Investigating Cybercrime: Cyber-Identify Theft

The prevalence of cybercrime in the international community is a growing concern for individual safety as it aligns with cyber-identity theft. Like many other citizens worldwide, Europeans are occasional victims of cyber-identity theft. Manap, Rahim and Taji (2015) perceived cyber-identity theft as an Internet-enabled theft where the adversary targets an individual's personally identifiable information (PII) to commit fraud or theft. PII includes sensitive private data such as social security numbers, names, national identity numbers, and addresses. Since people are constantly transacting, communicating, and sharing critical data through online platforms, they leave back digital footprints with PII that can permeate a cybercrime when targeted by an adversary. The United Kingdom (UK), France, and Denmark are excellent examples of European Union (EU) countries with alarming rates of cyber-identity theft (PrivSec Report, 2020; Clark, 2022). For example, Clark (2022) affirmed that the UK and France exhibited the highest fraud card losses in Europe in 2019. Fraudsters can use lost card data to perform online transactions. This post explores cyber-identity theft in the UK, drawing awareness and influencing policy. The rise of cybercrime, especially cyber-identity theft, necessitates cyberspace policing and regulation to secure private data in the UK.

Even though international regulations are instrumental in outlining the policies and regulations for best cybersecurity practices, their conflict with national rules impedes effective investigative outcomes. For example, the EU General Data Protection Regulation (EU GDPR) of 2016 and the UK's Data Protection Act (DPA) 1998 (2018 update) show misalignments regarding the purpose limitation of private data (Hut Six, 2022). Chapter IV, Article 25 of the GDRP permits controllers (entities collecting data) to extend personal data usage and processing beyond its initial

purpose as long as the individual to whom the information belongs is notified (EU, 2016). Conversely, DPA 2018 restricts data collection to lawful purposes, specifying that the use of such data must not go beyond the intended purpose (UK, 2018). That way, a UK national whose data resides with a controller has limited authority over their data usage and processing as long as they agree to the terms of use under the EU GDPR. Should adversaries hack the organization holding the citizen's PII (Company Z in this case), or should the company misuse the associated PII, the UK government may find it highly challenging to prosecute Company Z, which adheres to EU GDPR. At the same time, the UK national who may be the victim of a cyber-identity theft following Company Z's breach may never find justice due to varied DPA and GDPR data regulation acts.

Further, disparities in national and international cybersecurity regulations and policies complicate judicial processes. Authorities find it challenging to track and legally prosecute adversaries exploiting the security loopholes in the EU GDPR at the expense of local citizens' safety in cyberspace. The inconsistency in GDPR and DPA regarding the Purpose Principle (EU, 2016; UK, 2018) indicates how international corporate entities may misuse private data and get away with a crime by leveraging regulatory loopholes. Succinctly, specific cyber-incidents may remain highest in the UK if other EU member states' Purpose Principe regulations align with EU GDPR's principle. The underlying crime involves exploiting regulatory vulnerabilities in international law at the expense of local citizens' safety in cyberspace. Cyber-identity thefts cost both individuals and the country's economic growth. In 2019, the UK lost 707 million euros due to card fraud-related cyber incidents (Clark, 2022). Regulatory disparities likely promote cyber-identity theft, contributing to the UK's high ranking among countries with similar cyber incidents. Therefore, international and national

policies should align to limit adversarial compliance and regulatory vulnerability exploitations.

References

Clark, D. (2022) *Value of card fraud losses in Europe 2019, by country*, *Statista Research Department*. Available at: https://www.statista.com/statistics/911873/value-of-losses-to-card-fraud-in-europe-by-country/ (Accessed: 31 October 2022).

EU (2016) *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016*. Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

Hut Six (2022) *Data Protection Act's Eight Principles*, *Hut 6 Security Limited*. Available at: https://www.hutsix.io/what-are-the-eight-principles-of-the-data-protection-act/ (Accessed: 1 November 2022).

Manap, N.A., Rahim, A.A. and Taji, H. (2015) 'Cyberspace Identity Theft: The Conceptual Framework', *Mediterranean Journal of Social Sciences*, 6(4), pp. 595–605. Available at: https://doi.org/10.5901/mjss.2015.v6n4s3p595.

PrivSec Report (2020) *One in five Europeans have experienced identity theft fraud in the past two years*, *GRC World Forums*. Available at: https://www.grcworldforums.com/fraud/one-in-five-europeans-have-experienced-identity-theft-fraud-in-the-past-two-years/351.article (Accessed: 31 October 2022).

UK (2018) *Data Protection Act 2018: The data protection principles*. United Kingdom: Legislation.gov.uk. Available at:

https://www.legislation.gov.uk/ukpga/2018/12/part/4/chapter/2/crossheading/the-data-protection-principles.