AI & CYBERSECURITY IN GAMBLING FROM A EUROPEAN PERSPECTIVE

***By Philippe Vlaemminck**, Managing Partner, Vlaemminck.law*
***Beata Guzik,** Director Public Affairs, Vlaemminck.law*
***Valentin Ramognino,** Associate at Vlaemminck.law*

VLAEMMINCK.law

Philippe Vlaemminck

Beata Guzik

Valentin Ramognino

In October 2024, the European Commission published the findings of the Digital Fairness Fitness Check, which evaluates whether the current EU consumer protection laws are fit for purposes to ensure a high level of protection in the digital environment. **The report shows that consumers behave differently online than offline. Over the last 2 years, the EU has published a series of important texts relating to the digital environment: Data Act, Data Governance Act, DSA, DMA, DORA, Cyber resilience, AI Act, NIS2, and the Chips Act. Digital Fairness will indeed become a priority for future legislation, but is not the only concern.**

Addressing the various potential problems and emerging security risks of the digital world is thus of paramount importance.

Many studies and practices show that the use of AI for and against cybersecurity is rapidly developing. At the same time, 'Artificial intelligence' (AI) is a tremendous growth driver for lotteries, betting, and gambling firms today, especially for the online structures. AI tools to counter security breaches in the digital world will become essential for every big player.

2024 has become the year AI took the world by storm on the recognition of how to use AI in most sectors, but also was the year of the first regulatory framework (by the EU) and global influence thereof. Democratisation of AI and machine learning is one of the business's priorities today. The increasing integration of AI into our lives – from personal data security to cyber defence strategies – show also how AI can influence the digital landscape for lotteries, betting and gambling firms. Indeed, **AI is becoming a fundamental skill and necessary for game design, odds setting, risk management, customer profiling and responsible gaming, optimization of bonus programs and fraud detection.**

The transformative convergence of AI and security in gaming and gambling sets out how AI can contribute to risk management while mitigating its own associated risks. Implementing the ethical standards developed by various international bodies is of great value, but is not enough to address all potential problems. Legislation is certainly useful if it protects consumers and enables legal security and innovation.

The EU Artificial Intelligence Act (AI Act) entered into force on 1 August 2024 is the first comprehensive policy framework for AI. It categorizes AI systems into four risk categories, a real **RISK-BASED APPROACH:** unacceptable risk, high risk, limited risk, and minimal risk. This risk-based approach should be endorsed by companies in their daily business, and evaluation of AI-related risks implemented. **The AI Act defines AI system as a machine-based system that is designed to operate with varying levels of autonomy and adaptiveness,** which follows the global OECD's definition.

In the European Union area, the AI Act therefore provides general obligations of ROBUSTNESS, ACCURACY and CYBERSECURITY of the usage of AI. The EU AI Act also stresses the importance of HUMAN OVERSIGHT over automated decision-making systems, including those used in cybersecurity. The establishment of the European AI Office is also critical for many aspects of regulation, especially for general-purpose AI, the use of trustworthy AI, and international cooperation. Generative AI is particularly useful for cybersecurity purposes: it provides firms with efficient capabilities in proactive threat detection, incident response and operational efficiencies.

"Just like EU's General Data Protection Regulation in 2016 (GDPR), the EU AI Act of 2024 might spread worldwide, with many countries being influenced by the EU in regulating AI.

For instance, in the final days of 2024, South Korea joined the EU in establishing a comprehensive AI legislation which also imposes strict requirements on high-impact AI systems and creates oversight bodies. Japan also just announced its AI framework, with a focus to make Japan "world's most AI R&D friendly nation". UK is anticipated to develop an AI framework in 2025. One exception might still be the U.S where innovation and unconstrained AI development remains a priority.

The relationship between AI and cybersecurity has three dimensions. This is not different in the lotteries, betting and the gambling industry: **cybersecurity of AI,** which covers AI standardisation and cyber tools in AI; **AI in support of cybersecurity,** which empowers cybersecurity defenders to combat the **use of AI for malicious purposes,** which explores AI's potential to create new threats.

On cybersecurity of AI, the EU AI Act provides for so-called 'conformity assessments' to determine whether high-risk AI systems are cyber compliant with the EU Regulation on horizontal cybersecurity requirements (the Cyber Resilience Act Regulation (EU) 2024/2847), which involve considering "risks to the cyber resilience of an AI system as regards attempts by unauthorised third parties to alter its use, behaviour or performance, including AI specific vulnerabilities such as data poisoning or adversarial attacks and risks to fundamental rights". Companies also have a voluntary choice to comply with the cybersecurity scheme of the AI Act, provided in article 15 of the Act. In any case, companies must ensure that, in high-risk AI systems, the instructions for use contain the level of cybersecurity provided for in the EU AI Act.

Furthermore, standards in the EU of AI security requirements will become crucial for companies. In the EU, the European Committee for Electrotechnical Standardisation (CEN-CENELEC) was assigned to develop standards in support of the AI Act, with a deadline set for April 2025. In the meantime, the EU Agency for Cybersecurity (ENISA) has published a multilayer security framework for good AI cybersecurity practices with a step-by-step approach (FAICP). It consists of three layers: the groundwork of cybersecurity, focusing on the ICT infrastructure used; AI-specific aspects, focusing on the specificities of the AI components deployed; and sectorial AI, which is specific to the sector in which AI is being used.

On AI in support of cybersecurity, a number of companies have started to implement and showcase ways in which AI can be used to enhance cybersecurity, which involves four ways: DETECTION, PREDICTION, ANALYSIS AND THREAT MITIGATION.

In particular, for security purposes in AI development, the AI generative models will be critical to enhance security and risk management for lotteries, betting and gambling firms. AI models are rapidly transforming cybersecurity and fortifying IT defenses against sophisticated attacks. Thus, gambling-specific recommendations when using AI in security include implementing application Security Verification Standard (ASVS), conducting regular security testing with AI, developing educational materials with AI, implementing multifactor AI authentication, and deploying DDoS (denial-of-service) protection solutions. These measures enhance security, mitigate cyber risks, and safeguard user privacy and experiences, especially in online gambling.

In the lotteries, betting and gambling sectors, key is now to understand what cyber-attacks do, how to protect and defend both the customers and the organisations and how to use AI in the digital area. Specifically, there is a number of ways to counter cyber-attacks through AI, namely :

- Through network security trafficking mitigation: protect harmful cyber activities (data trafficking, malware and phishing attacks, illegal content) via AI models specifically designed for gambling platforms
- Software security: pinpoint vulnerabilities and enhance software codes
- Management security services: enhance education, top internal knowledge on the cyber risks and implementation of a risk management strategy
- Human intervention, even when using AI,: with penetration testing: Use anticipative models, to anticipate what attackers will attack next

As such, while the AI Act is setting some unnecessary burdens (for instance via the issuance of conformity certificates for high-risk AI by notified bodies) and reduce the potential for innovation development in the EU, there is a positive side with engaging tools, bodies and processes to defend consumers and organisations against cybersecurity.

Finally, lotteries, betting and gambling operators must be aware of the growing risk of malicious use of AI. AI can indeed be used itself for cyber-attacks, malware attacks, personal data attacks, deep-learning attacks and more risky behaviours have emerged with the use of AI. Generative AI can also supercharge dark patterns.

For the use of AI for cybersecurity purposes, the EU AI Act provides specifically a risk based approach to combat cybersecurity threats:

'Cybersecurity plays a crucial role in ensuring that AI systems are resilient against attempts to alter their use, behaviour, performance or compromise their security properties by malicious third parties exploiting the system's vulnerabilities. CYBERATTACKS AGAINST AI SYSTEMS can leverage AI specific assets, such as training data sets (e.g. data poisoning) or trained models (e.g. adversarial attacks or membership inference), or exploit vulnerabilities in the AI system's digital assets or the underlying ICT infrastructure.

To ensure a level of cybersecurity **appropriate to the risks,** suitable measures, such as security controls, should therefore be taken by the providers of high-risk AI systems, also taking into account as appropriate the underlying ICT infrastructure." (extracts from AI Act)

The lottery community, already strongly involved in the usage of AI, must of course continue to reflect on the new risks created by AI and continue their process of learning and exchanging best practices jointly with the suppliers, as was done recently during the WLA/EL Cybersecurity seminar in Marseille. **Lotteries perform a valuable service to society by channeling players to legal, safe and responsible gaming,** and this requires them also to stay upfront of new digital developments and incorporate them into their customer offer. The role of AI and its impact on security and responsible gaming is only at the beginning stage. The key to effective application of AI in all these spheres is follow-up. We look forward to working together with you and the community of lottery leaders to ensure AI is integrated into our businesses for optimal positive impact! ■