MAJOR SECURITY BREACH IN FINNISH PSYCHOTHERAPY CENTER: LEGAL ISSUES IN LIABILITY AND PERSONAL ID FACTORS

HENNA MARTTILA

Key-words: data breach - data security - healthcare - liability

Category: Legal Area

On October 21st, 2020, news about a severe data breach spread across the Finnish media. An unknown hacker had breached through psychotherapy center Vastaamo's database, downloading approximately 40 000 patient files including medical reports, personal information, and social security numbers. The hacker declared that they would publish 100 patient files in the anonymous Tor network unless their demand of 40 bitcoins (approx. 450 000 €) worth of ransom is not met by the psychotherapy center. The hacker proceeded by demanding money from the patients themselves in order to leave their data unpublished. Moreover, for a reason that yet remains unknown, the hacker allegedly released the whole data package consisting all the data of the 40 000 victims for a short while.[1]

According to the expert interviews by Helsingin Sanomat, a Finnish newspaper, the security breach was executed by relatively low-level hacking expertise and by exploiting major vulnerabilities in Vastaamo's servers, including outdated software and internal server URLs found from the public Internet.[2] [3] Furthermore, according to Yleisradio, the hacker themself claimed that he had used the default admin username and password to log in the database. Despite that Vastaamo has not confirmed these allegations, they raise important questions about what is the appropriate level of data security a health care company should possess in their patient archives.

Considering the count of the victims, the case seems to be one of the largest cases in Finnish criminal history. It has awaken nationwide attention not just because of the large quantity of the data, but also because of the quality of it: the attack has been considered to be especially reprehensible because it concerns very sensitive and confidential data of individuals in a vulnerable state. Indeed, the President of Finland Sauli Niinistö has described the attack as "ruthlessly cruel".[4]

The legal issues of the Vastaamo case can be reviewed from several points of view. One of them is the question of liability in psychical and monetary damages suffered by individual victims. The

Finnish National Bureau of Investigation is in search of the hacker for the breach. In the victims' point of view, the hacker is not the only one to blame: the attention is focused also on Vastaamo itself. The Office of the Data Protection Ombudsman in Finland has already started the investigation about Vastaamo's data protection measures and their compliance with GDPR (General Data Protection Regulation). Considering the allegations of hacker's ability to breach Vastaamo's database with relatively low level of effort, it appears that at least some of the claims for damages, if not all, can be directed at the company itself. The liability of Vastaamo depends on whether the Office of the Data Protection Ombudsman's Sanctions Board finds the company guilty of violating the data protection legislation. Only in the case of a violation, the victims are entitled to receive compensation from Vastaamo.

The second question arising is also liability-related, but this time on the company's inner point of view. Shortly after the news, Vastaamo fired its CEO on grounds of withholding information about two data breaches that had taken place in years 2018–2019. According to Finnish Limited Liability Companies Act (604/2006), a CEO of a company can be held liable of the damages they have caused for the owners in their commission by acting against their duty of care. By owners' application, the CEO's assets have already been taken into confiscation by court order in case the company's claim for monetary damages is successful.

However, the legal issues brought by the breach are not limited into the claims and faults *in casu*. The personal data of 40 000 victims has been published in the Tor network, providing social security numbers, full names, and addresses of private people. This set of information is in most cases enough for identity fraud in order to apply for instant credit or to make online purchases, which would be later charged from the victim. The full database was available for anyone to download in the Tor network. Some users have offered money to buy a specific data set or the whole package.

It is no doubt that the case poses a severe risk of a later identity theft for all the victims involved. In this regard, the Parliament of Finland discussed about the possibility of offering a new social security number for the victims of the breach.[5] However, it can be also argued whether changing the social security number would be the right remedy in a situation where there is no guarantee that similar data breaches cannot happen in the future as well. That said, the Vastaamo case has evoked discussion about the applicability of social security number as an identification measure in the first place. Whether or not this series of numbers should be asked by companies and authorities in the wide scale it is queried today has definitely been under discussion during recent years[6], but so far little has been done to change the procedure.

[1] As the main source for the facts in this work I have used the website of Yleisradio, the Finnish national broadcasting company. Please see e.g. Yle.fi 23.10.2020: Yle seurasi Vastaamon tietomurtotapausta: Vastaamo on ollut myös Kelan palvelutuottaja, kiristäjän verkkosivu palasi nettiin, HUSin, Tyksin, Taysin ja Kanta-Hämeen keskussairaalan asiakastietoja voinut vuotaa. Retrieved from https://yle.fi/uutiset/3-11610267 6.11.2020.

[2] Helsingin Sanomat 28.10.2020: Vastaamon potilasrekisteri on ollut erittäin helposti saatavilla, arvioivat HS:n haastattelemat asiantuntijat. Retrieved from https://www.hs.fi/kotimaa/art-2000006702821.html 6.11.2020.

[3] Helsingin Sanomat 24.10.2020: Poliisin lisäksi Vastaamon tietomurtajaa jahtaavat myös hakkerit – Jättikö terapia-aineistoa vienyt tietomurtaja itsestään ratkaisevia jälkiä vai onko kyse harhautuksesta? Retrieved from https://www.hs.fi/kotimaa/art-2000006697995.html 6.11.2020.

[4] Yle.fi 25.10.2020: Presidentti Niinistö Vastaamon tietomurrosta: Tämä koskettaa meitä kaikkia. Retrieved from https://yle.fi/uutiset/3-11612492 6.11.2020.

[5] Yle.fi 28.10.2020: Marin toivoo, että Vastaamon tietomurron uhrit voisivat muuttaa henkilötunnustaan nopeasti – hallitus pui tietomurtoa iltakoulussaan. Retrieved from https://yle.fi/uutiset/3-11617366 6.11.2020.

[6] See e.g. Yle.fi 28.01.2019: Henkilötunnusta kysytään joka paikassa – uskaltaako sitä antaa? Retrieved from https://yle.fi/uutiset/3-10612451 6.11.2020.