Resumen ejecutivo

Título: Análisis de la adecuación y funcionamiento de los sistemas antitrampas o «*anti-cheat*» en los videojuegos. Comentario especial del escaneo en tiempo real y a nivel de administrador del dispositivo de juego.

Autor: Darío López Rincón

Objetivo y justificación

Este estudio tiene como objeto servir de documento de análisis jurídico pormenorizado del tratamiento totalmente automatizado, en tiempo real, sin intervención humana y con efecto jurídico de los siguientes cinco sistemas algorítmicos antitrampas creados para evitar cualquier alteración indebida en partida en línea: Ricochet sobre Call of Duty: Warzone; Easy Anti-Cheat sobre Fornite; BattlEye sobre Xdefiant; VAC sobre Team Fortress 2 y Vanguard sobre Valorant.

Con especial énfasis, en su 1º fase de tratamiento más invasiva, notoria, externa a la plataforma de juego y considerada prioritaria para un funcionamiento adecuado del mismo: el escaneo en tiempo real y con nivel de privilegio de administrador a los archivos, programas y recursos del dispositivo desde el que el jugador acceda en cada momento al videojuego.

Asimismo, se incorpora una pequeña parte con las conclusiones y resultados del intento de auditoría técnica externa con dos programas especializados en métricas en tiempo real de uso de recursos y acceso a archivos realizado, a fin de poner de manifiesto dos elementos principales: la imposibilidad técnica de obtención de información personal real accedida para el contraste con la declarada por el responsable, y que el uso de sistemas de análisis profundo o forense que impedirían la carga del juego o la retirada de acceso automático al juego.

Entendiendo que son tratamiento intrínsecamente relacionados con la prevención de trampas, se incorpora el comentario separado de la problemática de los sistemas de grabación de chat de voz que intentan paliar la proliferación de acoso o discriminación, con especial incidencia sobre menores, así como del procedimiento de denuncia de otros jugadores ante trampas o comportamientos inadecuados detectados.

Diseño y metodología

Para la consecución del objeto indicado, el estudio se ha desarrollado sobre los siguientes cuatro apartados:

- Análisis a nivel general de los registros generados durante el juego, mediante la aplicación de programas de monitorización del uso de recursos y actividad del dispositivo utilizado para las pruebas de juego: Procmon y Sysmon;

- Análisis pormenorizado de las cláusulas informativas, políticas de privacidad, opciones y funcionalidades de privacidad, ejercicio de derechos, así como cualquier otro elemento relacionado de interés. Asimismo, con valoración general sobre la posible aplicabilidad de la DSA y el RIA;

- Valoración jurídica de la adecuación de cada uno de esos elementos, en atención al tenor literal de la normativa de protección y las directrices, informes o guías de las autoridades de control y supervisión en la materia; y

- Propuesta de soluciones para aquellos elementos analizados que se considera que no cumplen adecuadamente.

Resultados

Se considera que del estudio pueden concluirse los siguientes extremos:

- Que el tratamiento objeto de análisis no se considera, per se, imposible de realizar en base al interés legítimo utilizado ni es algo que no responda a una necesidad real, pero se considera que no cuenta con limitaciones y garantías suficientes a nivel de proporcionalidad y el RGPD;

- Que la existencia de alternativas menos invasivas, especialmente, para la 1º fase de mayor intensidad del escaneo previo a nivel de administrador del dispositivo de juego, implicaría la necesidad de revaluación. Asimismo, la necesidad de dotar al jugador de un verdadero derecho de oposición u opcionalidad en dicha fase;

- Que la legitima expectativa del jugador no abarcaría a todo el conjunto de fases y el marco de control actual de este tipo de sistemas;

- Que existe una falta de información adecuada sobre el tratamiento: información de 1º capa, omisión de determinados elementos o dispersión de elementos explicativos de funcionamiento en documentos totalmente ajenos a los de protección de datos; imposibilitando un cumplimiento adecuado del deber de información;

- Que existe una imposibilidad técnica de auditar de manera externa los datos personales objeto de tratamiento en cada caso analizado, en base al argumento de la protección del código fuente y propiedad intelectual. Asimismo, la dificultad que supone en el control efectivo de los datos por el interesado, y el propio enfoque más agresivo de forzar la obligatoriedad de autorización o desactivación de cualquier elemento técnico que pudiera crear conflicto: antivirus, vpn, cortafuegos, etc;

- Que existe problemática a nivel del ejercicio de los derechos de acceso por la protección del código fuente y propiedad intelectual que se aduce para desestimarla; y

- Que se aplica de manera indistinta a menores de edad, por no contar con sistemas adecuados de verificación y enfocarse en casi todos los casos a una edad recomendada de 12 años.

Novedad de dichos resultados, aplicabilidad y conclusión

Se considera que este estudio de análisis jurídico general, junto con la aplicación de la DSA, la entrada en vigor del Reglamento Europeo de IA o la futura normativa de protección de menores y verificación, puede servir como aproximación para que los responsables y resto de figuras involucradas (*objeto de estudio o distintas*), tengan la oportunidad de reevaluar el tratamiento, aplicar garantías o valorar la aplicación de alguna de las medidas propuestas en apartado específico.

Finalmente, se considera que, aunque existe cierta bibliografía de especialistas de seguridad de la información sobre funcionamiento general de este tipo de sistemas, no se conoce ningún otro estudio o documento que intente desarrollar con cierta profundidad esta cuestión desde la protección de datos.

Executive Summary

Title: Analysis of the adequacy and operation of anti-cheat systems in video games: a particular consideration of real-time and administrator-level scanning of gaming devices

Author: Darío López Rincón.

Objetive and motivation

The purpose of this study is to provide a comprehensive legal analysis of the fully automated, real-time processing with legal effects and without human intervention, currently deployed by the following five algorithmic anti-cheat systems to prevent any unauthorized alterations in online games: Ricochet in Call of Duty: Warzone; Easy Anti-Cheat in Fortnite; BattlEye in XDefiant; VAC in Team Fortress 2; and Vanguard in Valorant.

Particular emphasis is placed on the most invasive and notable stage of processing, external to the game platform and considered crucial for the proper functioning of these systems: real-time scanning with administrator-level privileges of the files, programs, and resources on the device from which the player accesses the video game at any time.

Additionally, a section is included that summarizes the findings and results of an attempted external technical audit using two programs specialized in real-time metrics of resource usage and file access. This is intended to highlight the technical impossibility of obtaining actual personal information for comparison with personal data declared by the controller, as well as the use of deep analysis or forensic systems that could hinder the loading or removal of automatic access to the game.

Recognizing that these processing activities are intrinsically related to the prevention of cheating, a separate commentary on the issue of voice chat recording systems is provided, addressing the growing concerns of toxicity, harassment, or discrimination, especially involving minors. This includes the procedures for reporting cheating or inappropriate behavior detected by other players.

Design and methodology

To achieve the stated objective, this report is structured into the following four sections:

- A general analysis of the logs generated during game testing by applying programs to monitor resource usage and activity of the device used for testing, namely Procmon and Sysmon;

- A detailed analysis of information clauses, privacy policies, privacy options and functionalities, the exercise of rights, as well as any other related elements of interest, with a general assessment of the potential applicability of the Digital Services Act (DSA) or the Artificial Intelligence Act (AIA);

- A legal assessment of the adequacy of each of these elements based on the literal wording of the applicable data protection regulations and the guidelines, reports, or guides issued by the relevant supervisory authorities; and

- A proposal of solutions for those elements analyzed that are not considered to be in adequate compliance with the GDPR.

Results

The following conclusions can be drawn from the study:

- The processing under review is not inherently impossible to justify based on legitimate interests, nor does it fail to address a real need. However, it is considered that it lacks sufficient limitations and safeguards to adequately comply with the GDPR and pass the necessary proportionality test;

- The existence of less invasive alternatives, particularly concerning the first and most intense phase of scanning at the administrator level of the gaming device, suggests the need for reassessment. Moreover, there is a need to provide the player with a genuine right to object or an opt-out option during this stage;

- The player's reasonable expectations do not encompass the entire set of steps and the current control framework of these systems;

- There is inadequate information provided about the processing activities, especially concerning first-layer information. Additionally, there is a dispersion of explanatory operational elements across documents entirely unrelated to those on data protection, which could hinder compliance with the duty of information;

- The technical impossibility of externally auditing the specific personal data accessed by the player in each case due to source code protection and intellectual property rights makes it difficult for the player to exercise control over their data. Furthermore, the more aggressive approach of mandating the authorization or deactivation of any technical elements that could create conflicts, such as antivirus software, VPNs, firewalls, etc.;

- There is a conflict in exercising access rights due to the protection of source code and intellectual property, which is argued to be grounds for dismissal; and

- These systems are applied indiscriminately to minors, as they lack adequate verification systems and, in almost all cases, focus on a recommended age of 12 years.

Innovation of these results, applicability and conclusions

It is considered that this general legal analysis study, along with the application of the DSA, the entry into force of the RIA, or future regulations on the protection of minors and verification, can serve as a preliminary framework for data controllers and other relevant entities (*either those under study or others*) to re-evaluate their processing activities, apply necessary safeguards, or consider implementing some of the measures proposed in the relevant section.

Finally, it is noted that, while there is some literature from information security specialists regarding the general operation of such systems, there is no known study or document that attempts to address this issue in depth from a data protection perspective.