



What is at risk?

- ✓ Right to private and family life
- ✓ Freedom of Expression
- ✓ Right to participate in democratic processes, such as elections, free from undue influences

The background of the image is a digital tunnel composed of binary code (0s and 1s) arranged in concentric, curved lines that create a sense of depth and perspective. The colors are primarily shades of blue and teal, with a bright light source at the end of the tunnel.

Managing Information Society

**What can
we do?**

Technology Companies ?

National Governments ?

Media Organisations ?

Civil Society ?

International Institutions ?



Top myths worldwide:

- The mRNA vaccines being developed for COVID-19 will alter human DNA.
- The COVID-19 vaccine will use microchip surveillance technology created by Bill Gates-funded research.
- The COVID-19 vaccine has been proven to cause infertility in 97 percent of its recipients.
- The COVID-19 vaccine being developed by Oxford University and AstraZeneca will turn people into monkeys.
- Government food stamps will be denied to those who refuse COVID-19 vaccines.

Source: [newsguardtech.com](https://www.newsguardtech.com)



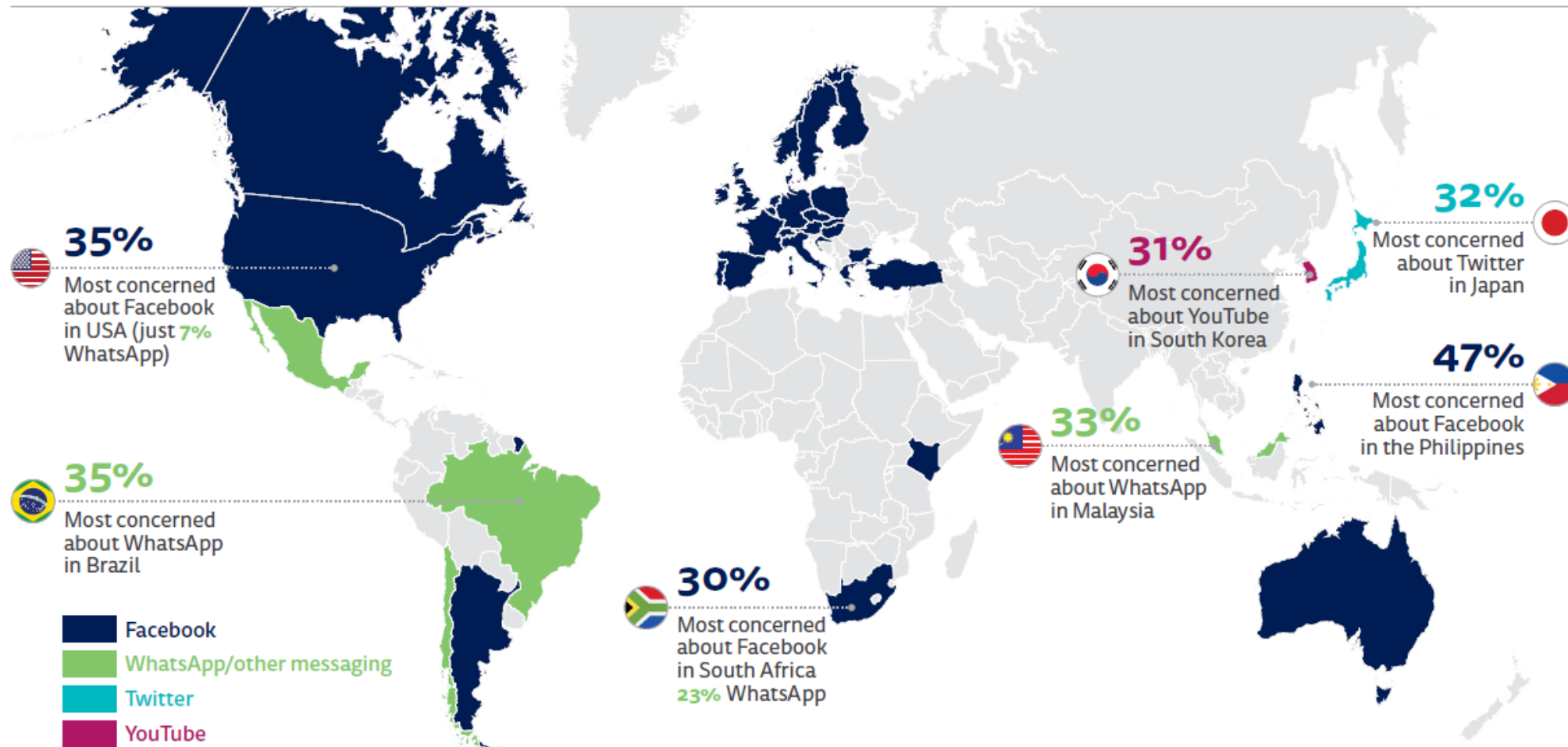
Coronavirus vaccine disinformation: new reports from online platforms by signatories of the Code of Practice on Disinformation

EXAMPLE - Google:

- In 2020 , we've blocked or removed **over 98,5 million coronavirus-related ads** - including Shopping ads - from EU-based advertisers and buyers for policy violations including price-gouging, capitalizing on global medical supply shortages, making misleading claims about cures, and **most recently, fake vaccine doses**.
- We have also suspended **more than 1900 accounts** - including Merchant accounts on Shopping - from EU-based advertisers for trying to circumvent our systems, including for Covid related ads and offers.
- We have also taken action on **over 7000 URLs** with Covid related content under our **Dangerous or derogatory content policy** , for harmful health claims.

Who spreads disinformation ?

MOST CONCERNING PLATFORM FOR FALSE AND MISLEADING INFORMATION – ALL MARKETS



Permanent suspension of @realDonaldTrump

By [Twitter Inc.](#)

Friday, 8 January 2021



After close review of recent Tweets from the @realDonaldTrump account and the context around them — specifically how they are being received and interpreted on and off Twitter — we have permanently suspended the account due to the risk of further incitement of violence.

people have a right to hold power to account

In the context of horrific events this week, we made it clear on Wednesday that additional violations of the Twitter Rules would potentially result in this very course of action. Our [public interest framework](#) exists to enable the public to hear from elected officials and world leaders directly. It is built on a principle that the people have a right to hold power to account in the open.

cannot use Twitter to incite violence

However, we made it clear going back years that these accounts are not above our rules entirely and cannot use Twitter to incite violence, among other things. We will continue to be transparent around our policies and their enforcement.

Should platforms be regulated more?

Tech companies face the real threat of government regulation in reaction to socially harmful content they are publishing.

Research into industries including television, movies, and video games suggests effective self-regulation can benefit both society and companies and keep government regulators at bay.



**Social Media Companies
Should Self-Regulate.
NOW.**

Given the increasing likelihood of government action, the goal of self-regulation should be to avoid a tragedy of the commons, where a lack of trust destroys the environment that has allowed digital platforms to thrive.

Division of responsibilities

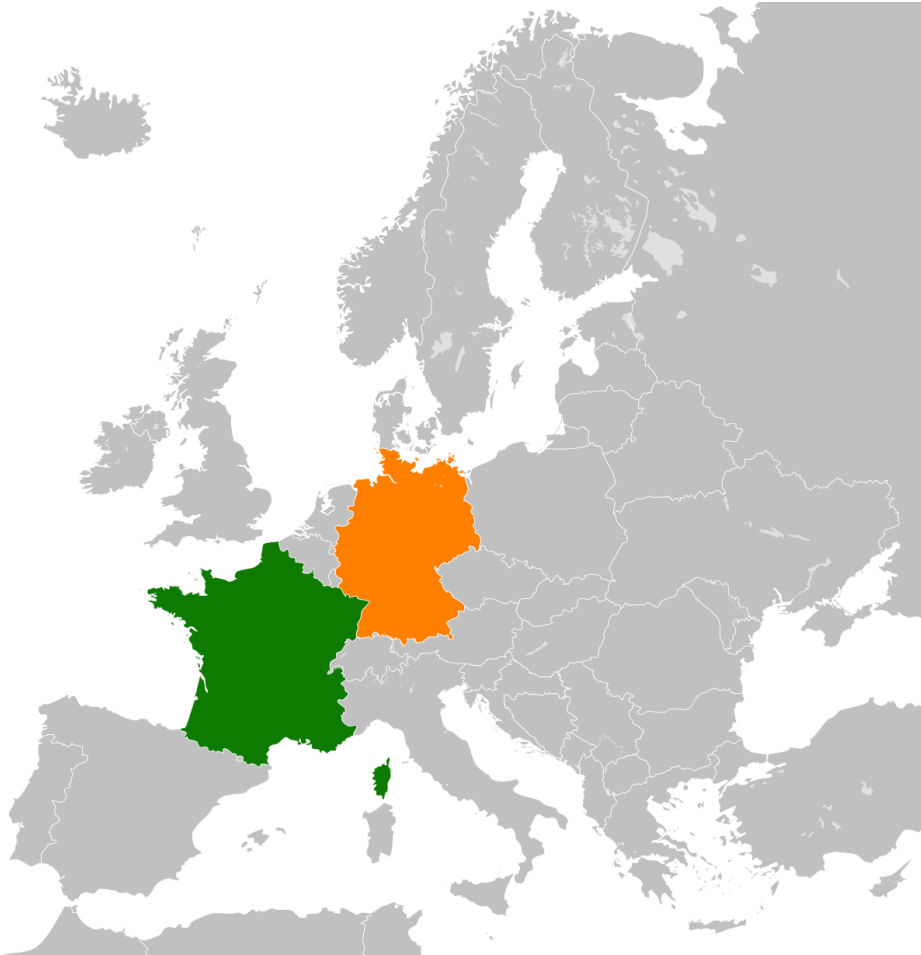
STATES

- **Often entrust the important task** of deliberating “what is true and what false”, together with the liability, to search and social media platforms
- **Some states have enacted legislation** for specific cases of disinformation



PLATFORMS

- **Routinely remove or block content** without explaining why, based on “community standards” rules
- **There is no independent oversight** of their takedown practices



National measures

In the national context, a duty to delete illegal content was imposed on the platforms by **Germany**'s Network Enforcement Act introduced in 2017.

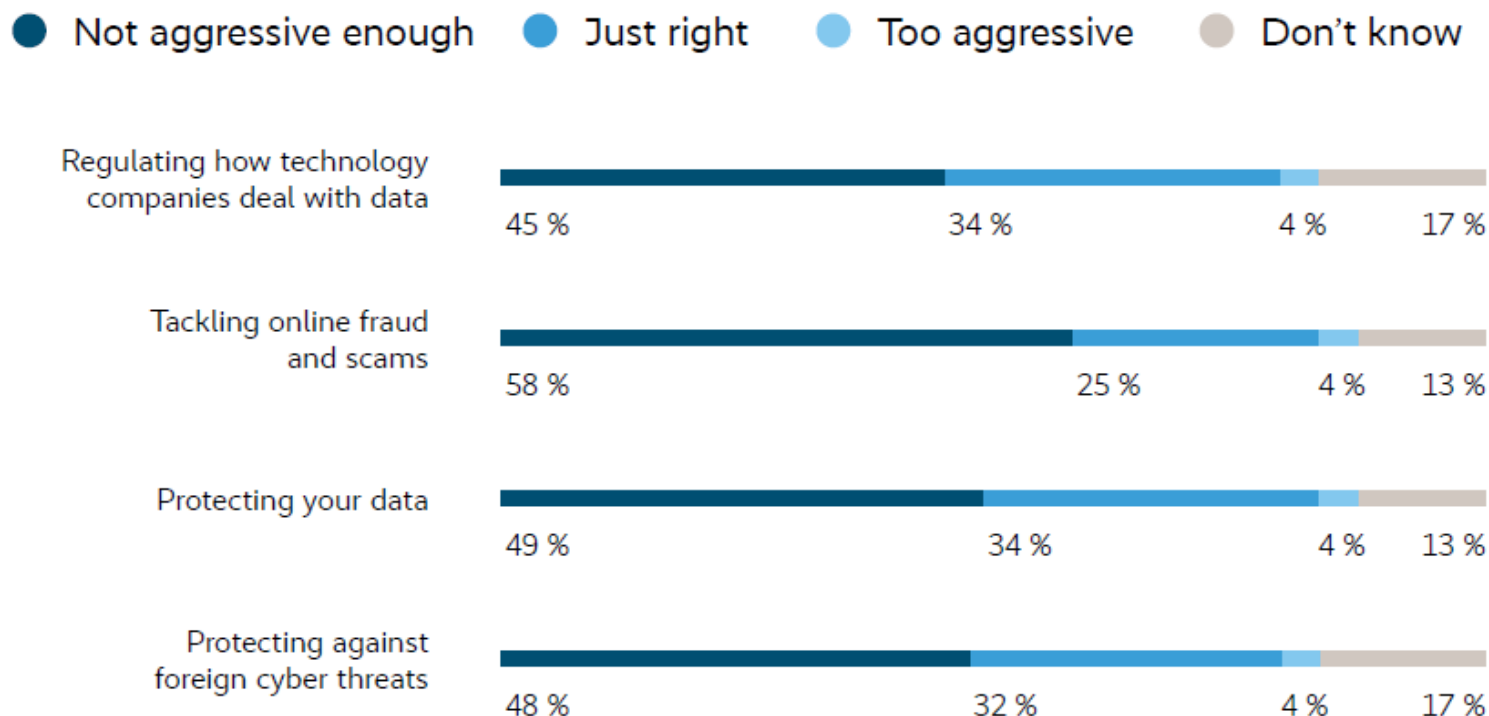
In 2018 **France** introduced a law which imposes on platforms certain obligations to take down misleading information ("fake news") during election periods.

Both these laws have received some criticism that they were **"outsourcing" decisions about freedom of expression to private companies** and possibly incentivising over deletion by introducing strict timeframes and substantial fines for violations.

Governments are expected to do more

Do you think your government is being too aggressive or not aggressive enough regarding...

Public opinion on government action, 2021*, percent



Source: [Munich Security Brief](#)

Data: Kekst CNC, commissioned by the Munich Security Conference.

Illustration: Munich Security Conference.

*General population in France, Germany, Italy, Poland, Sweden, and the United Kingdom.

Governments are expected to focus

What should be the top priority of European countries on digital technologies?

Priorities for government action on digital technologies according to Europeans,* 2021, percent

France

User security

30 %

Fair taxation of tech companies

24 %

That European companies are successful

14 %

That companies respect European values

10 %

Low prices

9 %

Germany

User security

39 %

Fair taxation of tech companies

14 %

Low prices

12 %

That companies respect European values

12 %

That European companies are successful

11 %

Source: [Munich Security Brief](#)

THE ETHICS OF ARTIFICIAL INTELLIGENCE

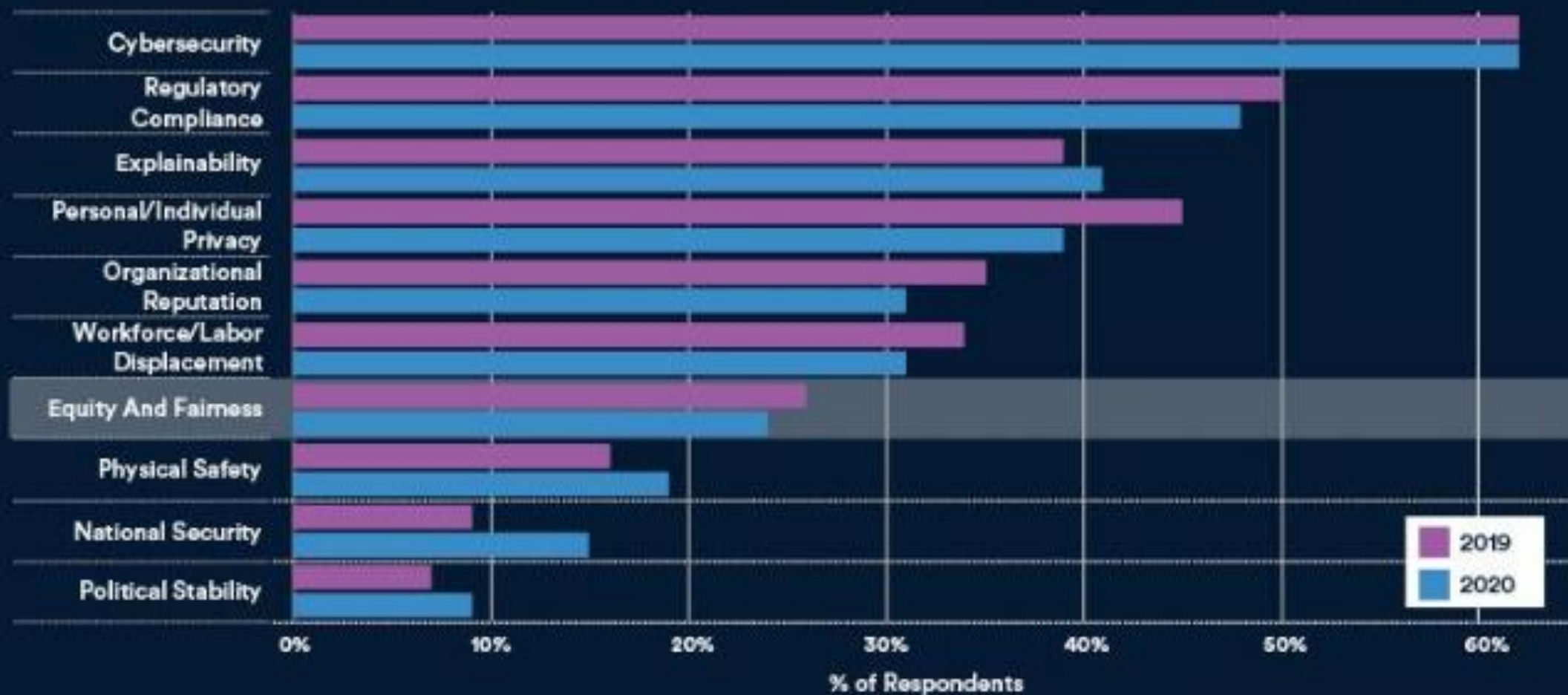
AI research increasingly focuses on ethics

NUMBER OF
PAPER TITLES
MENTIONING
ETHICS
KEYWORDS
AT AI
CONFERENCES,
2000-19



Companies tackle AI risks

RISKS FROM ADOPTING AI THAT ORGANIZATIONS CONSIDER RELEVANT



Countries develop national AI strategies

COUNTRIES
WITH PUBLISHED
AI STRATEGIES: **32**

COUNTRIES
DEVELOPING
AI STRATEGIES: **22**

Safeguarding
**Freedom of
Expression**

Developing
**Digital
Governance**



Protecting **Privacy**

Combating
Cybercrime

Framing
**Artificial
Intelligence**

TRIANGULAR

Methodology

STANDARDS

Recommendations
Conventions



Projects

Programmes

ASSISTANCE

Surveys

Mechanisms

MONITORING

OUR OBJECTIVE

Assist and cooperate with member States to change their policy, legislation and **practice** to effectively protect and promote freedom of expression, media freedom and data protection, in line with Council of Europe standards.

Tackling disinformation



Awareness raising

- Study “Information Disorder”

Standards

- ✓ Convention on **Access to Official Documents**
- ✓ Recommendation on promoting a **favorable environment** for quality journalism in the digital age
- ✓ Recommendation on the roles and responsibilities of **internet intermediaries**
- ✓ Recommendation on the human rights impacts of **algorithmic systems**

Standards

- Recommendation on **media pluralism and transparency of media ownership**
- Recommendation on the **roles and responsibilities of internet intermediaries**

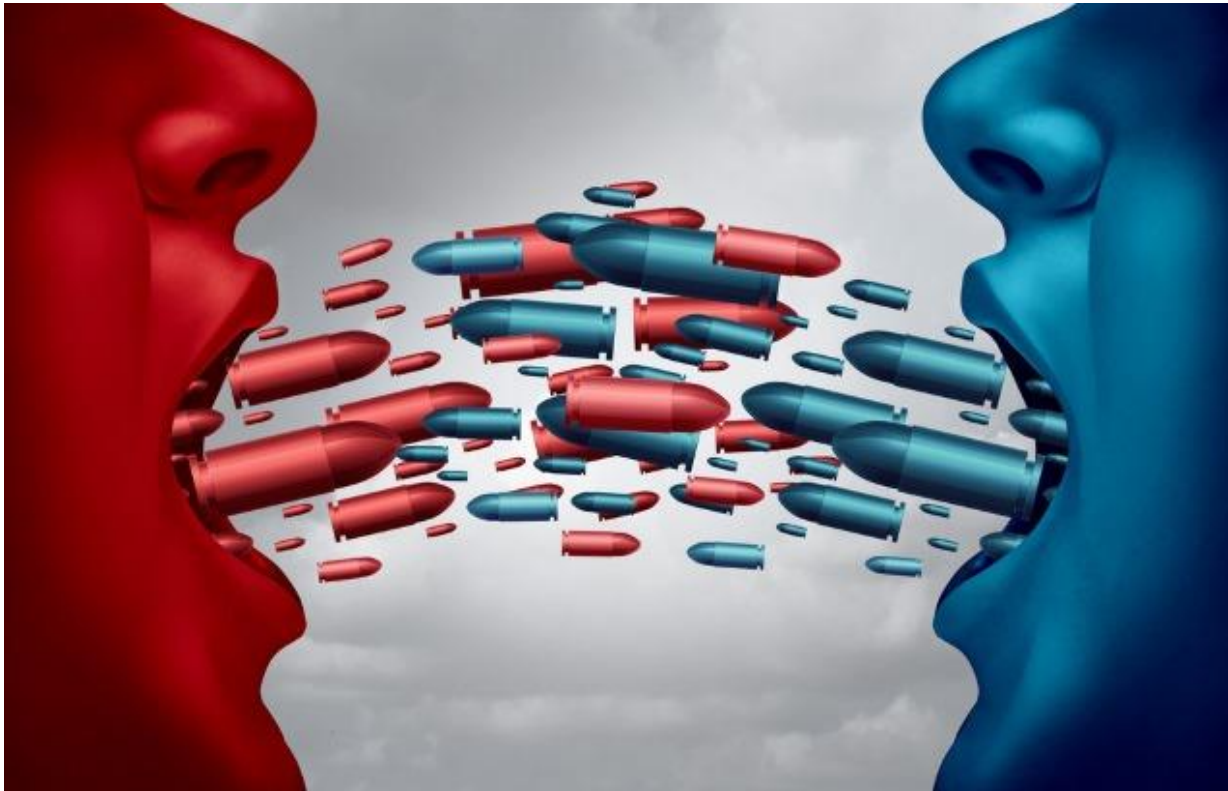


Awareness raising

- “Media Pluralism – How can we deliver?”, International Conference, Strasbourg, 2019



Addressing hate speech



Standards

- ✓ Recommendation on “hate speech”
- ✓ Recommendation on the media and the promotion of a culture of tolerance
- ✓ Recommendation on blasphemy, religious insults and hate speech against persons on grounds of their religion

Awareness raising

- “Addressing hate speech in the media: the role of regulatory authorities and the judiciary”, Regional conference, Zagreb 2018

2020 **2021**

In co-operation with the Steering Committee on Anti-discrimination, Diversity and Inclusion (CDADI), develop a **new and comprehensive legal instrument on combating hate speech** building on the case-law of the European Court of Human Rights and drawing upon existing Council of Europe texts

Strategy on combating hate speech

Protecting journalists



Standards

- ✓ Recommendation on **safety of journalists** and other media actors
- ✓ **Guidelines to states** on how to protect journalists

Awareness raising

- ✓ European survey of **"Journalists under pressure"**
- ✓ **Qualitative study of journalists' experiences and responses**
"Mission to inform: journalists at risk speak out"

Sustaining quality journalism



Standards

- ✓ Declaration on the **financial sustainability** of quality journalism in the digital age
- ✓ Draft Recommendation on promoting a **favorable environment** for quality journalism in the digital age

Awareness raising

- ✓ “(Last) call for quality journalism?”
International conference, Ljubljana, 28-29 November 2019
- ✓ Study on supporting quality journalism through **media and information literacy**





Cooperation

- ✓ Partnership with Digital Companies
 - 25 companies and associations

Standards

- ✓ Recommendation with regard to **network neutrality**
- ✓ Recommendation on **Internet freedom**
- ✓ Recommendation on the **roles and responsibilities of internet intermediaries**

Awareness raising

- ✓ Study “**Liability and jurisdictional issues in online defamation cases**”

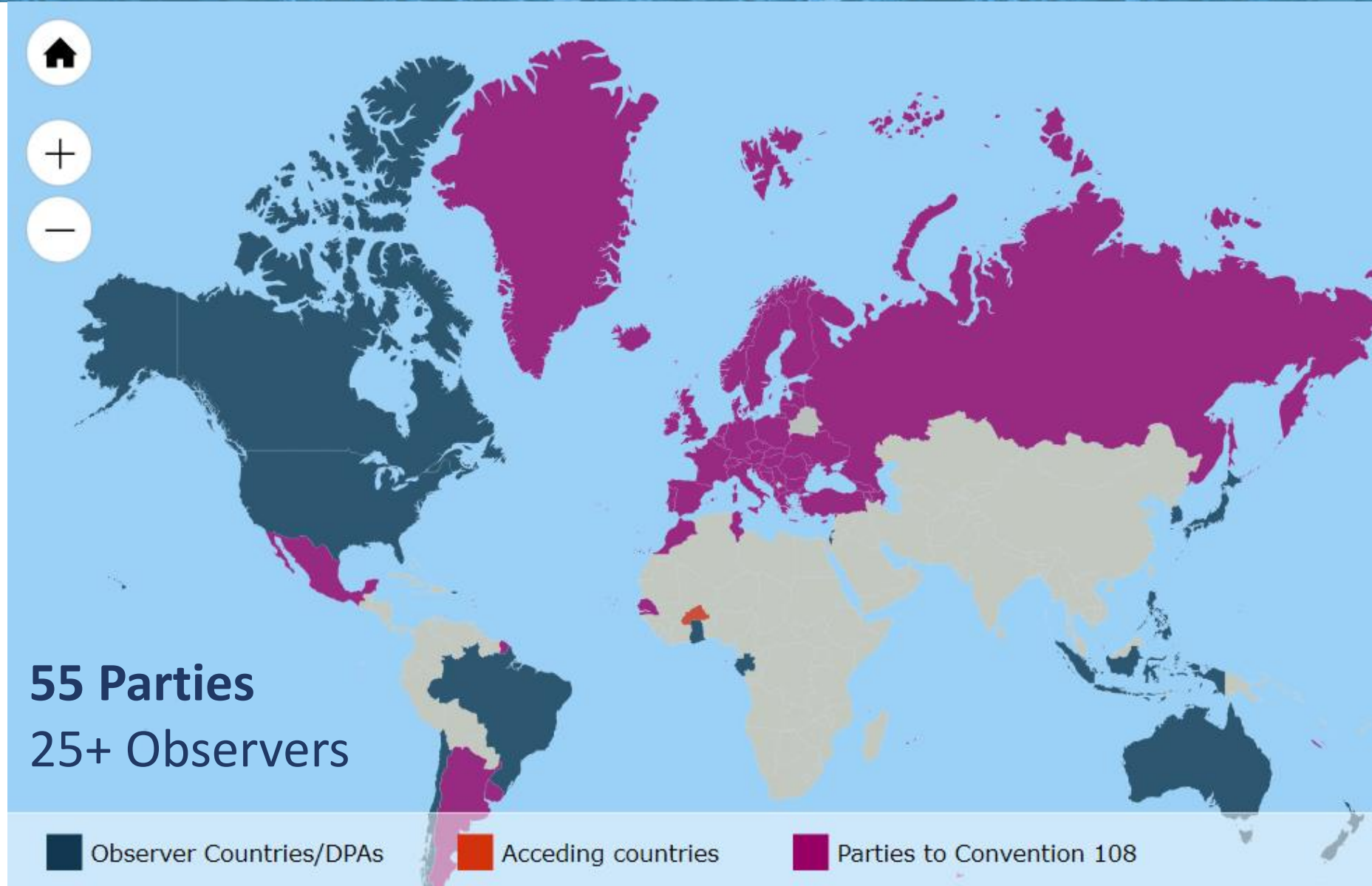
Enhancing digital governance





Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)

- **The only legally binding multilateral instrument** on the protection of privacy and personal data
- **A source of inspiration** since 1981 for international and national privacy legislation



Convention 108

- ➡ 55 countries
- ➡ Outlaws processing of sensitive data on:
 - Race
 - Politics
 - Health
 - Religion
 - Sexual life
- ➡ Enshrines the individual's right to access and correct personal data

Convention 108 +

(adopted on 18 May 2018)

- ➡ New rights for individuals related to big data and algorithms
- ➡ New obligations for data controllers on transparency and accountability
- ➡ Reinforced powers for Data Protection Authorities
- ➡ New monitoring mechanism
- ➡ Signed by 43 States and ratified by 9

Data Protection

➔ Data Protection Convention

✓ 70 participating countries

➔ Convention Committee

set international standards in areas of:

- Artificial Intelligence
- Big data
- Health related data
- Media and privacy
- Data processing by the police



Budapest Convention on Cybercrime

- A framework for effective **cooperation** with the necessary rule of law safeguards available to 65 states parties.
- An **efficient criminal justice response** against cybercrime and other crimes involving electronic evidence.
- A **well established and functioning system** used as a guideline by almost 80% of States worldwide.

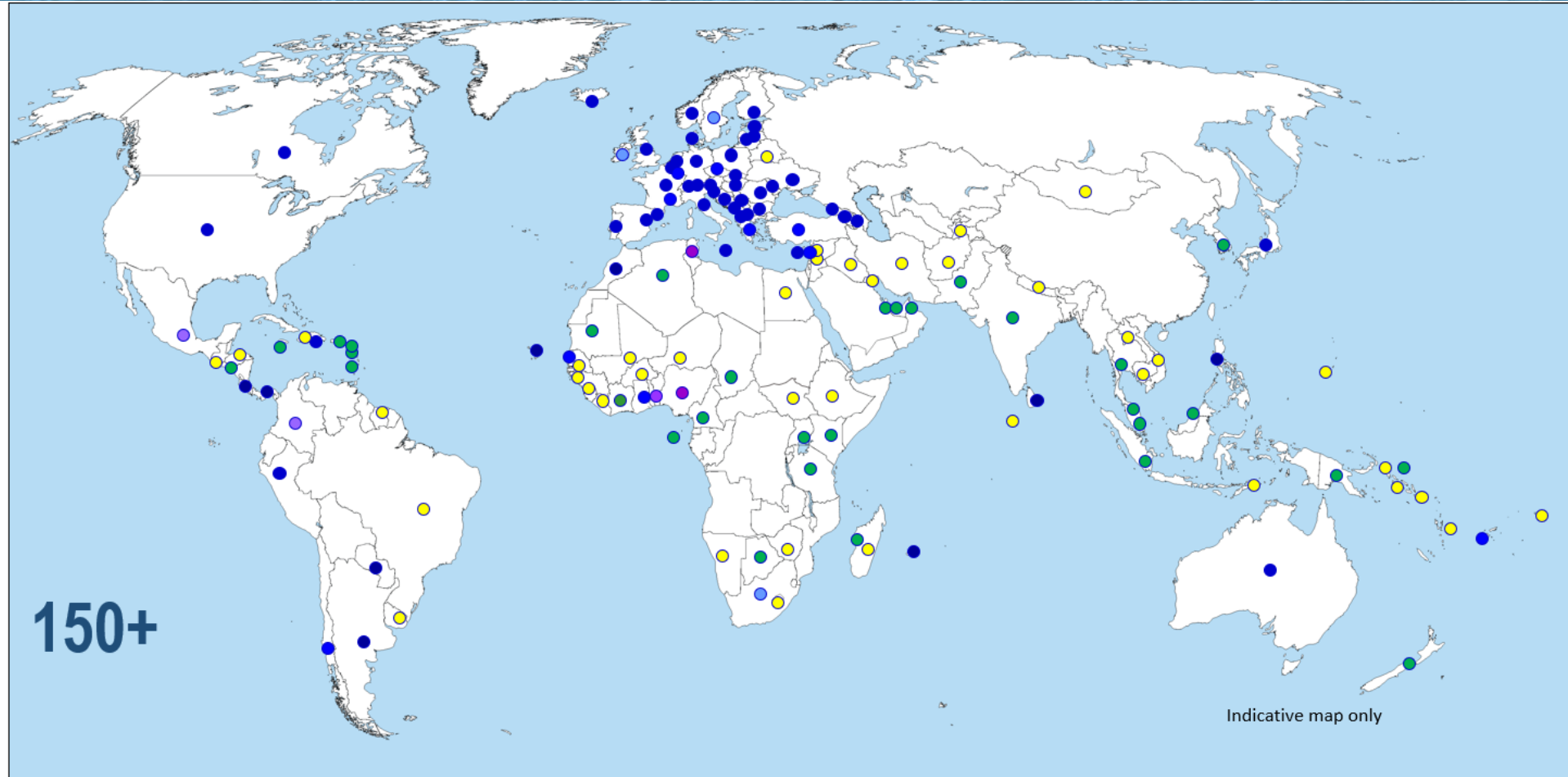
Combating Cybercrime

Key features

- Criminalises offences against and by means of computers
- Provides powers to secure electronic evidence
- Creates a framework for effective international cooperation



Combating Cybercrime



Reach of the Budapest Convention

Parties:	65
Signed:	3
Invited to accede:	8
TOTAL:	76

Other States with laws largely in line with Budapest Convention = 20+
Further States drawing on Budapest Convention for legislation = 45+

Combating Cybercrime



Cooperation framework

Cooperation between the criminal justice authorities of the 65 state parties to detect, investigate, attribute and prosecute cybercrime offences.

Capacity building for criminal justice authorities:

- **OCTOPUS community platform** offers webinars and access to specialized training material.

The 2nd Additional Protocol to the Budapest Convention that is currently under negotiations will be crucial to permit instant cooperation in urgent and emergency situations.

Combating Cybercrime



Council of Europe AI focus



- ✓ Data processing and human rights
- ✓ **Use of AI by the Judiciary**
- ✓ Criminal law implications of AI
- ✓ **Bioethics and AI**
- ✓ Environment
- ✓ **Education**
- ✓ Gender equality, Youth
- ✓ **Children**, Anti-discrimination
- ✓ Culture, Eurimages
- ✓ **Elections**
- ✓ Freedom of expression

CAHAI - Ad hoc Committee on Artificial Intelligence

- Identify major opportunities and negative impacts on human rights, democracy and the rule of law.
- Discover gaps in the current level of protection provided by existing international and national instruments.
- Propose an appropriate legal framework consisting of a combination of binding and non-binding legal instruments, that complement each other.
- **Council of Europe** is the organisation that could bring the « brick » of regulation to create trust based on human rights, democracy and the rule of law.

Artificial Intelligence

2020 **2021**

Develop a feasibility study and potential elements based on broad multi-stakeholder consultations, of **a legal framework for the development, design and application of artificial intelligence** based on Council of Europe standards.

CAHAI Intergovernmental
Ad Hoc Committee on Artificial
Intelligence

**Strategy on human rights
impacts of artificial intelligence**

Thanks for your
attention !



further resources:

www.coe.int/freedomofexpression

www.coe.int/internetgovernance

www.coe.int/dataprotection

www.coe.int/cybercrime

www.coe.int/AI

Facebook Page

Information Society Group

