Case Study: Genesis Market Criminal Case

Introduction

Genesis Market, one of the largest cyber fraud platforms in the world, has been seized by the authorities in April 2023 after an international joint effort labelled "Operation Cookie Monster"1 led by the FBI with tenths of collaborating parties, including the Police forces of up to seven other nations, under the governance of Europol23. This black market was initially put in place in 20184 and quickly specialized in the theft and resell of digital identities, with up to 1.5 million compromised computers and 80 million account credentials in the first year of its foundation5. The case of Genesis Market is especially insidious because they set up a website both in the dark and on the regular Internet6. They developed and sold cyber tools like malware and exploits which were eventually employed in millions of cyberattacks and identity frauds around the globe. Genesis Market was active on both the surface and dark web, selling permanent access to victims' computers and creating a botnet of zombie computers to execute malicious activities covered behind a proxy 7. The culprits have developed their own tools as well, an openly distributed web browser called "Genesis Security"8, interfacing seamlessly with these botnets. Not long before going down, it was revealed to be operated from within Russia by the American Secretary of State, Antony Blinken. Genesis Market was considered by the FBI as one of the top 3 platforms in the world to acquire the most recent and powerful computer viruses, both other websites being also located in Russia. Additionally, Genesis Market has been collecting huge amounts of stolen data, financial records, Private Identifiable Information, of hundreds of thousands of people and companies for an amount ranging in the billions of dollars in total.

---

[1] https://cyberscoop.com/fbi-seizure-genesis-market-cybercrime/ visited on November 29th, 2024.

[2] https://www.kommersant.ru/doc/5914938, visited on November 29th, 2024

[3] https://fr.euronews.com/, visited on November 30th, 2024.

[4] https://www.justice.gov/opa/pr/criminal-marketplace-disrupted-international-cyber-operation, visited on December 1st, 2024.

[5] https://arstechnica.com/tech-policy/2023/04/operation-cookie-monster-feds-seize-notorious-hacker-marketplace/, visited on November 29th, 2024.

[6] https://www.kommersant.ru/doc/5914938, visited on November 29th, 2024.

[7] https://therecord.media/genesis-market-takedown-cybercrime, visited on November 29th, 2024.

[8] https://therecord.media/genesis-market-takedown-cybercrime, visited on November 29th, 2024.

This analysis aims at examining the handling of this large-scale case through the lenses of European Laws, especially the General Data Protection Regulations, the chart of the European Council of Human Rights and the Network and Information Security 2 directives. We will be shedding light on potential jurisprudential insights and procedural shortcomings, this case might raise questions about the adequacy of data protection and privacy protections in a local scope and international cooperation in addressing cybercrime. We conclude this document with a critical opinion on the implications of such collaboration with the USA and other state actors, foreign to the EU, in terms of Data Protection and Privacy of our citizens, thus assessing to which extent a collaboration with foreign agencies aligns with the European Union's commitment to data protection and the privacy rights of its citizens.

That introduction leads to the following juridic questions: How is GDPR treated during a criminal investigation in Europe, with the cooperation of foreign actors?

Data Protection in the European Union

Genesis Market operated in obvious violation of all essential principles of the GDPR. Collecting and selling stolen data, credentials, corporate and financial information, biometric records or any information relating to an identified or identifiable natural person, as stated in the GDPR. Furthermore, Genesis Market, as data controller, demonstrated a complete lack of transparency and failed to uphold the rights of data subjects. Breaching the principles of integrity, confidentiality Article 5, §1, f) and accountability Article 5, 2). It also violated GDPR Article 33 and 34 by failing to comply with the data breach notification obligations. These practices highlight the platform's total disregard for any European data protection standards.

Compromised information often originates from vulnerabilities in third-party systems, human negligence, human error, insider threats or Advanced Persistent Threats such as state actors. Because preventing the exploitation of private and sensitive data is primarily about having sane and thoughtful processes and reliable means for detecting these threats early. Entities must not only secure their own infrastructures but also assess and manage risks associated with their suppliers and partners to prevent the exploitation of their data by illicit platforms like Genesis Market.

What is the status of the GDPR in that investigation? On the matter of Europol’s criminal investigation, and under the competence of the member states with the cooperation of the Federal Bureau of Investigation as foreign entity, one could argue that the latter might not be included under the guidelines of the GDPR, a European legislation. During such proceedings as the Genesis case, GDPR Article 2, §2, d), stipulated that it does not apply to competent authorities in the

context of their investigation9. Neither Europol nor the FBI are included in the effective range of the GDPR. However, for the European investigators only, a specific directive was introduced for data protection in all criminal investigations. Directive 2016/680/UE, 2016, broadly shares similarities with the preexisting GDPR in its objectives, but it applies to Genesis Market and all penal and criminal cases10. About the question of internal transactions of private information in the scope of investigations, everything is treated as Articles 35 and followings11. The authority transferred between the European institutions and foreign nations is allowed under strict conditions and principles. The most important being the urgency of such a need and the respect of national laws. Furthermore, a transfer is only allowed with an authority in charge on a state-to-state basis, depending on its effective scope. In the case of Genesis Market, the FBI does affirm its legitimacy on that matter, it is indeed considered a competent authority12. Among the general conditions of Article 35, we find a requirement for the third country to provide an adequate level of data protection, which allows for the transfer1314.

In our case, international agreements were established between the USA and the European Union to lay legal grounds for cooperation in the matter of data protection. Notably, the 2016 EU-U.S. Data Protection "Umbrella" Agreement15 provides a complete framework for all personal data transferred between EU and U.S. law enforcement authorities. Consequently, the FBI is required to comply with its provisions and enforce high levels of security concerning European citizens' personal data, ensuring that the data subject's rights are respected and that the investigation proceeds within the legal boundaries set by international and European data protection laws. Furthermore, if the conditions outlined in Article 35 of Directive (EU) 2016/680—

---

[9] Art. 2,§2, d), Regulation 2016/679 of the european parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[10] C., FORGET, C., « Titre 20 - La protection des données dans le secteur de la « police » et de la « justice » » in Le règlement général sur la protection des données (RGPD/GDPR), 1e édition, Bruxelles, Larcier, 2018, p.872.

[11] Directive (eu) 2016/680 of the european parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[12] Article 35, Directive 2016/680/EU.

[13] Article 36, Directive 2016/680/EU.

[14] C. FORGET, Ibidem, p.897.

[15] Directive (eu) 2016/680 of the european parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

which governs the transfer of personal data by competent authorities for law enforcement purposes—were not fully met, Article 38 of the same directive provides for exceptional and limited circumstances under which such transfers may still lawfully occur. More specifically, are permissible transfers if necessary for protecting the vital interests of people, safegarding legitimate interests of society or national security.

Also, it is important to address the potential implications of evidence irregularly obtained. If the aforementioned legislations were not to be respected, questions may arise about their admissibility in legal proceedings. This supports the critical importance of adhering to existing legal frameworks, to not only protect individual rights but also maintain the effectiveness of law enforcement efforts.

Being part of an international criminal organization, Genesis Market was convicted of hundreds of counts of computer forgery and took part in multiple computer sabotage operations. These offenses highlight the extreme nature of Genesis Market and the very high level of danger it represents for sovereign states and citizens. A 2021 study revealed that Italy and France combined represented over 20% of the total listing of compromised computing assets for rent on Genesis Market, far further the USA and the United Kingdom (around 3% each)16. Moreover, its dismantling by multiple international law enforcement agencies prove the existence of complex and intricate criminal procedures, tied together between different countries. The investigation likely required several specific criminal investigative actions over the years, warranted searches and seizures at locations associated with Genesis Market, leading to the arrest of almost 120 people17. Confiscating computers and any equipment used to facilitate illicit activities in the context of serious indications of criminal offenses (Articles 89bis and following of the Code of Criminal Procedure). Undercover internet infiltrations were very likely employed, as authorized under Article 46sexies of the Code, allowing investigators to interact with suspects online using fictitious identities. Furthermore, techniques such as intercepting non-public communications and searching computer systems (as outlined in Articles 90ter and following) were utilized to collect crucial data in the context of that case.

European citizens were spyed on, maybe some of them wrongly, quid of the rights to privacy and the protection of everyone involved data? Did investigators allow themselves some leeways, pushing their capabilities to the limits of our laws and customs? Were people not related to the case at all, surveilled as a result? Were they even informed afterwards that they have been monitored? Who is responsible if an FBI-led operation on our soil allows itself actions our laws forbid? Is our own government even in the know? Can the executive level use illegal means to

---

[16] https://www.securitymagazine.com/articles/95144-inside-look-at-the-genesis-market-a-cybercriminal-market, visited on November 29th, 2024.

[17] https://therecord.media/genesis-market-arrests-cybercrime, visited on November 29th, 2024.

convict in a trial? The Antigone jurisprudence (2003) bring valuable insights on the treatment of irregularly collected, or illegally collected proof in a penal court, it informs us that not all non-regularly collected proofs are indeed refused, the severity of the crime is a decisive factor in accepting such proofs. In the case of Genesis Market, rigorous adherence to criminal procedures was essential to secure the evidence needed for prosecution and to effectively bring the platform's operators to justice18. This principle is codified in Article 32 of the Preliminary Title of the Belgian Code of Criminal Procedure19.

Conclusion and Critical Opinion

The Genesis Market is a prime example of how challenging transnational cybercrime investigations are. Operating beyond legal and ethical boundaries, it violated numerous provisions of the GDPR and other regulations. In situations where offenses transcend national borders, robust cooperation is required to dismantle criminal networks operating at such a large scale. Europol and the FBI are specifically prepared to handle such challenges. However, despite the importance of this collaboration, it remains essential to respect European and national legislations in order to safeguard the fundamental rights of citizens.

Proportionality, necessity and transparency are key principles for a sane application and respect of legislation in place. However, that domain is extremely complex, it is very important to legislate thoughtfully and in strict knowledge of the full legal scope. As we have seen earlier, these rules are firmly defined through additional rules such as the Umbrella agreement, underlining USA and EU legal cooperation.

---

[18] E., CECI, P., MAUFORT et S., SCARNÀ, « Section 4 - La jurisprudence « Antigone » en droit fiscal » in Droit pénal fiscal en (r)évolution, Bruxelles, 2023, p.241 à 244.

[19] Article 32 du titre préliminaire du code de procédure pénale, 17 avril 1878.

BIBLIOGRAPHY

Legislations:

Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, December 10, 2016.

Regulation 2016/679 of the european parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Directive (eu) 2016/680 of the european parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Titre préliminaire du code de procédure pénale, 17 avril 1878.

Doctrine :

CECI, E., MAUFORT, P. et SCARNÀ, S., « Section 4 - La jurisprudence « Antigone » en droit fiscal » in *Droit pénal fiscal en (r)évolution*, Bruxelles, 2023, p.240 à 286.

FORGET, C., « Titre 20 - La protection des données dans le secteur de la « police » et de la « justice » » in *Le règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, 2018, p. 865 à 900.

Internet Links:

https://cyberscoop.com/fbi-seizure-genesis-market-cybercrime/, visited November 29th, 2024.

https://www.kommersant.ru/doc/5914938, visited November 29th, 2024.

https://fr.euronews.com/. visited November 30th, 2024.

https://www.justice.gov/opa/pr/criminal-marketplace-disrupted-international-cyber-operation, visited December 1st, 2024.

https://therecord.media/genesis-market-takedown-cybercrime, visited November 29th, 2024.

https://www.securitymagazine.com/articles/95144-inside-look-at-the-genesis-market-a-cybercriminal-market, visited November 29th, 2024.

https://therecord.media/genesis-market-arrests-cybercrime, visited November 29th, 2024.

https://arstechnica.com/tech-policy/2023/04/operation-cookie-monster-feds-seize-notorious-hacker-marketplace/, visited November 29th, 2024.