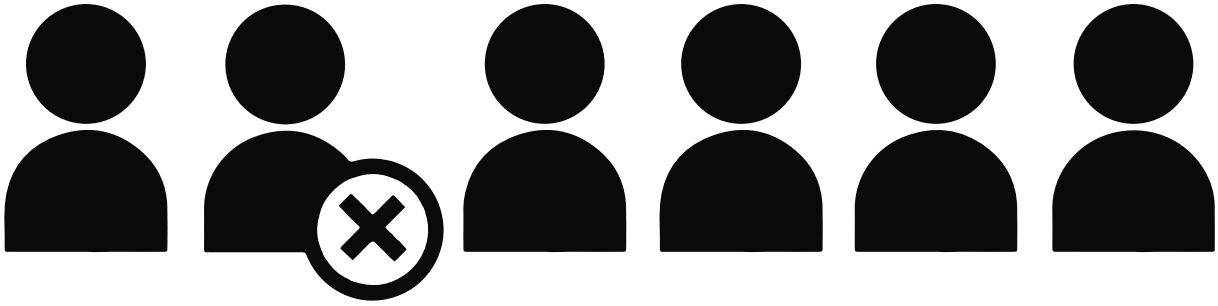
GENEVA INTERNET PLATFORM
digwatch
NEWSLETTER

Issue 60 – Friday, 4th June 2021



(Not) on social media

BAROMETER

A busy month for digital policy. What's hot, what's cold, and what's warming up? As usual, cybersecurity, digital economy, and content policy top the list.

Pages 4–5

BITCOIN

Just how volatile is the price of bitcoin? One tweet can send it tumbling by US$30,000 – though it's not just any tweet.

Page 6

GDPR

On the GDPR's third birthday, we take stock of the enforcement actions carried out at national and EU levels, and the challenges for the next three years.

Pages 8–9

PIPELINE

The US government's response to the Colonial Pipeline attack (and the SolarWinds breach) will have welcome effects on the private sector.

Page 10

Top trends in May: Deplatforming under scrutiny, ransomware attacks get nasty(ier), cryptocurrencies on a rollercoaster

Each month we analyse hundreds of unfolding developments to identify key trends and underlying issues which impact the work of policy practitioners working in these fields. Here's what mattered in May.

1. Deplatforming under scrutiny

A day after the violent 6 January mob attack on Capitol Hill in Washington, DC, a handful of social media companies took the bold decision of kicking one of the most powerful politicians off their platforms.

The deplatforming of former US President Donald Trump sent shockwaves among political leaders. Should a social media platform – that is, a private company – decide unilaterally whose account to ban? Wouldn't a ban be tantamount to an infringement of one's freedom of expression, affecting both the politician and the electorate?

Policymakers wouldn't have been half as concerned if the companies making these decisions weren't as wildly popular as Facebook, Twitter, and YouTube. But these platforms have billions of users. In some parts of the world, Facebook functions as the entry point to the internet, amplifying its importance. Banning Trump from these platforms means silencing him, with all of the implications for freedom of speech, no matter how controversial he might be.

But there's another issue at stake: the reason for banning Trump is that his social media posts were deemed to have instigated or contributed to the violent attack, in which five people were killed. This raises a host of other dilemmas. How should the limitations to our freedom of speech be interpreted? And who should enforce them when something pans out on social media?

These issues resurfaced in May, when Facebook's Oversight Board confirmed that the company was right in banning Trump, but wrong for banning him indefinitely, and will do so again in response to Facebook's latest decision to ban Trump for two years (which will be at odds with Florida's new law.).

Human rights experts believe that the generations-old US approach to an almost absolute right to freedom of expression is shifting.

When Twitter announced it would start fact-checking Trump's tweets in May 2020, Facebook's Mark Zuckerberg criticised the move. A month later, Facebook announced it would be slapping warning labels on posts that violate its policies.

Facebook's Oversight Board, created to act as an appeals court, started hearing its first cases last December. The decisions of the board are binding to the company. The fact that Trump was banned from several platforms further confirms the US shift on free speech. As does the Oversight Board's confirmation that the company was right in doing so.

Trump has put the centuries-old approach to the test. The result is a change in how the US First Amendment is viewed. The quasi-anything-goes approach is ebbing away.

2. Ransomware attacks get nasty(ier)

Two ransomware attacks in May crippled critical infrastructures in two countries: The Colonial Pipeline in the USA, which provides gas to almost half of the east coast *(more on page 10)*, and Ireland's healthcare system, which forced hospitals to slow down COVID-19 testing and cancel appointments. There were numerous other attacks throughout the month, including that on meat producer JBS.

This is not the first time that ransomware brought critical infrastructure to its knees. In 2017, the Wannacry and notPetya attacks affected countries worldwide.

One major difference is that the 2021 attacks were carried out by non-state actors. The victims of the

May 2021 attacks also reacted differently: Colonial paid almost US$5 million in ransom, while Ireland refused to pay up. Yet, the result is similar. A handful of hackers were able to bring entire industries to a halt in some of the world's most developed countries.

This shows just how vulnerable some systems still are, how sophisticated the attacks have become, how dependent on technology society is, and how anyone can be held ransom.

3. Cryptocurrencies on a rollercoaster

The vertiginous rise and fall in bitcoin prices show just how volatile the cryptomarket is. Prices are particularly sensitive to how the market is regulated, to any regulatory plans proposed by policymakers, and to what certain 'influencers' say on social media. *Jump to pages 6–7 for a deep-dive into May's triggers.*

Among governments' concerns is the financial well-being of its citizens. No government wants to see billions of dollars wiped off its citizens' personal balance sheets just because of an Elon Musk tweet.

One way of appeasing such concerns is to tighten regulatory oversight, such as what the US Treasury is proposing for transfers over $10,000. A more rigid approach, such as China's, is to ban private cryptocurrency mining and trading, opting instead to create a Central Bank Digital Currency (CDBC).

China is not the only country working on its CBDC. A recent report by Bison Trails, one of Facebook Libra's (now known as Diem) partners, said that there are now more than 40 national plans, including e-Krona (Sweden), e-Peso (Uruguay), Project Stella (EU and Japan), Singapore Dollar (Singapore), RBA DLT (Australia), and m-CBDC Bridge (Thailand, Hong Kong, UAE, and China). South Africa will soon join the list.

Regulatory shifts in the USA and China usually cause ripple effects around the world. But it's the CBDC's centralised nature (that is, ruled by a central bank, unlike cryptocurrency) which is now too attractive for governments to ignore.

In the spirit of altruism, the money-chasing criminals nobly tweeted they would start pre-vetting their targets to avoid creating problems for society. (A few days later, they announced they would be shutting down.)

Digital policy developments that made headlines in May

The digital policy landscape changes on a daily basis. Our aim is to save practitioners time: We decode, contextualise, and analyse ongoing developments, offering a bite-sized authoritative update. There's more detail in each update on the *Digital Watch* observatory.

same relevance

Global IG architecture

The WSIS Forum 2021's final week highlighted the challenges and opportunities of digital transformation.

Cyberattacks were among the topics discussed at the USA-China meeting in Alaska.

low relevance

Sustainable development

Zimbabwe launched its second Community Information Centre to foster digital inclusion. South Africa is considering integrating financial inclusion in its new industrial policy. Australia committed AUD$1.2 billion to spur the digital economy.

increasing relevance

Security

The sixth UN GGE adopted a consensus report. The UN General Assembly approved the outline and modalities of the future activities of a new ad hoc cybercrime committee.

US pipeline operator Colonial Pipeline, meat producer JBS, and Ireland's healthcare network were targeted by ransomware attacks, affecting their operations. SolarWinds hackers targeted 150 organisations in 24 countries, mostly involved in humanitarian and human rights work, Microsoft reported. The Belgian government's IT network went down after a DDoS cyberattack.

US President Biden issued an Executive Order on improving the nation's cybersecurity.

increasing relevance

E-commerce and the internet economy

The EU General Court annulled the European Commission's decision accusing Luxembourg of providing special taxation treatment to Amazon.

The European Commission presented plans for a corporate tax framework. G7 countries are advancing discussions towards an agreement on taxation.

Italy fined Google €100 million for abuse of dominant market position. Germany's competition authority opened investigations into Google's market dominance and data processing practices. The attorney general of Washington, DC launched an antitrust suit against Amazon.

The Biden administration proposed that cryptocurrency transfers over US$10,000 be reported to the Internal Revenue Service. China reiterated the ban on financial institutions and payment companies from providing any service involving cryptocurrency. Iran banned cryptocurrency mining for four months to avoid blackouts.

low relevance

Infrastructure

The global shortage in semiconductors is expected to last for at least a few more years.

India excluded Chinese companies from 5G trials.

France launched a national strategy for cloud computing.

same relevance

Digital rights

WhatsApp slowed down the rollout of its new privacy policy in several countries (including Argentina, Brazil, Germany, and India) due to regulatory scrutiny.

WhatsApp sued the Indian government to prevent the entry into force of new internet rules.

Germany and Belarus adopted new privacy and data protection laws.

---

increasing relevance

Content policy

Facebook decided to ban Donald Trump for two years, after its Oversight Board ruled that although the ban was justified, the penalty needed to be re-examined. Florida passed a law prohibiting permanent social media bans.

A court in Russia fined Facebook and Google over failing to remove content deemed illegal. China announced new measures to address 'unhealthy' online content.

The European Commission issued guidance to strengthen its Code of Practice on Disinformation.

---

same relevance

Jurisdictional and legal issues

The Irish High Court dismissed a legal challenge by Facebook regarding data transfers to the US.

The European Court of Human Rights ruled that bulk interception of communications data breaches the right to privacy and freedom of expression.

Russia asked internet platforms to store data on Russian users on databases inside the country by 1 July.

---

same relevance

New technologies (IoT, AI, etc.)

Amazon extended its ban on US police use of its facial recognition technology (FRT) 'until further notice'. Civil rights groups filed privacy complaints against FRT company Clearview AI in five European states.

EU institutions agreed on the proposal for a Digital COVID Certificate.

Germany announced a €2 billion investment in quantum computing. The US Food and Drug Administration issued guidance on implanted brain-computer interfaces.

#ICYMI: Spain rules gig delivery riders are employees

Food delivery apps operating in Spain have three months to classify their delivery riders as employees, according to a new law. The Rider Law comes after the Supreme Court ruled in 2020 that gig companies must engage their couriers as employees. Countries in Europe, including the EU, are revisiting the work status of drivers and couriers, with the aim of giving them more protections.

Credits: Robert Anasch @diesektion

Bitcoin's on a rollercoaster: Dare to ride?

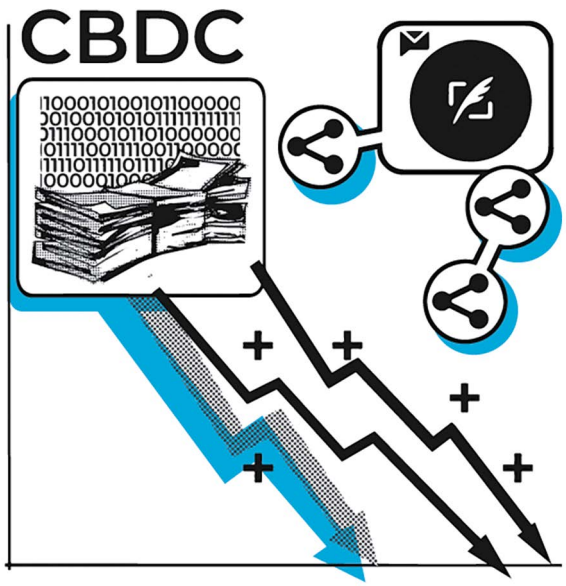
After dropping 50% from its all time high of US$59,000 and plunging to US$30,000, many observers thought bitcoin's time was up. Although bitcoin endured the ride, this showed – once more – just how volatile bitcoin's price is in reaction to regulatory shifts... and to Elon Musk's tweets.

The push which sent bitcoin on its rollercoaster ride can be traced back to a tweet by Tesla CEO Elon Musk, who said the company will stop accepting bitcoin as payment, contrary to an earlier announcement. This policy was updated for environmental reasons, Musk said. Although bitcoin accounts for less than 1% of global electricity consumption, it's still responsible for a large amount, especially when a portion of that electricity is derived from coal.

What followed in just one hour after Musk's tweet was a fine example of panic-selling. A large amount of bitcoin was instantly converted back to US dollars. Bitcoin stabilised soon after, but its value was still 50% lower from an all-time price in May.

The news that China's Central Bank reiterated its cryptocurrency ban continued to fuel the fluctuations in bitcoin's price. The ban was actually nothing new: In early 2020, China announced that it was banning financial institutions from trading in cryptocurrency.

News reports also emerged of **a large bitcoin mining industry being shut down in inland China,** due to environmental concerns. Some observers have noted that this is in line with the country's push to meet its CO2 emission goals. The mining exodus created an opportunity for miners in other countries to grab hold of the vacated mining operations. Chinese government officials confirmed they would start to crack down on bitcoin mining and trading behaviour.



Another plunge in bitcoin's price was in reaction to the US Treasury's proposal for cryptocurrency transfers over US$10,000 to be reported to the Internal Revenue Service. The fact that the government cannot confiscate cryptocurrency funds, or order networks to shut down, is a coveted characteristic of cryptocurrency. Without it, cryptocurrency ceases to be as attractive to those who want to move large sums around.

The Biden administration's tax enforcement is very likely to introduce these new limitations on trading. Once successful, this could potentially slow down the trading volume in the USA and as a consequence, throughout the rest of the cryptocurrency market.

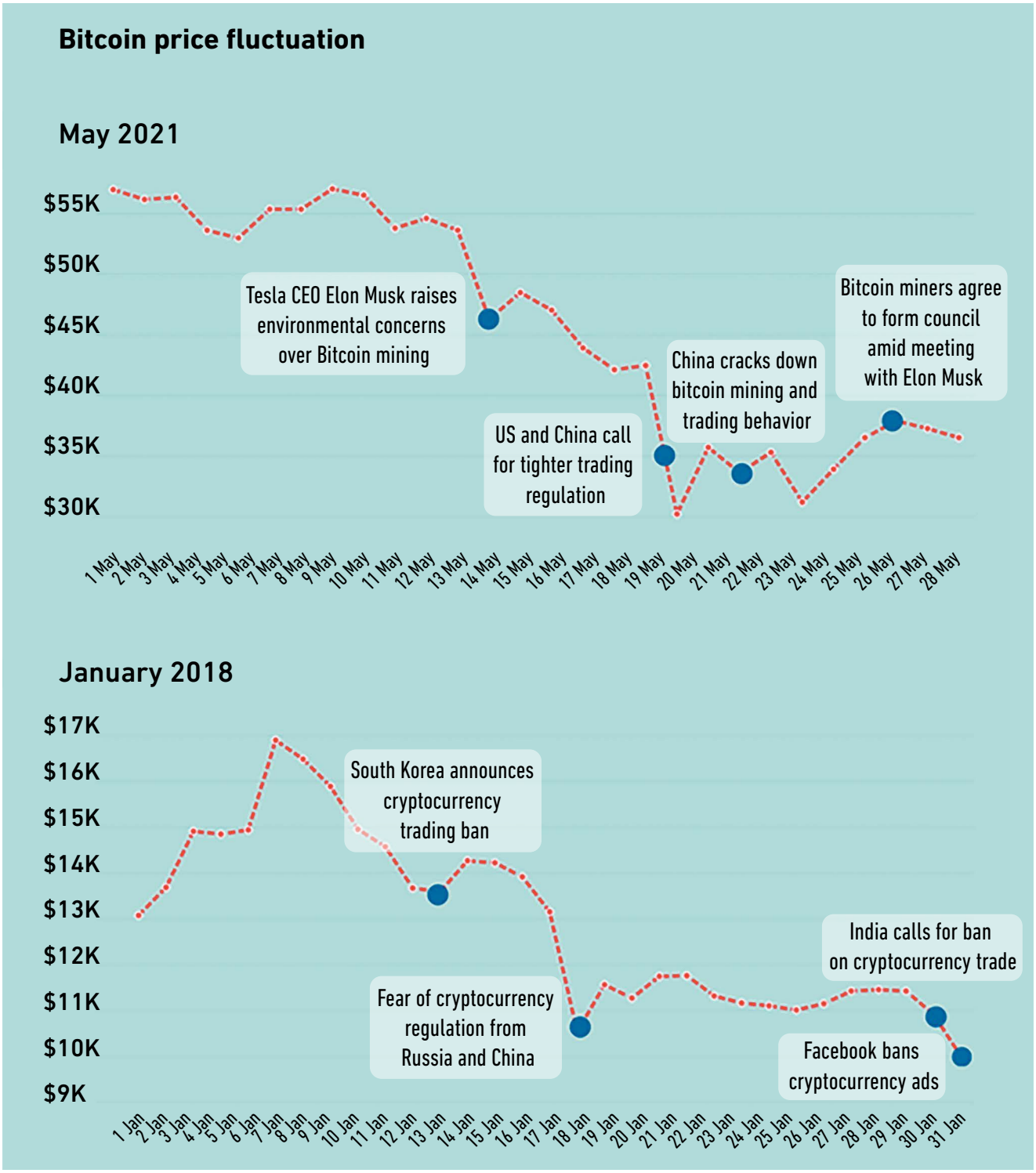
Bitcoin's price also dipped in reaction to the large-scale ransomware attacks, reported in May. This includes the Colonial Pipeline attack, and that on Ireland's healthcare system. In both cases, the perpetrators demanded a bitcoin ransom. This cemented the idea that cryptocurrency is criminals' preferred choice.

Bitcoin enthusiasts did not need these recent attacks to realise that cybercriminals are increasingly misusing cryptocurrency for illegal purposes, such as money laundering and blackmarkets. Governments have long been concerned about this problem, and have been slowly introducing cryptocurrency regulations. The industry has also been investing in financial and technological solutions for examining and tracking blockchain entries.

The regulations are aimed not only at countering abuse, but also to protect citizens from the financial damage caused by wild fluctuations. Governments know that cryptocurrencies are poor stores of value, mostly due to intense speculation associated with them. Yet, crypto is as much a financial phenomenon as it is a cultural one.

As is usually the case with many investor markets, the price of bitcoin is sensitive to public speculation,

fear and uncertainty, and other triggers. Regulated financial markets, such as the bonds, stocks, or currency markets, are closely monitored by financial authorities. When it comes to bitcoin's highly speculative market and the lack of oversight, however, it remains a bumpy and unsafe ride for investors.



News and tweets, and their impact on bitcoin prices

GDPR turns 3: Flexing enforcement muscles

On 25 May, the EU's General Data Protection Regulation celebrated its third anniversary since entering into force. Throughout this time, the regulation brought the issue of data protection to everyone's attention, from citizens and companies to national administrations and what the EU calls third countries.

Much of the attention has been focused on the significant fines and sanctions that this regulation now sets in case of data protection violations. The total amount of fines handed out comes to around €300 million.

There's also a trend: Sanctions have increased over the years, and as a result, so has the total amount of GDPR fines.

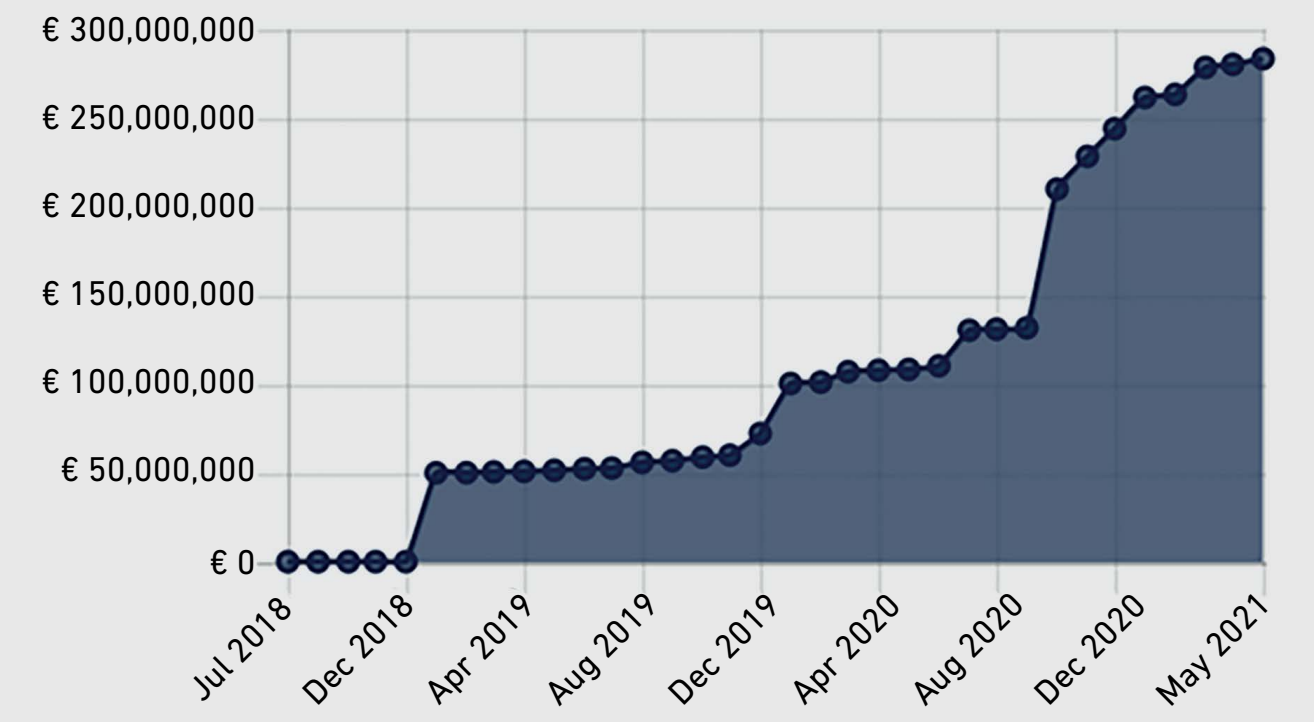
Behind this trend is a diverse mix of practices and actions taken by EU countries. Five countries – Italy, France, Germany, the UK, and Spain – account for the large majority of all GDPR fines.

The total sum of fines is the highest in Italy, followed closely by France. Spain is the member state that has issued the highest number of individual fines, far more than any other country. In terms of legal grounds, insufficient legal basis for data processing and a lack of technical and organisational measures are the main justifications for GDPR fines.

The fact that Ireland does not appear in this ranking is striking, yet rather unsurprising. In charge of regulating the many internet companies headquartered on its territory, including Google and Facebook, the Irish Data Protection Commission (DPC) has so far followed a slow pace in enforcing the GDPR – too slow, many are arguing.

Multiple investigations into tech giants are currently underway. The latest is into Facebook's practices following April's massive data leak. As many as half of the Irish authority's 27 cross-border investigations are related to Facebook and its WhatsApp and Instagram services. The slow pace of the investigations, however, goes contrary to the GDPR's requirement to tackle complaints 'without delay'. This has made the European Parliament unhappy, and in fact, MEPs are now calling on the European Commission to kick off infringement procedures.

Responding to criticism regarding the DPC's limited actions, DPC head Helen Dixon blames the 'one-stop shop mechanism' for slowing the enforcement process down and draining resources. This mechanism created by the GDPR sets the process by which national data protection authorities coordinate and reach decisions in the case of cross-border investigations.



Cumulative sum of GDPR fines between 2018 and 2021 (Source: www.enforcementtracker.com)

	Country	Sum of Fines
	ITALY	€ 76,271,601 (at 77 fines)
	FRANCE	€ 54,551,300 (at 14 fines)
	GERMANY	€ 49,186,833 (at 30 fines)
	UNITED KINGDOM	€ 44,221,000 (at 4 fines)
	SPAIN	€ 29,519,410 (at 229 fines)
	SWEDEN	€ 12,332,430 (at 17 fines)
	THE NETHERLANDS	€ 5,552,500 (at 12 fines)
	BULGARIA	€ 3,210,690 (at 20 fines)
	POLAND	€ 2,061,498 (at 24 fines)
	NORWAY	€ 1,316,550 (at 27 fines)

European countries with highest fines (Source: www.enforcementtracker.com)

Other national authorities have not shied away from issuing hefty sanctions. **The highest fine recorded so far was imposed by the French data protection authority (CNIL), with a €50 million penalty against Google in 2019.**

The reason behind this mega-penalty was what the authority said was a lack of transparency by and inadequate information for users from Google. The company also failed to obtain the required consent from users before implementing personalisation mechanisms for its adverts.

The investigation was initially triggered by group complaints from the associations None Of Your Business (noyb) and La Quadrature du Net. A number of complaints by these civil society groups are still being investigated in France, Germany, Sweden, and Austria. The latest is the legal complaint filed by several digital rights organisations with data protection authorities across Europe, on 26 May, against the facial recognition company Clearview AI.

The fines imposed by some EU countries compared to others says a lot about the GDPR's enforcement, and what will happen in the next three years. Existing imbalances create legitimate frustration for users and lead to unfair competition between companies.

This reluctance 'does not only lead to gross violations of citizens' rights, but also leads to unfair competition', argues noyb. 'Some players on the European market may not feel the need to comply, while others are worried about the possibility of fines.'

Observers are now advocating for reforming data protection law at the EU level, arguing that the GDPR is not fit for purpose, and should evolve. This debate will pick up speed, as more actors join the cause. Imbalances in enforcing the GDPR will be the biggest challenge for the EU and its member states in the coming years.

	Cotroller	Sector	Country	Fine [€]	Type of violation	Date
1	Google Inc.	Media, Telecoms and Broadcasting	FRANCE	50,000,000	Insufficient legal basis for data processing	21 Jan 2019
2	H&M Hennes & Mauritz Online Shop A.B. & Co. KG	Employment	GERMANY	35,258,708	Insufficient legal basis for data processing	01 Oct 2020
3	TIM (telecommunications operator)	Media, Telecoms and Broadcasting	ITALY	28,800,000	Insufficient legal basis for data processing	15 Jan 2020
4	British Airways	Transportation and energy	UNITED KINGDOM	22,046,000	Insufficient technical and organisational mesures to ensure information security	16 Oct 2020
5	Marrriott International, Inc.	Accomodation and Hospitality	UNITED KINGDOM	20,450,000	Insufficient technical and organisational mesures to ensure information security	30 Oct 2020

Top 5 GDPR Fines (Source: www.enforcementtracker.com)

Colonial Pipeline attack: Forcing the USA's hand?

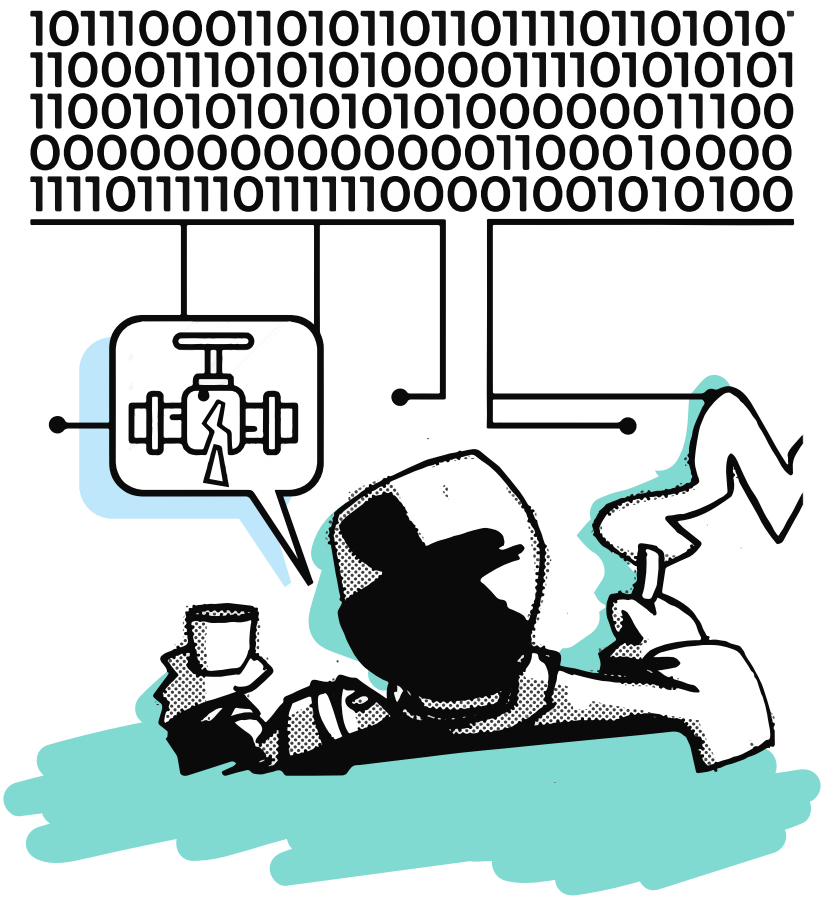
On 8 May, Colonial Pipeline, one of the largest oil and gas pipeline operators in the USA, was forced to halt its operations and freeze its IT systems following a ransomware attack. Almost half of the east coast was affected.

The Russian group DarkSide, confirmed by the FBI as the (non-state) actor behind the attack, is known for attacking only English-speaking countries and avoiding former Soviet countries altogether.

In a bid to restore its operations quickly, Colonial paid around 75 bitcoin, the equivalent US$4.4 million. It received the decrypting software – albeit a very slow tool – from the hackers soon after. Colonial restarted their operations five days later; it took a few more days for the supply chain to return to normal.

The pipeline attack has placed extra pressure on the US government to rethink its cybersecurity approach. DarkSide's announcement that it would be shutting down its operations is not reassuring, as the criminals could easily regroup under a new name. Plus, there are hundreds of other malicious actors lurking in the dark web. As we wrote last month in connection with the SolarWinds attack, experts have been asking whether the USA should beef up its defences.

President Joe Biden responded with an Executive Order on securing US supply chains, signed on 12 May. Three elements are particularly important.



The first is that the National Institute of Standards and Technology (NIST) will take the lead in developing new security standards. This will directly impact the industry producing critical software, but eventually extend to consumer software.

The second is that the executive order paves the way for closer collaboration between the Department of Defence and Department of Homeland Security to quickly detect and respond to attacks on federal networks. Linked to this is the obligation for companies to share breach information that can impact government systems.

The third is that a new Cyber Safety Review Board will be tasked with probing significant cyber incidents. It will be co-chaired by government and private sector leads – a clear signal that both stakeholders are in need of each other.

What stands out, therefore, is that **although the Executive Order is aimed at protecting federal systems, it will also impact the protection of critical infrastructure in the USA**. As private sector observers have commented, 'In many ways, the federal government's most powerful tool for influencing the private sector is its own purchasing power. By including cybersecurity requirements in purchasing contracts, the government can influence a wide swath of the private sector.'

Policy updates from International Geneva

Many policy discussions take place in Geneva every month. In this space, we update you with all that's been happening in May. For other event reports, visit the Past Events section on the *GIP Digital Watch* observatory.

COVID-19, Health under Threat: A Cyber Perspective 18 May 2021

This event, organised by the Permanent Missions of the Kingdom of the Netherlands and Switzerland to the United Nations Office, explored the arrays of action for the international community to ensure the protection and resilience of the health sector, which has been the target of malicious cyberattacks during the pandemic.

Cyberattacks against the sector, which are unavoidable due to various possibilities for criminals to reap financial benefits, compromise societies' trust, disrupt health services, and put lives at risk. A preventive approach should be taken by rendering the health sector more prepared to defend itself against cyberattacks, persistently investing in financial and technological resources and building required capacities.

A comprehensive, coordinated, multidimensional, and multistakeholder approach is key in securing cyber resilience in the health sector. This requires acknowledging cybersecurity as critical infrastructure, engaging state responsibility to bring criminal groups to justice, as well as operationalising legal and technical instruments and enhancing interstate enforcement cooperation mechanisms. Civil society too can take an active role by documenting what is happening to people and elevating relevant information and risks to policymakers.

Road to Bern via Geneva Dialogue: Environmental Data 19 May 2021

The 6th dialogue, co-hosted by the United Nations Environment Program (UNEP), the World Trade Organization (WTO), and the Geneva Environmental Network, looked at how to use data and digital technologies to advance sustainable trade and environmental transparency.

The discussion comprised two sessions. The first panel provided an overview of various issues on trade and environment transparency outlining a range of different ways in which digital technologies, tools, and data can support transparency and advance more sustainable trade. The second panel talked about digital product passports and their implications for the environment and for trade.

Navigating Digital Geneva: A Digital Environment Tour 26 May 2021

The roundtable discussion, organised by the Geneva Internet Platform as part of the 12 Tours to Navigate Digital Geneva series, debated the interplay between digital technologies and the environment. The discussion was approached from two standpoints: data and the circular economy.

Sophisticated AI tools are already being used for complex numerical analyses related to weather prediction, and at the same time work is underway on how the latest technological developments, especially those regarding the collection and analysis of aerial data, can help to favour biodiversity in the broader Geneva region. *Read our event report.*

What to watch for: Global digital policy events in June

Let's look ahead at the global digital policy calendar. Here's what will take place next month around the globe. For even more events, visit the Events section on the *Digital Watch* observatory.

June

7–11 June, RightsCon (online)

Organised by AccessNow, RightsCon is celebrating its 10th anniversary with a programme of 500+ sessions, sorted into 20 programme categories. These include content control, internet access, democracy and elections, civil society resistance, and AI.

11–13 June, G7 (Cornwall, UK)

Aiming to 'build back better from coronavirus,' the G7 meeting has set as policy priorities (a) leading the global recovery from coronavirus, (b) championing free and fair trade to promote prosperity, (c) tackling climate change, and (d) promoting shared values such as global development and democracy, supporting girls' education, food security, health and sustainable development financing. Leaders are also expected to reach agreement over plans for a digital tax. The G7 is chaired by the UK, who extended the invitation to the meeting to Australia, India, South Korea, and South Africa.

14 June, NATO Summit (Brussels, Belgium)

The 31st formal meeting of NATO Heads of State and Government Summit will address decisions on the NATO 2030 agenda, dealing with the threat of terrorism, cyberattacks, emerging and disruptive technologies, and the security impact of climate change.

14–17 June, ICANN 71 (online)

ICANN71 Policy Forum will be held as a Virtual Public Meeting, preceded by a preparatory week. During the forum, ICANN supporting organisations, the advisory committee and broader ICANN community will discuss various issues pertaining to ICANN's activity and the management of the domain name system.

28–30 June, EuroDIG 2021 (online)

The regional internet governance forum will tackle access and literacy issues; development of the internet governance ecosystem; human rights; innovation and economic issues; media and content; security and crime; and technical and operational issues. Special focus sessions will be held on green internet governance and sustainability, the role of Europe in governing digital interdependence, the EU's new proposals on cybersecurity, and on (re)creating a trusted public sphere in the European mediascape.

July

About this issue

Editor's note: A heartfelt thank you to all our readers for following us month after month, on behalf of all the people who make our newsletters shine.

Issue 60 of the *Digital Watch* newsletter, published on 4 June 2021 by the Geneva Internet Platform and DiploFoundation | Contributors: Katarina Anđjelković, Stephanie Borg Psaila (editor), Andrijana Gavrilović, Tereza Horejsova, Pavlina Ittelson, Arvin Kamberi, Marco Lotti, Boris Ohanyan, Virginia (Ginger) Paque, Clement Perarnaud, Nataša Perućica, and Sorina Teleanu | Editing and design: Dorijan Najdovski, Aleksandar Nedeljkov, Viktor Mijatović, and Mina Mudrić | On the cover: (Not) on social media. Credit: Vladimir Veljašević | Get in touch: digitalwatch@diplomacy.edu

On the cover

(Not) on social media. Credit: Vladimir Veljasević

The Geneva Internet Platform is an initiative of:

GENEVA INTERNET PLATFORM digwatch

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

REPUBLIQUE ET CANTON DE GENEVE

DiPLO www.diplomacy.edu