5 | 2019
20th Year
15 October 2019
P. 129–160

CRi

Computer Law Review International

A Journal of Information Law and Technology

cr-international.com

ottoschmidt

86203501905

Austria: First Award of Immaterial Damages under GDPR

GDPR Art. 82

The processing of a person's "political affinity" expressed as a percentage calculated from sociodemographic factors is considered a special category of personal data; such processing without the data subject's express consent violates Art. 9 GDPR. A breach of this kind justifies damages in the amount of € 800. *(ed.)*

LG Feldkirch, decision of 7 August 2019 – 57 Cg 30/19b

Facts

The Austrian Post stores personal data of several million persons. It has been conducting anonymized opinion polls, whereby it enquired about some sociodemographic criteria like sex, age, permanent residence, type of residence (flat, house, etc), education as well as interest to receive election advertising. Based on these criteria, the Austrian Post forms "marketing groups" of around 100 persons, for which it calculates average probabilities of certain "affinities". These affinities include probabilities of a person's preferences regarding investments, bio products, donations, distance selling. They also contain a so called "political party affinity", i.e. the probability of a person's alignment with a political party's program and values. In a final step, each individual person within these marketing groups is assigned specific affinities.

The plaintiff, an Austrian lawyer, filed suit against the Austrian Post on the basis of Art. 82 GDPR for infringing his rights under the GDPR and claimed € 2,500 of damages.

The Austrian Post had assigned certain affinities to the plaintiff, inter alia the plaintiff's "political party affinity". The plaintiff considered his alleged political opinion a special category of personal data, the storage of which requires a legal basis, in particular his consent (Art. 9 GDPR). The Austrian Post had not informed the plaintiff about this processing of his data.

The plaintiff argued that by such illegal and careless processing, he has irretrievably lost control over his data and thus suffered an immaterial damage.

The Austrian Post argued that the "political party affinity" not even qualifies as personal data, because such data is collected via anonymized polls and provides merely a general probability-related statement. Because such data is the result of a probability calculation, this data could not be rectified..

Held

The court found that the assignment of a "political party affinity" to an individual person qualifies not only as personal data because it reflects a political opinion that is directly linked to a person, but also as special category of personal data according to Art. 9 GDPR.

The court further held that the Austrian Post collected and processed this special category of personal data without any legal basis, in particular without the plaintiff's explicit consent. It also did not inform the plaintiff about such processing.

Thus, the Austrian Post was held to have substantially breached Art. 9 GDPR as well as Art. 14 GDPR (information duties). Both of these breaches were considered to have substantially affected the plaintiff's fundamental rights and freedoms. In terms of immaterial damages, the Court has awarded the amount of € 800.

Comments

So far, there are only few court rulings in Austria dealing with damages claims for breach of data protection law.

▶ a) Amount of Immaterial Damages

This is the first ruling by an Austrian court in a civil procedure regarding damages based on Art. 82 GDPR. Contrary to all predictions that Art. 82 damages would be massive, the damages award of this first court decision is relatively low – even more so compared to past rulings from the pre-GDPR era:

- In 2011, one case concerned a wrongfully published credit rating of the plaintiff, namely information about forced recovery proceedings against him that had already been completed. Such publication resulted even in a material damage – a telecom provider's refusal to offer a certain cheap tariff to the plaintiff. In this case, the court awarded damages in the amount of € 1,000.[1]
- In 2015, a case dealt with the publication of intimate videos on social media. During her relationship with the defendant, the plaintiff gave the defendant her consent to take photos and videos of their sexual activities. However, she never gave her consent to publishing these videos. The defendant had also made videos without her consent, and once their relationship was over, published several videos online, where they could be downloaded and copied. In fact, they were downloaded some 10,000 times. Family and friends of the plaintiff got hold of them. The plaintiff suffered a severe psychological state of fear and humiliation. In this case, the court awarded damages in the amount of € 8,000.[2]

In the current case, the "political affinity" is with no doubt to be considered personal data.[3] It directly relates to an individual and shows his or her (probable) political opinion which – as a special category of personal data – deserves to be treated more sensitively. The plaintiff has never been informed about the collection and processing of such data. Insofar, the awarded damages amount seems indeed rather low.

However, when multiplying the awarded damages with the number of affected data subjects (more than 7 million), the result would be more than twice the amount of the Austrian Post's market capitalization.

▶ b) Accuracy of the Data

Another interesting aspect raised by the Austrian Post is the argument that the data about the plaintiff's political affinity was not "wrong". Although not verified by the plaintiff himself and thus perhaps not reflecting his real political opinion, such data was the result of a prob-

1 LG Innsbruck 4th Jan 2011, 12 Cg 72/10h.

2 OLG Wien 26th Aug 2015, 11 R 119/15y.

3 Other opinion *Rainer Knyrim*, ecolex 2019, 715.

ability calculation based on a number of social factors attached to the plaintiff. Therefore, the data only reveals a certain probability that the plaintiff has a preference for a particular political party and its program – and this probability is accurate! Consequently, this data could not be subject to a request for rectification under Art. 16 GDPR by the plaintiff.

This argument seems mistaken. An individual's political preference is something very subjective and needs to be verified by the data subject or based on objective facts which clearly show such preference (e.g. given vote in a political election, membership in a political party). A mere probability statement on the other hand, derived from general social factors like age, sex, residence, education, marital status, must be supplemented by the additional information that it only reflects a calculated probability based on such sociodemographic prerequisites (which also must be listed).

The case will remain pending for quite a while, as both parties announced their intention to appeal against the judgement.

Dr. Stephan Winklbauer, LL.M.

Dr. Stephan Winklbauer, LL.M.

Attorney-at-law and partner at aringer herbst winklbauer attorneys at law in Vienna.

Outsourcing, Software and Data Privacy Law

winklbauer@ahwlaw.at

www.ahwlaw.at

UK: Legitimacy of Police Using Automated Facial Recognition Technology

ECHR Art. 8; GDPR Art. 4 Nr. 1; Directive 95/46 Art. 2

The use of automated facial recognition technology involves processing data of identifiable individuals because the data suffice to single out and distinguish an individual from all others. *(ed.)*

High Court of Justice, decision of 4 September 2019 by Lord Justice Haddon-Cave and Mr. Justice Swift – Bridges v. Chief Constable of South Wales ([2019] EWHC 2341 (Admin))

Facts:

The presence of networks of surveillance cameras has become a significant feature of our towns and cities. Most systems rely for their utility on monitoring by human operators. Developments on biometrics are allowing image recognition to be conducted automatically. It used to be the case that systems were primarily used within closed environments such as immigration facilities at airports where machine readable passports allow the identity of the carrier to be verified. This calls for the individual to stand in a precisely marked location and to look unblinkingly at a fixed point. More sophisticated systems of Automated Facial Recognition (AFR) technology are increasingly being used to monitor public and private spaces. Cameras used in conjunction with their IT capabilities are capable of scanning many faces, comparing them against a data base of images of persons of interest and flagging them up for further action. The technology may typically be applied in situations where large crowds of individuals may be expected, such as a major sporting event and where there is the potential for violence.

In the present case it was reported that in the case of South Wales police a system known as AFR Locate had been used and that:

"Over the 50 deployments that were undertaken in 2017 and 2018, around 500,000 faces may have been scanned (albeit not necessarily 500,000 different individuals). AFR Locate is currently set to detect up to five faces in a given frame and may capture 10 frames per second."[1]

The claimant, it was accepted, had been in the vicinity of some of the deployments although his image had not been matched and no further action was taken against him. He argued, however, that the use of the technology was unlawful as involving breaches of human rights legislation and, the prime focus of the present article, the Data Protection Act 2018.

"The algorithms of the law must keep pace with new and emerging technologies. This case raises novel and important issues about the use of Automated Facial Recognition technology ("AFR") by police forces. The central issue is whether the current legal regime in the United Kingdom is adequate to ensure the appropriate and non-arbitrary use of AFR in a free and civilized society. At the heart of this case lies a dispute about the privacy and data protection implications of AFR. Counsel inform us that this is the first time that any court in the world had considered AFR"[2]

Held:

The court noted with approval *dicta* in *R(S) v Chief Constable of the South Yorkshire Police* [2004] 1 WLR 219 concerning the role of technical evidence in criminal cases:

"The benefits to the criminal justice system are enormous. For example, recent Home Office statistics show that while the annual detection rate of domestic burglary is only 14%, when DNA is successfully recovered from a crime scene this rises to 48%."

The challenge for the law is to maximise the benefits arising from the use of new technologies whilst minimising the associated risks.

▶ 1. Human Rights Issues

The Court had to consider the potential application of Article 8 of the Human Rights Convention to the use of AFR technology. Two questions arose:

- *first* whether the capturing of images in a public space brought the Convention into play and,
- *second*, assuming it was, whether there had been a breach of its requirements.

1 Bridges v. Chief Constable of South Wales ([2019] EWHC 2341 (Admin)) at para 36.

2 Bridges v. Chief Constable of South Wales ([2019] EWHC 2341 (Admin)) at para 1.