MONITORING REPORT

N. 24/2019

efamro

the European Research Federation

IN THIS ISSUE

THE EP RESEARCH SERVICE PUBLISHES BACKGROUND NOTE ON ECJ RIGHT TO BE FORGOTTEN

DELIVERING ITS JUDGMENT IN GOOGLE V COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL) ON 24 SEPTEMBER 2019, THE COURT OF JUSTICE OF THE EUROPEAN UNION (CJEU) HELD THAT GOOGLE DOES NOT HAVE TO REMOVE SEARCH ENGINE RESULTS WORLDWIDE IN ORDER TO COMPLY WITH A 'RIGHT TO BE FORGOTTEN' REQUEST UNDER EU DATA PROTECTION LAW. THE LANDMARK DECISION LIMITS THE TERRITORIAL SCOPE OF THE EU RIGHT TO DE-REFERENCING BUT LEAVES MANY OPEN QUESTIONS

Author: Tambiama Madiega. Available here

Background 2014 Google Spain v Agencia Española de Protección de Datos (AEPD) case

In its 2014 Google Spain ruling, the CJEU held that under the Data Protection Directive, citizens in the EU have a right to request search engines such as Google to remove links to personal information when this information is 'inadequate, irrelevant or no longer relevant'. As a result, search engines must ensure that the personal information in question cannot be found through online searches on the individual's name, even though the content itself remains online. Such a right to de-referencing or delisting is commonly referred to as the 'right to be forgotten'. Although, the Article 29 Working Party (now the European Data Protection Board), an EU advisory body on data protection, issued some guidelines on the implementation of the Google Spain judgment, the territorial scope of the 'right to be forgotten' was not fully clarified.

Internet users in the EU have increasingly used the right to de-referencing. Since June 2014, Google has processed more than 850 000 requests to remove more than 3.3 million website addresses (i.e. uniform resource locators or URLs) from its search engine. Google ultimately delisted more than 1.3 million website addresses (around 45 % of the website addresses) (See Google transparency report).

2018 General Data Protection Regulation and the 'right to be forgotten'

The General Data Protection Regulation (GDPR) replaced the Data Protection Directive from 25 May 2018 and enshrined a 'right to erasure' into EU law to strengthen the 'right to be forgotten' online. Pursuant to Article 17 GDPR, individuals have the right to have their personal data erased without undue delay; and the right to end any processing of the data where such data are no longer necessary in relation to the purposes for which they are collected, or where the individual has withdrawn their consent or objected to the processing of personal data. Furthermore, companies and organisations that are considered data controllers under Article 4(7) GDPR must comply with individuals' requests to take down links to personal information. In a limited set of circumstances, this general obligation does not apply, including when the personal data are needed to exercise the right of freedom of expression, when there is a legal obligation to keep that data, and for reasons of public interest such as public health or statistical research purposes.

2019 Google v Commission nationale de l'informatique et des libertés (CNIL) case

The question of the territorial scope of the 'right to be forgotten' was central to the dispute arising between the French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés, or CNIL) and Google. The CNIL asked Google, in its Decision 2015-047, to remove, on a worldwide basis, the links to web pagesfrom the list of results displayed following a search conducted based on a person's name. Google refused to comply with that formal notice, and appealed the CNIL decision to fine Google for its refusal. The case reached the French supreme administrative court (Conseil d'Etat), which in turn referred a question on the interpretation of the territorial scope of the right to be forgotten to the CJEU for a preliminary ruling. The court asked the CJEU to clarify whether a search engine operator is obliged to carry out de-referencing on all search engines worldwide, on search engines provided in the European Union, or only on the search engine of the Member State in which the person concerned requested de-referencing.

CJEU decision in Google v CNIL

Key findings The CJEU Grand Chamber judgment Google v CNIL (C-507/17), delivered on 24 September 2019, finds that:

¬ As matter of principle, under the Data Protection Directive and under the GDPR, search engine operators are not required to carry out de-referencing on all versions of its search engine (i.e. worldwide de-referencing). The Court argues that numerous third countries do not recognize the right to de-referencing or have a different approach to this right and that EU law only envisages providing a high-level protection for personal data within the Union.

¬ As a result, search engine operators are asked to carry out de-referencing on versions corresponding to all EU Member States (i.e. EU-wide de-referencing), to ensure a consistent and high level of protection throughout the EU.

¬ However, the right to data protection is not an absolute right. A balance must be struck between the rights to privacy and protection of personal data guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights of the EU, and the right to freedom of information guaranteed by Article 11 of the Charter, to decide the territorial scope of de-referencing.

¬ Furthermore, EU law does not per se prohibit global de-referencing. The authorities of the Member States remain competent to weigh up, in the light of national standards of protection of fundamental rights, a user's right to privacy and the protection of their personal data, and the right to freedom of information. After weighing those rights against each other, where appropriate, a national authority could order the search engine operator to carry out de-referencing concerning all versions of that search engine.

¬ Finally, search engines operators must put geo-blocking measures in place to effectively prevent or, at the very least, seriously discourage, internet users in the Member States from gaining access to the links, which appear on versions of that search engine outside the EU.

First reactions and comments

The French supreme administrative court must now decide on the merits of the case at national level in light of the CJEU decision. CNIL stresses that one of the key issues for the French court will be to assess whether Google geo-blocking measures are adequate in the specific case at hand. Stakeholders from civil society and the technology sector were rather supportive of the CJEU decision. Article 19, an advocacy group for freedom of expression rights, welcomed the outcome of the case as a victory for freedom of expression. The Computer and Communications Industry Association stressed that the Court's decision recognizes search engines' efforts to guarantee EU residents' rights to be delisted without compromising constitutional guarantees from countries outside the EU, including when freedom of information is at stake.

However, academics and commentators’ question whether the decision provides suitable guidance on the territorial scope of the 'right to be forgotten'. Some academics emphasize that the CJEU decision leaves national authorities the opportunity to impose a worldwide 'right to be forgotten' and argue this creates a risk of fragmentation in the enforcement of the 'right to be forgotten' in the EU. Other experts stress the discrepancy between the accessibility of data worldwide and the 'right to be forgotten' territorial scope of application and call for the EU legislator to intervene to provide clarification.

Potential inconsistencies between several recent CJEU decisions regarding the territorial scope of EU law applied to the online environment have been pointed out. In Google v CNIL the CJEU limits the extraterritorial application of the GDPR, while in Glawischnig-Piesczek v Facebook, it imposes no territorial limitation on the removal or blocking of illegal online content in the application of the 2000/31 E-Commerce Directive. Furthermore, EU Directive 2017/541 on combatting terrorism imposes an obligation on Member States to obtain the removal of terrorist content hosted outside their territory.

EDPS GUIDELINES ON THE CONCEPTS OF CONTROLLER, PROCESSOR AND JOINT CONTROLLERSHIP

While these guidelines are aimed at the Data Protection Officers, Data Protection Coordinators and all persons having responsibility within the EUIs for the processing operations of personal data, other external organisations might equally find them useful.

The guidelines focus on:

- the concepts of controller, processor and joint controllership;
- the distribution of their obligations and responsibilities, in particular when dealing with the exercise of the rights of data subjects;
- specific case studies on controller-processor, separate controllership and joint controllership situations.

The identification and assessment of whether EUIs may be considered as controllers, processors or joint controllers, together with their respective duties are presented in flowcharts and checklists.

These guidelines will also be useful to senior management in supporting a culture of data protection from the top of the organization and to implement the principle of accountability.

They are available here

EDPS “FACIAL RECOGNITION: A SOLUTION IN SEARCH OF A PROBLEM?”

BY **WOJCIECH WIEWIÓROWSKI** *ACTING EUROPEAN DATA PROTECTION SUPERVISOR*

“Be water”. This is the evocative and enigmatic phrase of the current mask-wearing protestors in Hong-Kong. It seems to represent the fight of citizens for the right to be shapeless and anonymous among the crowd, including when exercising the right to protest, versus surveillance by the state authorities.

It is undeniable that facial recognition, the biometric application used to identify or verify a person’s identity, has become increasingly present in many aspects of daily life. It is used for ‘tagging’ people on social media platforms and to unlock smart phones. In China it is used for airport check-in, for monitoring the attentiveness of pupils at school and even for dispensing paper in public latrines.

In the general absence of specific regulation so far, private companies and public bodies in both democracies and authoritarian states have been adopting this technology for a variety of uses. There is no consensus in society about the ethics of facial recognition, and doubts are growing as to its compliance with the law as well as its ethical sustainability over the long term.

The purposes that triggered the introduction of facial recognition may seem uncontroversial at a first sight: it seems unobjectionable to use it to verify a person’s identity against a presented facial image, such as at national borders including in the EU. It is another level of intrusion to use it to determine the identity of an unknown person by comparing her image against an extensive database of images of known individuals.

In your face

There appear to be two big drivers behind this trend.

Firstly, politicians react to a popular sense of insecurity or fear that associates the movements of foreigners across borders with crime and terrorism. Facial recognition presents itself as a force for efficient security, public order and border control. Facial recognition is a key component of the general surveillance apparatus deployed to control the Uighur population in Xinjiang, justified by the government on grounds of combating terrorism.

The second justification is the lure of avoiding physical and mental efforts - ‘convenience’: some people would prefer to be able to access to an area or a service without having to produce a document.

France aims to be the first European country to use such technology for granting a digital identity. Meanwhile the Swedish data protection authority recently imposed a fine on a school for testing facial recognition technology to track its students’ attendance.
Although there was no great debate on facial recognition during the passage of negotiations on the GDPR and the law enforcement data protection directive, the legislation was designed so that it could adapt over time as technologies evolved.

Face/Off

The privacy and data protection issues with facial recognition, like all forms of data mining and surveillance, are quite straightforward.

First, EU data protection rules clearly cover the processing of biometric data, which includes facial images: ‘relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person’ (GDPR Art. 2(14)). The GDPR generally forbids the processing of biometric data for uniquely identifying purposes unless one can rely on one of the ten exemptions listed in Art. 9(2).

Second, any interference in fundamental rights under the Article 52 of the Charter must be demonstrably necessary. The bar for this test becomes higher the deeper the interference. Is there any evidence yet that we need the technology at all? Are there really no other less intrusive means to achieve the same goal? Obviously, 'efficiency' and 'convenience' could not stand as sufficient.

Third, could there be a valid legal basis for the application of such technology given that it relies on the large-scale processing of sensitive data? Consent would need to be explicit as well as freely-given, informed and specific. Yet unquestionably a person cannot opt out, still less opt in, when they need access to public spaces that are covered by facial recognition surveillance. Under Article 9(2)(g) the national and EU legislators have the discretion to decide the cases where the use of this technology guarantees a proportionate and necessary interference with human rights.

Fourth, accountability and transparency. The deployment of this technology so far has been marked by obscurity. We basically don't know how data is used by those who collect it, who has access and to whom it is sent, how long do they keep it, how a profile is formed and who is responsible at the end for the automated decision-making. Furthermore, it is almost impossible to trace the origin of the input data; facial recognition systems are fed by numerous images collected by the internet and social media without our permission. Consequently, anyone could become the victim of an algorithm's cold testimony and be categorised (and more than likely discriminated) accordingly.

Finally, the compliance of the technology with principles like data minimisation and the data protection by design obligation is highly doubtful. Facial recognition technology has never been fully accurate, and this has serious consequences for individuals being falsely identified whether as criminals or otherwise. The goal of 'accuracy' implies a logic that irresistibly leads towards an endless collection of (sensitive) data to perfect an ultimately unperfectible algorithm. In fact, there will never be enough data to eliminate bias and the risk of false positives or false negatives.

Saving face

It would be a mistake, however, to focus only on privacy issues. This is fundamentally an ethical question for a democratic society.

A person's face is a precious and fragile element her identity and sense of uniqueness. It will change in appearance over time and she might choose to obscure or to cosmetically change it - that is her basic freedom. Turning the human face into another object for measurement and categorisation by automated processes controlled by powerful companies and governments touches the right to human dignity - even without the threat of it being used as a tool for oppression by an authoritarian state.

Moreover, it tends to be tested on the poorest and most vulnerable in society, ethnic minorities, migrants and children.

Where combined with other publicly available information and the techniques of Big Data, it could obviously chill individual freedom of expression and association. In Hong Kong the face has become a focal point. The wearing of masks has been a reaction to the use of facial recognition and in turn has been prohibited under a new law.

Does my face look bothered?

It seems that facial recognition is being promoted as a solution for a problem that does not exist. That is why a number of jurisdictions around the world have moved to impose a moratorium on the use of the technology.

We need to assess not only the technology on its own merits, but also the likely direction of travel if it continues to be deployed more and more widely. The next stage will be pressure to adopt other forms of objectification of the human being, gait, emotions, brainwaves. Now is the moment for the EU, as it discusses the ethics of AI and the need for regulation, to determine whether- if ever - facial recognition technology can be permitted in a democratic society. If the answer is yes, only then do we turn questions of how and safeguards and accountability to be put in place.

Independent DPAs will be proactive in these discussions.

FINLAND EYES EPRIVACY AGREEMENT BEFORE YEAR'S END

Jennifer Baker for IAPP

The Presidency of the EU Council is expected to propose yet another iteration of the ePrivacy text for the next meeting of the Working Party on Telecommunications and Information Society Nov. 7.

Ever since the European Commission first presented its plans to overhaul the ePrivacy law in January 2017, the file has been mired in lobbying and conflicting positions of EU member states. In fact, until Finland took over the presidency in July, it appeared to be completely stalled.

Sources within the Finnish Justice Ministry told The Privacy Advisor they are keen to get an agreement between member states before the end of the year. Only then can the council negotiations move on a final text with the commission and the European Parliament.

Gabriela Zanfir-Fortuna, senior counsel at the Future of Privacy Forum, agreed. “All signs from Brussels point to the general agreement being on the horizon in the council, with the Finnish Presidency looking adamant on delivering as much as possible on this file. The ambition is to reach an agreement, and the presidency has until the end of the year to reach it. However, once the trilogue finally starts, I doubt it will be smooth sailing. There are some differences between the European Parliament’s negotiating mandate and the current draft of the council, particularly on permissible uses, and this may trigger again delays,” she said.

Dutch MEP Sophie in ’t Veld also sounded a warning note regarding trilogue negotiations: “We are waiting for the council to move. We’ll see when there are results, but on the whole, my expectations are not very high. The national governments tend to have a double agenda: They want to regulate tech-giants, while keeping access to the data gold mines, for security purposes. So I expect difficult trilogues. One would say even national governments have learned a few lessons from disasters like Cambridge Analytica, and from a raft of court rulings (not least [last] week’s ruling regarding cookie consent), yet they seem to be unfazed by all that.”

But a common position hasn’t been reached between the EU countries yet. On Sept. 18, the Finns put forward an 88-page compromise proposal with considerable changes and amendments. According to sources, only Germany and Spain gave vocal support for the text, while France and Poland are vehemently against it. Italy is also against agreeing a common position as it believes the new European Commission should sit before a decision is made on such an important file — something that is currently stalled for political reasons.

A new commission is, however, unlikely to make a huge difference to the file, since the new digital vice president will be Margrethe Vestager, who has already voiced her support for the law. To untangle all these political knots, it is likely that the national negotiators will have to begin Committee of Permanent Residents meetings in mid-November.

The law itself

The ePrivacy Regulation will in effect set out what is and isn’t confidential in electronic communications, as well as the general tracking of internet users, and will replace the 2002 e-Communication and Privacy Directive (2002/58/EC). It is intended to cut down on pre-ticked consent boxes for cookies — meaning websites will have to explain what information they are gathering on users and what they do with it, as well as allowing users to opt out. The Parliament version of the text states that even if users do opt out, the website will still have to provide the service. The “no visit if no cookies” status quo — known as a “cookie wall” — could be a thing of the past, but could also make it difficult for websites to generate revenue through behavioral advertising, which relies on cookies.

More broadly, the regulation is also intended to combat problems such as spam by making consent a requirement for communications.

Currently, companies like Skype, Facebook and Google are not subject to the same rules as telecoms providers and can conduct targeting based on content of communications, but this could be ruled unlawful under some drafts of the new law. Metadata — information about information, time, location, etcetera — is also included in the scope of the legislation, limiting further what online businesses can and can’t do with such (non-personal) information.

Given the model for a huge number of online businesses is based on advertising and the associated cookies and tracking, the potential disruption has alarmed the industry. Several members of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs say that this is the most heavily lobbied piece of legislation they have encountered, surpassing even that of the GDPR. Many of those opposed to the GDPR are now engaged in attempting to block the ePrivacy Regulation — ironically, the organizations that were most opposed to the GDPR now argue that the GDPR is so perfect there is no need for an ePrivacy Regulation.

Lobbying

On Oct. 18, the European Publishers Council, along with nine other European publisher and advertiser trade bodies, wrote a letter asking the council to alter the current text. "The ePrivacy Regulation puts the future financial viability of independent, advertising-funded media at risk," the trade bodies wrote. "Under the current ePrivacy law proposals, publishers and any site owners would need explicit consent in order to use any form of cookie."

They argued that the current draft of the law could seriously damage publisher advertising revenue, while benefiting the major tech platforms whose products make it very easy for users to stay logged in.

However, Alan Toner, policy expert at Brave, also wrote to representatives to urge the prohibition of cookie walls and the inclusion of privacy by default, arguing that there are good economic and practical reasons to reinstate them "Advertising is fundamental to financing the web, but it must respect users' rights and expectations. As technologists, we know that the rights to privacy and data protection enshrined in the European Charter are compatible with innovation. Many companies, including Brave, have developed advertising systems that support publishers with no privacy sacrifice. A robust ePrivacy Regulation will spur further innovation, whereas cookie walls would stifle it. But as currently drafted, the text will permit 'cookie walls' that make pervasive tracking a condition of access to a website. Competition authorities in several member states are examining the problems of the online advertising and media market caused by these same practices," Toner said.

But DigitalEurope's Cecilia Bonefeld Dahl remains concerned.

"This proposal has been problematic for virtually everyone in industry. Many [internet-of-things] sectors such as automotive, medical or construction equipment have joined our call to rethink the text. It would have such a broad application that for many services the ePrivacy Regulation would in practice replace the GDPR," Dahl said. "Importantly, very different AI use cases will have to rely on communications data, device data or both, and inflexible rules will only be detrimental. It's not too late to rewrite the text in a way that avoids hard contrasts with GDPR compliance — this is the right time for the Council and the new Commission to make bold changes."

European Telecommunications Network Operators' Association, GSMA and Cable Europe also issued a joint statement attempting to strike a balance between their concern at stricter regulation and their joy that so-called "over-the-top" services would also have to follow the rules. "While the ePrivacy Regulation proposal rightly seeks to level the playing field between telcos and digital service providers offering similar services, gaps remain. A viable regulatory framework should protect confidentiality and enable us to innovate and provide ever more relevant services to our customers," the open letter said.

"Telcos and cable operators ask for the ability to implement a risk-based approach to processing communications metadata. Legislating for the future means leaving some space for unknown use cases. Rules for processing communication metadata need to be more future-proof and not focus disproportionately on consent," said the organizations.

Recent ruling

However, a ruling from the Court of Justice of the European Union Oct. 1 could supersede such arguments. In the so-called Planet49 case, the European Union's highest court ruled that people must actively choose to let companies install cookies that track their internet browsing — not just check a box by default. Many experts believe this provides legal certainty that will give a boost to the legislative efforts to adopt the ePrivacy Regulation.

Zanfir-Fortuna explained. "The recent judgment of the CJEU in Planet49 concerning the ePrivacy Directive may help speed up the legislative process. One of the points of contention in the council was to define the interaction between ePrivacy and the GDPR, with some even contesting there is a need for a separate law," she said. "The court clarified in the Planet49 case that the ePrivacy regime protects both personal and non-personal data, and this is because it aims to protect the user from interference with his or her private sphere, regardless of whether or not that interference involves personal data'. Hopefully this will bring some clarity."

"I do think it is fair to say that the negotiations will be heavily influenced by the recent CJEU court cases, including of course Planet49. I do think that also the Right to be Forgotten cases and the hate speech case will however make an impact," added Paul Breitbarth, director EU operations and strategy at Nymity.

However, looking ahead to the trilogue negotiations, German MEP Patrick Breyer predicted that tracking walls are "the greatest industry battlefield, but there is also bulk data collection and communications security/encryption where I am concerned the council has moved to unacceptable positions. Clearly publishers and advertising industry are on the forefront of the lobbyism for tracking walls. This is what the much-discussed surveillance capitalism is about, and what their business model is built on."

For now, it looks like we'll wait until November's aforementioned COREPER meetings to find out what progress has been made and how likely it is Finland closes a deal before year's end.

NATIONAL DPAS GUIDANCE

An Coimisiún um
Chosaint Sonraí
Data Protection
Commission

IRISH DPC RELEASES GUIDE TO DATA PROTECTION IMPACT ASSESSMENTS

Under the general data protection regulation, controllers need to undertake a data protection impact assessment (DPIA) for any processing that is '*likely to result in a high risk to individuals*', including some specified types of processing. A DPIA describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. DPIA are important tools for negating risk, and for demonstrating compliance with the GDPR.

Guide to data protection impact assessments: full guidance note .

úřad pro ochranu
osobních údajů
the office for personal
data protection

CZECH DPA LAUNCHES PUBLIC CONSULTATION ON DPIA METHODOLOGY

The DPIA methodology was published for public discussion on the website of the Office for Personal Data Protection. Personal Data Protection Impact Assessments must now be carried out under GDPR by every controller whose intent related to the processing of personal data can be assessed as high risk in terms of interference with the rights and freedoms of individuals.

The methodology for the general privacy impact assessment, which can be found below in PDF format, is open to public consultation. Send your suggestions and comments electronically to posta@uoou.cz by December 15, 2019 . Include **"Methodology - Public Discussion"** in the subject of the email.

- **General Data Protection Methodology** [PDF, 700 kB]

ICO: LIVE FACIAL RECOGNITION TECHNOLOGY – POLICE FORCES NEED TO SLOW DOWN AND JUSTIFY ITS USE

BY ELIZABETH DENHAM, INFORMATION COMMISSIONER.

As far back as Sir Robert Peel, the powers of the police have always been seen as dependent on public support of their actions. It's an ideal starting point as we consider uses of technology like live facial recognition (LFR).

How far should we, as a society, consent to police forces reducing our privacy in order to keep us safe?

That was the starting point to my office's investigation into the trials of LFR by the Metropolitan Police Service (MPS) and South Wales Police (SWP). LFR is a step change in policing techniques; never before have we seen technologies with the potential for such widespread invasiveness. The results of that investigation raise serious concerns about the use of a technology that relies on huge amounts of sensitive personal information.

We found that the current combination of laws, codes and practices relating to LFR will not drive the ethical and legal approach that's needed to truly manage the risk that this technology presents.

Full story on ICO blog

NETHERLANDS: AP PUBLISHES GUIDANCE ON THE LEGAL BASES FOR PERSONAL DATA PROCESSING

THE AP CONTINUES THE CAMPAIGN 'WHAT DOES THE PRIVACY LAW MEAN FOR YOU (YOUR COMPANY)?' TODAY WITH PRACTICAL INFORMATION ABOUT THE FOUNDATIONS FOR THE PROCESSING OF PERSONAL DATA.

The guidance, only available in Dutch, is here

ENFORCEMENT

THE POLISH SUPERVISORY AUTHORITY IMPOSED FIRST ADMINISTRATIVE FINE ON A PUBLIC ENTITY

THE PRESIDENT OF THE PERSONAL DATA PROTECTION OFFICE ("THE PRESIDENT OF THE OFFICE") IMPOSED FIRST ADMINISTRATIVE FINE OF PLN 40,000 ON A PUBLIC ENTITY FOR FAILURE TO COMPLY WITH THE GDPR. THE REASON FOR IMPOSING THE FINE WAS THAT THE MAYOR OF THE CITY DID NOT CONCLUDE A PERSONAL DATA PROCESSING AGREEMENT WITH THE ENTITIES TO WHICH HE TRANSFERRED DATA.

The data processing agreement was not concluded with a company whose servers hosted the resources of the Public Information Bulletin (BIP) of the City Hall in Aleksandrów Kujawski. Such an agreement was also not concluded with another company, which provided software to create BIP and provided service in this area. The President of the Office concluded that Article 28 (3) of the GDPR had been violated. This provision obliges the controller, on behalf of whom personal data processing is performed by another entity, to conclude data processing agreement with him.

As a consequence of the absence of such an agreement, the mayor committed the act of sharing personal data without a legal basis, which violated the principle of lawfulness of processing (Article 5(1)(a) of the GDPR) and the principle of confidentiality (Article 5(1)(f) of the GDPR).

However, these are not the only violations established during the control procedure conducted by the President of the Office. It was also found that there were no internal procedures in place to review the resources available in the BIP in order to determine the timing of their publication. This caused, for example, that in the BIP the property declarations from 2010 were available, among others, while the period of their storage is 6 years, which results from the sectoral regulations. n. In the case of data whose retention period is not regulated by law, the controller should determine it himself in accordance with the purposes for which he is processing them. Therefore, the controller violated the principle of storage limitation, set forth in Article 5(1)(e) of the GDPR.

It was also established during the investigation that the recorded materials from the city council meetings were available in the BIP only through a link to a dedicated YouTube channel. There were no back-up copies of these recordings at the Municipal Office. Thus, in case of loss of data stored on YouTube, the controller would not have at his disposal the recordings. No risk analysis was carried out for the publication of recordings from board meetings exclusively on YouTube. Thus, the principles of integrity and confidentiality were infringed (Article 5(1)(f) of the GDPR) as well as the principle of accountability (Article 5(2) of the GDPR).

The principle of accountability was also breached in connection with the shortcomings in the register of processing activities. For example, it did not indicate all data recipients, nor did it indicate the planned date of data deletion for certain processing activities.

When imposing a penalty, the President of the Office took into account the fact that despite the irregularities found in the course of the proceedings, the controller did not remove them or implement solutions aimed at preventing future infringements. The controller also did not cooperate with the supervisory authority. Therefore, the President of the Office decided that there were no premises that could mitigate the amount of the fine.

Apart from the financial penalty, the President of the Office also ordered the controller to take action to remedy the relevant infringements within 60 days.

To read the full press release in Polish, click here

THE ROMANIAN SUPERVISORY AUTHORITY FINES RAIFFEISEN BANK S.A. AND VREAU CREDIT S.R.L.

On the 1st of October 2019, the National Supervisory Authority finalised two investigations at **Raiffeisen Bank S.A. and Vreau Credit S.R.L.** noting the following:

- **Raiffeisen Bank S.A.** infringed the provisions of **Article 32 paragraph (4) in conjunction with Article 32 paragraph (1) and paragraph (2) of the GDPR**, which led to imposing an administrative fine in the amount of 150,000 Euros

- **Vreau Credit S.R.L.** infringed the provisions of **Article 32 paragraph (4) in conjunction with Article 32 paragraph (1) and paragraph (2) of the GDPR**, as well as of Article 33 paragraph (1) of the GDPR, which led to imposing an administrative fine in the amount of 20,000 Euros.

As regards **Raiffeisen Bank S.A.**, the National Supervisory Authority has initiated an investigation, following the notification of a personal data breach to the supervisory authority, by filling in the form on the personal data breach in compliance with Regulation (EU) 2016/679.

The breach of security consisted in the fact that two employees of Raiffeisen Bank S.A., **using the data from the identity documents of some natural persons**, transmitted by the employees of the company Vreau Credit S.R.L. through the WhatsApp mobile application, **performed queries to the Credit Bureau system** to obtain the necessary data in order to determine the eligibility to credit of the respective individuals, through prescoring simulations. In this respect, 1194 simulations were performed, with regards to 1177 individuals.

Also, for 124 individuals, the database of the National Agency for Fiscal Administration (NAFA) was also consulted.

The above mentioned prescoring simulations were performed through the computer application used by Raiffeisen Bank S.A. in the crediting activity, and the negative crediting decision was communicated by the employees of Raiffeisen Bank S.A. to the employees of Vreau Credit S.R.L., with the infringement of the internal procedures.

The sanction was imposed to the controller **due to the fact that it did not implement the appropriate measures in order to ensure that any natural person acting under its authority** and who has access to personal data **processes the data only following its request**, except for the case where this obligation rests with them under the Union or national law.

Also, the controller **did not implement adequate technical and organisational measures in order to ensure an adequate level of security and did not evaluate the risks presented by the processing**.

This situation led to the **unauthorized access to the personal data processed** through the computer application used by Raiffeisen Bank S.A. in the crediting activity and to **the unauthorized disclosure** of personal data by the employees of the bank.

Concerning the controller **Vreau Credit S.R.L.**, it was also sanctioned for the breach of data security, but also for the fact that until the end of the investigation it did not notify the supervisory authority of the personal data breach, without undue delay, although it has become aware of this security incident since December 2018, which led to the breach of the confidentiality of the personal data of their clients (the data subjects) and to the unauthorized/illegal processing of their personal data.

THE ROMANIAN SUPERVISORY AUTHORITY FINES INTELIGO MEDIA

On the 26th of September 2019, the National Supervisory Authority completed an investigation at **INTELIGO MEDIA SA, finding the following**:

Violation of the provisions of **Article 5 paragraph (1) letters a) and b), Article 6 paragraph (1) letter a) and Article 7 of the GDPR**, which led to imposing an administrative fine in the amount of **9000 Euros**.

The sanction was imposed as a result of an intimation indicating that for the creation of a new account on the website avocatnet.ro - belonging to the controller Inteligo Media SA, **an unchecked box** will be displayed, with a text having the following content: «I do not want to receive "Personal Update", the information sent daily, free of charge, by email, by avocatnet.ro».

According to these conditions established by the controller, to the extent that a user omits the check this box, he/she is automatically subscribed, respectively his/her e-mail is entered automatically in the subscriber database to this information.

Thus, the subscription took place in the absence of a manifestation of will on the part of the users, which clearly indicates the acceptance of the processing for the purpose established by the controller.

During the investigation, the controller **could not prove** that it obtained an explicit consent, under the conditions provided by Article 7 of the GDPR, for a number of **4357 users**, for which it processed their personal data.

Also, for the transmission of daily information by e-mail, the controller processed the data on the basis of a legal basis that is not appropriate for the purpose, namely the "execution of a contract".

In this context, we emphasize that according to Article 7 of the GDPR, if the processing is based on consent, the controller must be able to demonstrate that the data subject has given his/her consent for the processing of his/her personal data.

THE BERLIN COMMISSIONER FOR DATA PROTECTION AND FREEDOM OF INFORMATION ISSUED A FINE OF AROUND € 14.5 MILLION AGAINST DEUTSCHE WOHNEN SE FOR VIOLATING THE GENERAL DATA PROTECTION REGULATION (DS-GVO).

During on-site inspections in June 2017 and in March 2019, the regulator has determined that the company is responsible for the storage of personal data of tenants used an archive system that did not provide a way to remove unwanted data.

Tenants' personal data has been stored without checking that storage is permitted or even required. In isolated individual cases, therefore, it was possible to look into private information of affected tenants, some of which were years old, without these serving the purpose of their original survey.

It concerned data on the personal and financial circumstances of the tenants, such as: Salary certificates, self-disclosure forms, extracts from employment and training contracts, tax, social and health insurance data and account statements.

After the Berlin Data Protection Supervisor issued an urgent recommendation to change the archiving system in the first test date of 2017, the company was unable to clean up its data or legal data in March 2019, more than one and a half years after the first test date and nine months after the application of the General Data Protection Regulation To provide reasons for the continued storage. Although the company had made preparations for the elimination of the abuses found, these measures had not led to the creation of a lawful state of personal data storage. The imposition of a fine for breach of Article 25 (1) of the GDPR and Article 5 of the GDPR for the period from May 2018 to March 2019 was therefore mandatory.

The General Data Protection Regulation obliges supervisory authorities to ensure that fines in each individual case are not only effective and proportionate, but also dissuasive. The starting point for the calculation of fines is therefore the worldwide sales of affected companies in the previous year. Due to the annual turnover of more than one billion euros reported in the Annual Report of Deutsche Wohnen SE for 2018, the statutory scope for calculating the fine for the data protection violation was approximately 28 million euros.

The Berlin Data Protection Supervisor used the legal criteria to determine the exact amount of the fine, taking into account all aspects of the burden and exoneration. Above all, it had a negative impact the fact that Deutsche Wohnen SE deliberately created the archive structure and that the affected data was processed inappropriately over a long period of time. On the other hand, it was taken into account that the company took very early measures to rectify the unlawful situation and formally cooperated well with the supervisory authority.

In view of the fact that the company could not be shown any abusive access to the inadmissibly stored data, the result was a fine in the middle range of the prescribed fine. In addition to the sanctioning of this structural violation, the Berlin Data Protection Supervisor imposed further fines of between 6,000 and 17,000 euros against the company for the inadmissible storage of personal data of tenants in 15 specific individual cases.

The fine decision is not yet final. Deutsche Wohnen SE can file an appeal against the fine.

The press release, only available in German is available here

THE SPANISH DATA PROTECTION AUTHORITY FINES VODAFONE ESPAÑA €36,000

AEPD fined the company €36,000 for violating Article 6(1) of GDPR - processing the claimant's personal data without his consent.

The original fine amounted to €60,000 and was reduced to €36,000 on account of Vodafone España's voluntary payment.

You can read the Decision, only available in Spanish, here.

CANADA: PRIVACY COMMISSIONER SHARES LESSONS LEARNED AFTER ONE YEAR OF MANDATORY BREACH REPORTING

THE OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (OPC) HAS PUBLISHED A BLOG POST TO MARK THE ONE-YEAR ANNIVERSARY OF MANDATORY BREACH REPORTING UNDER THE *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT* (PIPEDA), CANADA'S FEDERAL PRIVATE SECTOR PRIVACY LAW.

The blog post provides some observations and statistics on the breach reports received by the OPC, as well as some early trends. It also contains helpful compliance tips.

Organizations subject to PIPEDA are required to report to the OPC any breaches of security safeguards involving personal information that pose a real risk of significant harm to individuals. They also need to notify affected individuals about those breaches, and keep records of all data breaches within the organiza

Available here

NHS PAGERS ARE LEAKING MEDICAL DATA

UNPROTECTED PAGER MESSAGES ARE BROADCASTING HEALTH AND MEDICAL DATA ACROSS UK CITIES

Full story on TechCrunch

An amateur radio rig exposed to the internet and discovered by a security researcher was collecting real-time medical data and health information broadcast by hospitals and ambulances across U.K. towns and cities.

The rig, operated out of a house in North London, was picking up radio waves from over the air and translating them into readable text. The hobbyist's computer display was filling up with messages about real-time medical emergencies from across the region. For some reason, the hobbyist had set up an internet-connected webcam pointed at the display. But because there was no password on the webcam, anyone who knew where to look could also see what was on the rig's computer display.

THE GERMAN DATA ETHICS COMMISSION PRESENTED ITS OPINION TO THE FEDERAL GOVERNMENT

The task of the Federal Government's Data Ethics Commission ("Datenethikkommission") was to build on scientific and technical expertise in developing ethical guidelines for the protection of the individual, the preservation of social cohesion, and the safeguarding and promotion of prosperity in the information age.

Full article available here.

GOOGLE CEO SUNDAR PICHAI ON ACHIEVING QUANTUM SUPREMACY

IN AN EXCLUSIVE INTERVIEW WITH MIT TECHNOLOGY REVIEW, PICHAI EXPLAINS WHY QUANTUM COMPUTING COULD BE AS IMPORTANT FOR GOOGLE AS AI.

Gideon Lichfield for MIT Technology Review

In a paper today in Nature, and a company blog post, Google researchers claim to have attained "quantum supremacy" for the first time. Their 53-bit quantum computer, named Sycamore, took 200 seconds to perform a calculation that, according to Google, would have taken the world's fastest supercomputer 10,000 years. (A draft of the paper was leaked online last month.)

The calculation has almost no practical use—it spits out a string of random numbers. It was chosen just to show that Sycamore can indeed work the way a quantum computer should. Useful quantum machines are many years away, the technical hurdles are huge, and even then, they'll probably beat classical computers only at certain tasks. (See "Here's what quantum supremacy does—and doesn't—mean for computing.")

But still, it's an important milestone—one that Sundar Pichai, Google's CEO, compares to the 12-second first flight by the Wright brothers. I spoke to him to understand why Google has already spent 13 years on a project that could take another decade or more to pay off.

The interview has been condensed and edited for clarity. (Also, it was recorded before IBM published a paper disputing Google's quantum supremacy claim.)

Full interview available here

NEW AI FACIAL RECOGNITION TECHNOLOGY GOES ONE STEP FURTHER

By Ljubinko Zivkovic for Unite.ai

It seems that the use of artificial intelligence in facial recognition technology is one that has grown the farthest so far. As ZDNet notes, so far companies like Microsoft have already developed facial recognition technology that can recognize facial expression (FR) with the use of emotion tools. But the limiting factor so far has been that these tools were limited to eight, so-called core states – anger, contempt, fear, disgust, happiness, sadness, surprise or neutral.

Now steps in Japanese tech developer Fujitsu, with AI-based technology that takes facial recognition one step further in tracking expressed emotions.

The existing FR technology is based, as ZDNet explains, on "identifying various action units (AUs) – that is, certain facial muscle movements we make, and which can be linked to specific emotions." In a given example, "if both the AU 'cheek raiser' and the AU 'lip corner puller' are identified together, the AI can conclude that the person it is analysing is happy.

As a Fujitsu spokesperson explained, “the issue with the current technology is that the AI needs to be trained on huge datasets for each AU. It needs to know how to recognize an AU from all possible angles and positions. But we don’t have enough images for that – so usually, it is not that accurate.”

A large amount of data needed to train AI to be effective in detecting emotions, it is very hard for the currently available FR to really recognize what the examined person is feeling. And if the person is not sitting in front of the camera and looking straight into it, the task becomes even harder. Many experts have confirmed these problems in some recent research.

Fujitsu claims it has found a solution to increase the quality of facial recognition results in detecting emotions. Instead of using a large number of images to train the AI, their newly created tool has the task to “extract more data out of one picture.” The company calls this ‘normalization process’, which involves converting pictures “taken from a particular angle into images that resemble a frontal shot.”

As the spokesperson explained, “With the same limited dataset, we can better detect more AUs, even in pictures taken from an oblique angle, and with more AUs, we can identify complex emotions, which are more subtle than the core expressions currently analysed.”

The company claims that now it can “detect emotional changes as elaborate as nervous laughter, with a detection accuracy rate of 81%, a number which was determined through ‘standard evaluation methods.” In comparison, according to independent research, Microsoft tools have an accuracy rate of 60%, and also had problems with detecting emotions when it was working with pictures taken from more oblique angles.

As the potential applications, Fujitsu mentions that its new tools could be, among other things, be used for road safety “by detecting even small changes in drivers’ concentration”.

THE NEW COUNTERINTELLIGENCE

Ryan Howard for ResearchLive

THE LATEST DEVELOPMENTS IN EXPLAINABLE MACHINE LEARNING ARE A GIFT TO MARKET RESEARCH WRITES RYAN HOWARD.

Were my six-year-old self to stumble across a new swear word, my mother would threaten to put mustard on my tongue. This sent me screaming around the house in terror. Silly as it seems now, I have levelled the same at my own students, should they suggest that correlation implies causation. To a statistician, there are few ideas more profane.

Interpreting data in this way means that you live in a world where ice-cream causes drowning and washing your car causes it to rain. In reality, we buy ice-cream and swim at the same time of year and, sometimes, it rains. No matter how intuitive or consistent correlations appear, they are invitations to overestimate, to claim insight where there is none or misinterpret reality entirely.

As humans, we naturally want to think in these terms, and as researchers, we want to explain why things happen. So, what does it mean to cause something? Philosophy lends us a useful trick – the study of counterfactuals. The counterfactual framework of causal inference assumes that an individual can have many causal states with more than one potential outcome at a time. The difference between what might have happened and what actually happened is inferred to be the cause. Simple enough, right? No. Not really.

For example, can we prove our sponsorship campaign causes sales to increase? To isolate causality, we need enough information to answer some 'What happens if…?' questions about both the customer and campaign.

At an individual level, we might observe a customer buying our product after being exposed to the campaign. Our first counterfactual is that the customer would have bought our product regardless. Counterfactuals are the things that could have happened but didn't.

Both actual and counterfactual outcomes are conditional on the specifics of the customer, pricing, competitor activity – a moment in time – too many conditions for a matched test and control experiment. Though, it stands to reason that if we have enough observations of both outcomes under enough conditions in enough combinations, we may yet shape a convincing case at an aggregate level. This is different from citing mere association. Rather, all other things being equal, the probability of purchasing does not increase *but for* the campaign.

Starting out with this everyday common sense, counterfactual thinking becomes complex disconcertingly quickly.

Causal inference relies heavily on identifying and adjusting of effects, in a world where it is impossible to account for everything and nothing remains constant. Just as with statistical inference, we are dealing in hypotheticals. Though lacking empirically, it is a pragmatic framework capable of addressing causality.

Quasi-experimental counterfactual thinking in its various guises, most notably propensity score matching, has been part and parcel of marketing science for decades. However, as machine learning ingratiates itself, it has received renewed interest and I've spent most of the past two years enthralled with it.

Unlike traditional modelling, machine learning's unrestrained mathematical violence produces black box models. Black boxes are anathemas to insight professionals who want evidence to believe and a hands-on way to engage and share, before even feigning interest in prediction. Our insights are the relationships algorithms discover, not what they spit out. Confronted with black boxes, our role is diminished in modern marketing.

Counterfactuals are our crowbar into these boxes, for what is any machine-made algorithm but layer upon layer of conditions, packaged as a 'what happens if' calculation.

Forensic data science has codified counterfactuals, a gift to those that need to be transparent and human friendly. Picture if you will, Jack Bauer-like algorithms, interrogating models by pursing combinations, challenging relationships, manipulating, imputing and contrasting, shaking the box into confession. This is counterintelligence by machines into machines.

These confessions allow us to quantify causal drivers indirectly and map how different measures interact with each other. We can audit and debug, then demonstrate that our models make sense and get buy-in for them. Where once we were hostage to impenetrable prediction engines, explainable machine learning will now emphasise our strengths as translators and storytellers.

By the age of 10, I knew all the useful expletives. My dear Mum had no option but to make good on her promise. It backfired spectacularly – hopefully my relief and surprise reflects how you feel about data science today.

"Mmmm…" I thought, as I gestured for more, "this is pretty good stuff. I fancy using it everywhere.

efamro