Case Studies [Data Ethics and Data Protection]

Guido Spina

July 2023

1 Law and Technology - The Law of the Horse

1.1 Online defamation - From publisher to ISPs

1.1.1 Cubby Inc. v. CompuServe Inc.

In 1991, United States Distric Court was called to review the case of CompuServe, an Internet service provider that hosted a third party daily newsletter. Cubby Inc. sued CompuServe after defamatory content was published on the newsletter they hosted.
The court ruled that, since the newsletter was **unmoderated** by CompuServe, *CompuServe was merely a distributor, rather than a publisher of content on its forums, and hence could only be liable for defamation if it knew, or had reason to know, of the defamatory nature of the content.*

1.1.2 Stratton Oakmont Inc. v. Prodigy Services Co.

In 1995 a similar case was brought to the ruling of the United States Supreme Court.
Prodigy Services Co. was a *content hosting site* that hosted a moderated bulletin board about finance. Stratton Oakmont, an investment banking firm, sued Prodigy Services after defamatory content was published on the board.
The Court ruled that, since Prodigy Services exercised editorial control over the content published on the board, they were considered *publishers* of the content posted on the site, and therefore liable for the postings of third party users.
This was considered by many to be conflicting with the case of CompuServe Inc., and that "punishing" sites for moderating the content posted on them was an incentive not to do so.

To regulate the matter, in 1996 the **Communications Decency Act** was published, stating (among other things) that *operators of Internet services are not to be considered publishers, and therefore are not legally liable for the words of third parties that use their services.*

2 Right to Privacy

2.1 Balancing of interest

2.1.1 Google Inc. v. Mario Costeja Gonzalez

In 2012, Mr. Costeja Gonzalez lodged with the Spanish Data Protection Authority a complaint against *La Vanguardia*, a spanish daily newspaper, and against Google Spain and Google Inc.
The complaint was based on the fact that, when an internet user entered Mr. Costeja's name in the Google search engine, they would obtain links to two pages of *La Vanguardia* from 1998, related to a real-estate auction connected to the recovery of social security debt.
Costeja Gonzalez requested to *La Vanguardia* to remove or alter those pages, so that the personal data relating to him no longer appeared.
They also requested to Google to remove the personal data relating to him. He stated in this context that the proceedings concerning him had been fully resolved for a number of years, and that reference to them was now entirely irrelevant.
The Spanish Data Protection Authority rejected the complaint related to *La Vanguardia*, stating that the publication of the the information was legally justified and intended to give maximum publicity to the auction. On the other hand, the complaint against Google Inc. was upheld, since the Authority considered that operators of search engines are subjected to data protection legislation, and that one individual could request hyperlinks to be removed from the search engine's index.

2.1.2 Mosley v. the United Kingdom

A British national newspaper published a front page article about Max Mosley (VIP in the automobile world), reporting his alledged "Nazi" sexual activities and including photographs taken from a secretly recorded video.
The European Court of the Human Rights stated that the publication of the pictures was a severe infringement of Mosley's privacy, and that there was a distinction between reporting facts and lucrate over the private life of celebrities. Nevertheless, it ruled that the sum of money awarded to Mosley in compensation for the invasion of privacy was sufficient, and that the newspaper had the right to freedom of press and freedom of expression.

3 Data Processing

3.1 Household activity

3.1.1 Mr Buivids tapes police officers

Mr Buivids taped police officers at a police station, and uploaded the video on YouTube.

The Latvian Data Protection Authority ordered to remove the video because he had infringed data protection law. Court of Justice of the European Union stated that the principle of *household activity* didn't stand in this case because the video was uploaded on the internet, ruling in favour of the Latvian DPA.

3.2 Bodil Lindqvist case

Mrs Lindqvist worked as a catechist in Sweden. She set up a web page in order to give useful information to church goers, including personal information about her catechist colleagues, who were not aware. Again, the CJEU stated that the household activity exemption didn't stand, because it relates only to activities carried out in the course of private or family life, and never through the publication of data on the Internet, so that it is accessible to an indefinite number of people.

4 Consent and Legitimate Interest

4.1 Newspapers and paywalls

In October 2022, several sites of GEDI Group (newspapers and magazines publisher) have introduced a message, asking visitors who are not subscribers to subscribe or to accept cookies in order to access all the pages on the website.
The Italian Data Protection Authority has opened an investigation into the use of these paywalls. Are these paywalls legitimate?
The Austrian and French Authorities have already stated that the cookie paywall sysrtem is a valid solution, if the subscription proposed by the site has a moderate cost as not to restrict the user's freedom.
The decision of the Italian Data Protection Authority on paywalls is still awaited.

4.2 Pizza Order

Claudia orders a pizza via a mobile app on her smartphone but does not opt-out of marketing on the website. Her address and credit card details are stored for the delivery. A few days later Claudia receives discount coupons for similar products (***Legitimate interest, impact***) from the pizza chain in her letterbox at home (***impact***).
The pizza chain has a legitimate interest in attempting to sell more of its products to its customers. There doesn't appear to be any significant intrusion into Claudia's privacy, or any other undue impact on her interests and rights. The data and the context are relatively innocent (consumption of pizza). The pizza chain established some safeguards: only relatively limited information is used (contact details) and the coupons are sent by traditional mail. In addition, an easy to use opportunity is provided to opt-out of the marketing on the website (***additional safeguards***).

5 Individual Rights

5.1 Right to erasure

5.1.1 BPER Banca S.p.A

On January 2019, a data subject emailed BPER Banca (data controller) requesting to erase his professional profile. Few days later, the bank asked for the subject ID to enable his identification. The data subject immediately sent the requested information. However, the bank took no further action.
The data subject submitted reminders both in April and in May 2019. Only on June 2019 the bank confirmed the erasure.
The Italian DPA concluded that the controller's late and inadequate response to the request for erasure submitted by the data subject was unlawful and issued a 10k fine.
GDPA states that the maximum time in order to delete the data after a request is 30 days, which can be extended for another 30 days if the deletion is difficult or there is a high volume of requests. In this case the data subject must be notified.

5.2 Right to access

5.2.1 Osterreichische Post

A data subject asked the Austrian Postal service for access to the personal data concerning him which were being stored or had previously been stored by said company and, if the data had been disclosed to third parties, for information as to the identity of the recipients.
Osterreichische Post gave a generic response and did not disclose the identity of the specific recipients of the data.
The CJEU declared that the subject's right to access to personal data entails an obligation to the controller to provide the data subject with the actual identity of those recipients, unless:

- It is impossible to identify the recipients, or
- the controller demonstrates that the data subject's requests for access are manifestly unfounded or excessive

In which cases the controller may indicate to the data subject only the categories of recipient in question.

6 Examples of GDPR fines

6.1 Caffeina Media - Data transfer to the US

Caffeina Media s.r.l. was sending data to Google LLC (based in the US) through Google Analytics.

Following the *Max Schrems II Case*, in which Facebook Ireland was sending data to Facebook US, a complaint was filed to the European Center for Digital Rights, that ruled that Caffeina Media infringed Art. 46 of GDPR regarding data transfers, since they transferred data to a third party without taking appropriate measures of safety

6.2 OneDirect - Inability to exercise rights

Two complaints were filed, regarding the sending of promotional emails by the company OneDirect, without consent and despite the opposition of the recipients expressed via email.
The absence of clear indications on how to contact the company, the lack of adequate technical and organizational measures to enable the operation of the unsubscribe button to work, and the monitoring of the email inbox have made it **impossible for complainants to exercise their rights**.
OneDirect was fined for 30k euros.

6.3 Aggressive Telemarketing

6.3.1 Vodafone and WindTre

Both these companies were fined for 12 and 17 millions of euros after they unlawfully processed personal data of their users for telemarketing purposes. They failed to register the consent of the users, used fictious numbers of numbers not recorded in the Register of Communication Operators to make promotional contacts, acquired name lists from external suppliers (without the free, informed and specific consent of users), and took inadequate security measures relating to customers management systems.

6.4 Giessegi - Lack of Data processing agreement

Giessegi was a controller and it was in a contractual relationship with a processor (*Verizon*) who provided geolocation devices. The controller installed these devices to track **vehicles** delivering goods on its behalf. These vehicles were not directly owned by the controller, but rather by a third company, to which the controller outsourced certain services.
The Data Subject was a driver employed by this third company, and he had no direct contractual relationship with the controller.
No controller-processor agreement existed between Giessegi and Verizon
The Italian DPA fined Giessegi for 50k euros.

6.5 ISWEB S.p.A - Lack of Authorization to engage a sub-processor

ISWEB was a web application provider, who entered an agreement with a group of hospitals to create an application for collecting and managing employees's

whistleblowing reports. ISWEB contracted the company *Seeweb* for hosting the whistleblowing application.
ISWEB **did not ask the prior written authorization from the controller for engaging a sub-data-processor relationship with Seeweb** through a contract or other legal act.
The Italian DPA fined them for 40k euros for violating Art. 28.2 of GDPR about subprocessing.

6.6 Jehovah Witness Community - Joint controllers

Jehovah witnesses collect personal data during their door to door activities, including names and addresses of persons unknown to them without their knowledge or consent. Both the members and the community were involved in the activities, that were aimed at engaging in a preaching, keeping records about preachers and distributing community publications.
They were forbidden to do so, unless the legal requirements for processing were satisfied.
The Court held that *a religious community is a controller,* ***jointly*** *with its members who engage in preaching , for the processing of personal data carried out by the latter in the context of door to door preaching, without it being necessary that the community has access to those data.*

6.7 Glovo Spain - Non-appointment of a Data Protection Officer

The Spanish Data Protection Authority imposed a fine of 25k on Glovo for the non-compliance of its duty to appoint a Data Protection Officer.
Glovo stated that they weren't required to do so because they aren't included in the mandatory appointers according to article 37 of GDPR. They also stated that they had an internal Data Protection Board with the exact same task.
The Authorities did not accept these allegations.

6.8 GIE INFOGREFFE - Password Security

The Data Controller has a website which allows consultation of legal information on companies. A data subject filed a complaint at the CNIL, stating that he ws able to get a password on the phone only by telling his name. The Data Subject also complained that the website stored users' passwords in plain text.
The Data Controller violated article 32 of GDPR for not ensuring a safe level of security against identity theft.

6.9 Marriott - Lack of security measures

Investigations followed after Marriott's IT Systems were attacked, resulting in unauthorized access to millions of customers personal data.

Marriott had a severe lack of security measures: insufficient monitoring of privileged accounts, insufficient monitoring of databases, poor control of critical systems and systems with access to large amount of personal data, only certain type of sensitive data was encrypted (e.g. credit card numbers) but not all (e.g. passport numbers).
Even after mitigating factors, such as the efforts that Marriott made to inform and help the victims, they were fined for 20M euros.

6.10 Foodinho and Deliveroo - Failure of data minimization

Garante della Privacy stated that these companies violated the principle of data minimization and protection by design and by default.
The app systems were configured to collect and store all data relating to the management of the order, and to allow authorized operators to pass simple functions from one system to another, with consequent sharing of the data collected across the various systems.

6.11 Data Breaches

6.11.1 Bank of Ireland - Data Breach Notifications

Inaccurate customers data was uploaded to the Central Credit Register (CCR) by the controller "which gave an erroneous view of BOI's customers' finances and credit history"
The controller failed to report 17 personal data breaches without undue delay and to provide the information required under Art.33.3 of GDPR. The controller also contravened Art.34 GDPR as it did not inform the data subjects about the personal data breaches without undue delay in at least 14 cases.
They were fined for 463k euros.

6.11.2 Enel Energie - Wrong Email Recipients

Customer data was sent via email to a wrong recipient, a different customer. The recipient, when he saw personal data of a different customer, filed a complaint with the DPA.
Enel (the data controller) did not adopt sufficient security measures and failed to notify the breach within 72 hours from the moment it became aware of it.
They were fined for 10k euros and warned for the failed notification to the DPA.

6.11.3 Vastaamo - Personal Data Breach

Vastaamo was a Finnish private psychoterapy service provider which operated as a sub-contractor for Finland's public health system.
In October 2020 Vastaamo announced that its patient database had been hacked in an extortion attempt. Thousands of patients information was published online, including full names, addresses, social security numbers and doctors notes

from the therapy sessions.
The data was found to be protected by insufficient security measures: no encryption, no anonymization.
As a consequence, victims suffered anxiety, insecurity and stress. Vastaamo was declared bankrupt in 2021.
The Finnish DPA found that Vastaamo had violated several GDPR provisions, including articles 33 and 34 for having failed to report in time the data breaches to the DPA and the Data Subjects, respectively. Moreover they failed to implement appropriate security measures and to embed core GDPR principles (accountability, data protection by design and by default)

7 Urban Data Protection Issues

7.1 Sidewalk in Toronto

A project for a smart sidewalk was started in 2017 in Toronto. Alphabet Google got the job, seeking to transform a sidewalk into a *smart zone* smart urban area, that allegedly had the purpose to improve the quality of life of the residents, working also as a testing ground for future urban design projects and technology. The robust quantity of data collection raised some criticism on the project, that was ultimately abandoned in 2020. Another problem was the privatization of public administration, meaning that citizens and the community would have lost control over it.

7.2 The London Bike Sharing case

A Bike Sharing company in London was forced to change their system's design after data pseudonymization issues surfaced.
They were using the same user ID for different tracks, making it possible to identify all the tracks done by the same user. This highly increased the risk of identification, making it also possible to identify (for example) where a user lived or worked.

8 Prediction Models and Sources of Bias

8.1 COMPAS - Prediction of Crime Reiteration

COMPAS stands for Correctional Offender Management Profiling for Alternative Sanctions. It is a system developed by Equivant, a company based in the US, with the task to predict the likelihood of recidivism in defendants of court cases.
The system, who worked through the analysis of 137 features (questions asked in a questionnaire that every person that gets arrested has to fill in), had deep negative bias against minority races, such as black or latino. On the other hand, it had a positive bias towards white people. White defendants who got

rearrested were nearly twice as likely to be misclassified as *"low risk"*, while black defendants who did non get rearrested were nearly twice as likely to be misclassified as higher risk.
It was proved that similar or even better prediction results could have been obtained with simpler models that used less data. Two features were sufficient: age, and prior criminal history.
COMPAS had a series of issues, including, but not limited to:

- ***Target-construct mismatch***: not all who "re-offended" got re-arrested, resulting in a **measurement bias**.
- ***Distribution shift***: data changed overtime in the time and geographical field, which wasn't taken into consideration in the algorithm **(Representation bias)**
- ***Limits to prediction model***: the model was essentially *bad*, comparable to a linear model with only two features
- ***Disparate performance***: the model lacked **independence** and **separation**, meaning that the result was heavily depending on the race of the subject.
- ***Lack of contestability***: the subjects could not challenge the information.
- ***Goodhart's law***: the model had a deep **social desirability bias**, because some features were heavily involved in the final decision.

8.2 Algorithmic Profiling of Job Seekers in Austria

In 2018, the Austrian Public Employment Service (AMS) announced the development of a system capable of classifying job-seekers into three categories: Group H, with a high chance of finding a job in the following 6 months, Group L, with a bad outlook of employment in the next 2 years, and Group M, that included data subjects who didn't fit in any of the other two groups. This last group would have been the main focus of public funding, helping them find a job more actively, in contrast with Group L or H.
The goal was to make funding instruments (money, time and workforce) more effective, since according to the AMS, expensive active labor market programs do not significantly increase the chances of hiring for both high and low job seekers prospects.

The algorithm fetched data from two different sources, that provided two types of data: data from the procedure of registration to the AMS network, and data from the Main Association of Austrian Social Security Institutions, that collects personal data on the individuals (like gender, nationality, age).
The precision of the algorithm (calculated as $TP/(TP + FP)$) is only known for the high and low segments, and it is respectively 80% - 84% for H, and 81% - 91% for L. This means that around 120.000 people got assistance when they

shouldn't have had the right for it, while we don't know anything about people that had the right for help and didn't get it.

AMS reflects the high degree of historical inequality in the labor market, for example:

- when both at the beginning of their unemployment, women were twice as often classified to be in the low segment compared to men.
- People with a migration background and people over 50 would systematically get lower scores.
- in general marginalized groups were disadvantaged in the classification.

Other types of errors and bias are weak abstraction of variables and hard thresholds (only three groups, for example, or only two types of occupational groups), or measurement bias (like the fact that *"care obligation"* field only applied to women.
The system also had omitted variable bias and representation bias, not taking into consideration regular changes in the labor market, changes of social values, extraordinary events like 2007 recession or COVID in 2020, and legislative changes and local changes (e.g. bankrupt of an important local company).
Other considered issues are the **lack of transparency** about data collection and design details, the lack of ability to **verify, contest and remedy** AMS decisions, the use of **sensitive information** initially collected for other purposes, and the **social stigma** and **psychological consequences** of the evaluation.

8.3 SyRI - Detecting social welfare frauds in the Netherlands

8.3.1 Mechanism of SyRI

SyRI stands for System Risk Indicator, and it was an algorithm used to support officials in investigating welfare frauds. Its goals were to reduce inspections time and their related cost, allocate better economical resources and reduce waiting time and administrative burdens.

The mechanism was adopted this way: when a government agency suspected welfare fraud in a specific neighborhood (benefits, allowances or taxes), it should cooperate with another agency and ask the Ministry of Social Affairs and Employment to have SyRI **deployed**.
Municipalities, the Employee Insurance Agency, the Social Security Bank, inspectors of the Ministry of Social Affairs and Employment and the tax Authority can ask access to the system.

SyRI was trained on historical data of residents of Dutch Municipalities for patterns of social security fraud. SyRI produced a **prediction** on which citizens of a selected neighborhood were suspected of welfare fraud. **Positive**

predictions (meaning a suspected welfare fraud) is then sent to the Inspectorate of the Ministry of Social Affairs and Employment.
Next step was **verification**: the Inspectorate analyse and verify the predictions, and then report back to the requesting agencies and to the Ministry of Social Affairs and Employment (MoSAE). MoSAE then examines flagged citizens for false positives, and keep confirmed positive risk reports for a maximum of two years. The requesting agencies further investigates the fraud, and only if it is confirmed, a sanction could be imposed.

8.3.2 Data used by the system and its impact

Since 2014, SyRI integrated personal data (such as work, fines, penalties, taxes, properties, housing and more) about citizens from several governmental bodies (both central and decentralised).
The data was then pseudonymized: citizen's names were replaced by a unique identifier for each individual, so that data from different sources could be merged. Identifiers were translated back into real names when there was the need of a sanction.
SyRI was deployed only in low-income neighborhoods, with the selection bias that more high risk citizens would have been found there. When the training data was updated with the new consequent fines, this would result into a **feedback loop**. This reinforced stereotyping and caused negative image of "problem zones", with high potential of structural impact.

Citizens were not automatically informed about the investigation, and SyRI's reports were inserted in a registry that citizens could view only upon request. This meant that if individuals do not know they are investigated, they will not require to check their own data and cannot access the reasons why they have been flagged. In practice, when an individual was sanctioned, **they could not defend themselves**. The system was kept secret, because the Ministry of Social Affairs thought that if it was made public, citizens could adjust their behavior accordingly.
An independent audit, carried by the Netherlands Organization for Applied Scientific Research research institute, concluded that "The results of the algorithm do not appear to be reproducible, and they appear to be largely randomly determined."