FIVERS

Regulatory update
Data protection, AI, IT and IP

No. 14 / 2024

DATA PROTECTION.

5 November 2024 - European Data Protection Board: first report on the status of implementation of the EU-US agreement (Data Privacy Framework) for the transfer of personal data from the EU to the US.

ARTIFICIAL INTELLIGENCE.

12 November 2024 - Milan Polytechnic's Fintech & Insurtech Observatory: IIA Index (Insurtech Investment Index) data show a strong surge of investments in artificial intelligence by the insurance industry in 2024.

DIGITAL MARKETS

11 November 2024 - EU Commission adopted further technical standards for the application of Regulation on digital operational resilience for the financial sector (Regulation (EU) 2022/2554) (DORA).

---

6 November 2024 - ESAs issue guidelines for DORA cooperation, focusing on communication and critical ICT service provider oversight.

---

6 November 2024 - EU Commission: published the Implementing Regulation of the Digital Services Act for the implementation of the reporting and transparency obligations of VLOPs and VLOSEs.

INFORMATION TECHNOLOGY

7 November 2024 - Supreme Court of Cassation: the crime of unauthorised access to the computer system also includes access by the manager using the employee's credentials.

---

6 November 2024 - Supreme Court of Cassation: telematic appeal valid even if the party has filed a complaint with an analogue copy of native digital documents.

INTELLECTUAL AND INDUSTRIAL PROPERTY

12 November 2024 - Ministry of Enterprises and Made in Italy (MIMIT): the provision in the Made in Italy Law for the protection of trademarks of particular national interest and value is operational.

---

12 November 2024 - Ministry of Enterprises and Made in Italy (MIMIT): - subsidies for green and tech transition of the fashion, textile and accessories industry under the Made in Italy Law available starting from December 11, 2024.

---

8 November 2024 – European Court of Justice: Member States are required to protect works of art in the European Union, irrespective of the country of origin of those works or the nationality of their author.

---

8 November 2024 – European Court of Justice: the directive on the legal protection of computer programs does not allow the holder of that protection to prohibit the marketing by a third party of software which merely changes variables transferred temporarily to a game console's RAM.

DATA PROTECTION

5 November 2024 - European Data Protection Board: first report on the status of implementation of the EU-US agreement (Data Privacy Framework) for the transfer of personal data from the EU to the US.

During its latest plenary, the European Data Protection Board (EDPB) adopted a **report on the first review of EU-U.S. Data Privacy Framework (DPF)**.

The EDPB welcomes the efforts by the U.S. authorities and the European Commission to implement the DPF and takes note of several developments that took place since the adoption of the adequacy decision in July 2023.

Regarding commercial aspects, i.e. the application and enforcement of requirements applying to companies self-certified under this framework, the EDPB notes that the U.S Department of Commerce took all relevant steps to implement the certification process. This includes developing a new website, updating procedures, engaging with companies, and conducting awareness-raising activities.

In addition, the redress mechanism for EU individuals has been implemented and there is comprehensive complaint-handling guidance published on both sides of the Atlantic. However, the low number of complaints received so far under the DPF highlights the importance of having U.S. authorities initiate monitoring activities concerning compliance of DPF-certified companies with the substantive DPF Principles.

The EDPB encourages the development of guidance by U.S. authorities, clarifying the requirements that DPF-certified companies would need to comply with when they transfer personal data that they have received from EU exporters. Guidance by U.S. authorities on human resources data would also be welcome.

Concerning the access by U.S. public authorities to personal data transferred from the EU to certified organisations, the EDPB focused; on the effective implementation of the safeguards introduced by the Executive Order 14086 in the U.S. legal framework, such as the necessity and proportionality principles and the new redress mechanism. The Board considers that the elements of the redress mechanism are in place; at the same time, it renews the call to the European Commission to monitor the practical functioning of the different safeguards, e.g. the implementation of the principles of necessity and proportionality. The EDPB also recommends that the Commission monitors future developments related to the U.S. Foreign Intelligence Surveillance Act, in particular given the extended reach of Section 702 after its reauthorisation by the U.S. Congress earlier this year.

Finally, the Board recommends that the next review of the EU-U.S. adequacy decision should take place within three years or less.

ARTIFICIAL INTELLIGENCE.

12 November 2024 - Milan Polytechnic's Fintech & Insurtech Observatory: IIA Index (Insurtech Investment Index) data show a strong surge of investments in artificial intelligence by the insurance industry in 2024.

The Italian insurtech sector is experiencing a moment of strong growth, driven by a surge in investments in artificial intelligence, as revealed by updated data from the Insurtech Investment Index. The index, devised by the Italian Insurtech Association (IIA) and monitored by the Milan Polytechnic's Fintech & Insurtech Observatory, confirmed a score of 20 out of 30 for 2024, up from 14 points in 2022, signalling a maturation of the insurance sector towards the adoption of advanced technologies.

At the heart of Italian insurance companies' interest is artificial intelligence, with 88% of companies investing in projects or partnerships in this area in the first six months of the year. The main applications relate

to claims management, policy underwriting and back-office processes, areas where AI has been shown to significantly improve the efficiency and speed of operations.

The Index also shows further growth in collaborations between startups and insurance companies: in 2023, partnerships increased by 80 per cent year-on-year to 45. These ties, together with the companies' internal projects, pushed total investments in the sector to EUR 44.8m, up 89% from EUR 23.7m in 2022. According to IIA forecasts, 2024 could become a record year for investments in AI: an estimated 50 million euros will be allocated by the end of the year, with a projection to reach 90 million in 2025. Insurtech has moved beyond the exploratory phase and is consolidating the ecosystem thanks to growing investments, which show how the industry has grasped the importance of innovating to improve processes and expand the market.

In 2024, Italian insurance companies invested mainly in AI integration in claims management (71%), improving the speed and quality of responses to customers, and in contract administration and customer management (52%), areas where automation has brought smoother and more personalised processes. Artificial intelligence has also found its way into policy underwriting and risk management (50 per cent), increasing the accuracy of analysis and predictive capacity of the industry.

The digitisation of back-office processes has received particular attention: 88% of companies have used AI to automate internal tasks, enabling more effective and flexible management. In addition, some specific technologies are finding wide adoption: chatbots and virtual assistants (78%), generative AI (76%) for customised responses, Machine Learning (73%) for predictive risk analysis and Robot Process Automation (45%) for document management.

Despite progress, the adoption of AI in insurance still presents several difficulties. Among the main issues encountered are integration with existing infrastructure (62%) and ethical concerns (52%), followed by privacy issues (57%) and regulatory compliance (48%). 'To overcome these challenges and remain competitive, insurance companies must invest not only in technology, but also in new skills,' commented Simone Ranucci Brandimarte, President of IIA, anticipating that by 2030 more than half of all policies will include at least one AI element.

The drive towards innovation, fuelled by collaboration between companies and start-ups, is set to grow, but it remains crucial to ensure adequate funding to compete at the European level

DIGITAL MARKETS

11 November 2024 - EU Commission adopted further technical standards for the application of Regulation on digital operational resilience for the financial sector (Regulation (EU) 2022/2554) (DORA).

The technical standards include the:

- Implementing Technical Standard (ITS) on standard forms, templates, and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat (the Reporting ITS);

- Regulatory Technical Standard (RTS) on the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents, and the content of the voluntary notification for significant cyber threats (the Reporting RTS); and

- RTS on harmonisation of conditions enabling the conduct of the oversight activities (the Harmonisation RTS).

The Reporting ITS

The Reporting ITS contains templates for the initial notification, intermediate report, and final report on major ICT-related incidents to be given to competent supervisory authorities under Article 19(4) of DORA. The Reporting ITS also clarifies that financial entities that provide information on non-major recurring ICT-related incidents that cumulatively meet the conditions for one major ICT-related incident must provide

information in an aggregated form. Likewise, financial entities that conclude after an assessment that the ICT-related incident previously reported as major does not meet such criteria must notify competent supervisory authorities of the reclassification.

The Reporting RTS

The Reporting RTS details the required contents of initial notifications, intermediate, and final reports to be given under Article 19(4) of DORA.

In addition, the Reporting RTS outlines the time limits for submission of the above notification and reports. Initial notification should be made within four hours from the classification of ICT-related incidents as major incidents and no later than 24 hours from the moment the financial entity becomes aware of it. Intermediate reports should be made within 72 hours of the initial notification, and an updated intermediate report should be submitted without undue delay where regular activities have been recovered. The final report should be made no later than one month after either the submission of the intermediate report or after the latest updated intermediate report.

Notably, when an ICT-related incident is not classified as major within 24 hours of becoming aware of it but later reclassified as major, the financial entity must submit the notification of the incident as major within four hours of the reclassification.

The Reporting RTS also notes the contents of voluntary notification of significant cyber threats under Article 19(2) of DORA.

The Harmonisation RTS

The Harmonisation RTS concerns the role of critical ICT third-party service providers in the financial sector under Article 31 of DORA. Specifically, critical ICT third-party service providers that submit a voluntary request to be designated as critical must provide a European Supervisory Authority (ESA) with all the information necessary to prove its criticality. The Harmonisation RTS details what must be included in the submission to the ESAs by critical ICT third-party service providers, alongside the content, structure, and format of such submissions.

The Harmonisation RTS also includes the information to be submitted to the Lead Overseer which is necessary to carry out its oversight duties under DORA.

The ESAs include the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA).

---

6 November 2024 - ESAs issue guidelines for DORA cooperation, focusing on communication and critical ICT service provider oversight.

On November 6, 2024, the Joint Committee of the European Supervisory Authorities (ESAs) published the Joint Guidelines on the oversight cooperation and information exchange between the ESAs and the competent authorities under the Digital Operational Resilience Act (DORA).

The ESAs constitute the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA). The Guidelines apply only to Article 31 of DORA and do not apply to, among others, one specific authority, financial entities, and critical ICT service providers, and the governance arrangements subject to the rules of procedure of the ESAs.

The Guidelines outline recommendations relating to language, communication, and accessibility. Specifically, communication should be made by electronic means, a single point of contact should be used for exchanging confidential information, and a dedicated online tool should be used to share information on a confidential and secure basis.

Critical ICT third-party service providers

The Guidelines also address the designation of critical ICT third-party service providers. For the purpose of designating them, those that are critical for financial entities, under Article 31(1)(a) of DORA, competent authorities should, without undue delay following the receipt of the register of information under DORA, make the full register available to the ESAs. Competent authorities should also make any quantitative or qualitative information necessary for the criticality assessment under Article 31(2) of DORA available to the ESAs.

The ESAs should make available to competent authorities of the financial entities using the services provided by ICT third-party service providers the legal name, identification code, country of registered office, and if necessary, parent group of the critical entity within 10 working days of receipt from the ICT third-party service provider. The lead overseer should also share with competent authorities of financial entities using the service of ICT third-party service providers:

- notification of any changes to the structure of management of the subsidiary; and
- the starting date from which the ICT third-party service provider will be subject to oversight.

In addition, the Guidelines detail information exchanges between the lead overseer and competent authorities. The lead overseer should inform competent authorities of financial entities using ICT services provided by a critical ICT third-party service provider of any:

- major incidents with direct or indirect impact on financial entities; and
- events that could represent an important risk to the continuity and sustainability of the provision of ICT services.

Suspension of services

The Guidelines outline that competent authorities must inform the lead overseer of their intention to notify financial entities of the possible decision being taken if the financial entity does not adopt appropriate contractual arrangements to address risks. The lead overseer must then assess the impact of such a decision on the critical ICT third-party service provider.

Notably, the Guidelines consider the scenario where two competent authorities plan or adopt decisions regarding financial entities using the same critical ICT third-party service providers, and how the competent authorities should be informed of inconsistent or divergent supervisory approaches.

The Guidelines (available here) enter into force on January 17, 2025.

---

6 November 2024 - EU Commission: published the Implementing Regulation of the Digital Services Act for the implementation of the reporting and transparency obligations of VLOPs and VLOSEs.

The European Commission published the Implementing Regulation – laying down templates concerning the transparency reporting obligations of providers of online platforms. The Implementing Regulation establishes uniform reporting templates and periods for providers of Very Large Online Platforms (VLOPs), Very Large Online Search Engines (VLOSEs), providers of intermediary services, and providers of hosting services under the Digital Services Act (DSA).

Reporting under the DSA.

Article 15(1) of the DSA requires providers of intermediary services to make publicly available, in a machine-readable format and in an easily accessible manner, at least once a year, clear, easily comprehensible reports on any content moderation that they engaged in during the relevant period. Article 15(1) of the DSA also establishes the required contents of such reports, including:

- information about the content moderation engaged in at the providers' own initiative, including the use of automated tools, and measures taken to provide training and assistance to persons in charge of content moderation; and
- for providers of intermediary services, the number of complaints received through the internal complaint handling systems, and for providers of online platforms, the basis of those complaints and decisions taken in respect of them.

Article 24(1) of the DSA outlines additional required information that must be included in the reports under Article 15(1) of the DSA.

Reporting under the Implementing Regulations.

The Implementing Regulation establishes an annual reporting period from January 1 until December 31. VLOPs and VLOSEs must publish their transparency reports every six months covering the period from January 1 until June 30, and from July 1 until December 31. The reports must be published at the latest two months after the conclusion of each reporting period.

Transparency reports must be retained for at least five years after their publication, and remain publicly available during this period. Where transparency reports are updated, they must be clearly marked that the report is an updated version alongside the changes that were made.

Annex II to the Implementing Regulation provides instructions for completing the transparency report templates. The templates include a Quantitative Template, to contain quantitative machine-readable information on content moderation, and a Qualitative Template to provide meaningful information on content moderation. Annex II clarifies that because the reporting requirements are not the same for VLOPs, VLOSEs, or providers of intermediary services among others, not all fields of the templates will apply to all types of service providers.

Transition period.

Annex II also notes that a transition period, to align the reporting timelines of providers of intermediary services, providers of hosting services, and providers of online platforms with the timelines of VLOPs and VLOSEs, ends on December 31, 2025. Annex II clarifies the applicable deadlines for the two different groups of service providers above during the transition period ending on December 31, 2025.

INFORMATION TECHNOLOGY

7 November 2024 - Supreme Court of Cassation: the crime of unauthorised access to the computer system also includes access by the manager using the employee's credentials.

The manager of a hotel acquired from a female collaborator access credentials to the company's protected computer system for the storage and management for promotional purposes of the customer base comprising approximately 90 thousand individual cards, accessing it for purposes unrelated to the mandate received.

The Supreme Court intervened on the matter. The appellant argued that in his capacity as director and superior of the employee he was entitled to ask for her credentials, also for the purpose of controlling her work, and further pointed out that shortly before, he had first-hand access to that data. For the Court, that fact is irrelevant.

The Court states that in the case of a computer system protected by credentials, each authorised person has his own personal ‘key’. That is because it is data which, quite simply, the owner considers must be protected, both by limiting access to those who are provided with those credentials and, at the same time, by ensuring that a digital trace is left of the individual accesses and of who carries them out.

It is wrong to take the view that, in the present case, the director alone, by reason of his duties, automatically had the power to access data which, on the other hand, according to the employer's discretionary

assessment, were to remain available only to certain employees, however subordinate to the applicant. The latter gained access to a database for which he did not have the credentials and, moreover, falsely claimed that the access was carried out by the employee who had unwittingly revealed his credentials to him.

In conclusion, the Supreme Court states that 'an employee who, although in a hierarchically superordinate position with respect to the holder of access credentials to a company computer system, reveals his credentials in order to gain access to it without having specific authorisation, infringes the employer's directives (even if implicit, but clear), since the very protection of data by means of access credentials is sufficient to make such directives manifest'.

---

6 November 2024 - Supreme Court of Cassation: telematic appeal valid even if the party has filed a complaint with an analogue copy of native digital documents.

The dispute reached the Court of Cassation. According to the appellants, the filing of the analogue copy of the certified e-mail message, its attachments and the receipt of acceptance and delivery with the relevant certificate of conformity replaced the filing of the electronic original for all purposes. In addition, it was to be considered that this document had not been contested by the counterparties; nor had the complaint of forgery been lodged; therefore, the declaration of unfeasibility of the appeal had to be considered unlawful.

The Court of Cassation, Civil Division II, in its Order No. 28207 of 4 November 2024, considers the plea to be well-founded. The lower court judge, explains the Supreme Court, had ascertained that 'the defence counsel for the main appellants, who had served the notice of appeal in telematic form, entered an appearance in the proceedings according to the traditional paper forms, filing analogue copies of native digital documents (of the summons, the service report, the receipts of acceptance and delivery of the certified e-mail message, with certification of conformity), without filing telematically the originals or computerised duplicates of such documents'. And with the closing appearance the defence of the appellants had filed the report of notification of the appeal accompanied by the receipts of acceptance and delivery in digital format.

The Court ofCassation does not agree with ' the formal rigour of the Court of Appeal' according to which in the case of telematic constitution of the appellant, the proof of service by certified mail of the summons instituting the appeal proceedings must be provided, by the hearing referred to in Article 350 of the Code of Civil Procedure, only by telematic means.

There is in fact no obligation to produce the notification by telematic means. For these reasons, the appeal is allowed by order No. 28207 of 4 November 2024.

INTELLECTUAL AND INDUSTRIAL PROPERTY

12 November 2024 - Ministry of Enterprises and Made in Italy (MIMIT): the provision in the Made in Italy Law for the protection of trademarks of particular national interest and value is operational.

By means of a special decree issued by the Head of the Department for Enterprise Policies, the Ministry of Enterprise and Made in Italy, with the publication in the Official Gazette, renders operative the Ministerial Decree of 3 July 2024, by which the MIMIT issued the implementing provisions of Article 7 of the so-called 'Collegato Made in Italy' (Law No. 206 of 27 December 2023).

The aim of the provision is to avoid dispersing the heritage represented by Made in Italy trademarks with at least 50 years of history, which enjoy a significant notoriety and are used for the marketing of products or services made by a national productive enterprise of excellence linked to the national territory.

Starting from next 2 December 2024, companies intending to terminate the activity linked to a trademark of particular interest and national value (not subject to transfer for consideration) will be able to send,

through a special format defined by the Ministry, their termination project to the Directorate General for Industrial Policy, Industrial Conversion and Crisis, Innovation, SMEs and Made in Italy (DGIND) of MIMIT.

The General Directorate, within three months from the receipt of the project, in case it expresses the interest to take over the ownership, will proceed to the preparation of the deed of free transfer of the trademark by the company.

The national or foreign company that intends to invest in Italy or transfer to Italy production activities located abroad and interested in using one or more trademarks owned by MIMIT, may then submit a specific request to the Mission Unit for the Attraction and Unlocking of Investments (UMASI).

The licence agreement by which MIMIT makes the trademark available is terminated if the licensee company ceases its activity or relocates its production plants outside the national territory.

---

12 November 2024 - Ministry of Enterprises and Made in Italy (MIMIT): - subsidies for green and tech transition of the fashion, textile and accessories industry under the Made in Italy Law available starting from December 11, 2024.

The Ministry of Enterprise and Made in Italy, in implementation of the interministerial decree of 8 August 2024, has set the terms and procedures for opening applications for access to subsidies for the implementation of investments aimed at the ecological and digital transition of companies in the textile, fashion and accessories sector, throughout the country, with a special director's order.

The measure, introduced by Art. 11 of the Made in Italy Law (206/2023), has a budget of 15 million euro.

From 12.00 noon on 11 December 2024 and until 31 January 2025, interested SMEs (identified with the specific ATECO codes) will be able to submit applications for subsidies exclusively through the online counter Invitalia, manager of the measure on behalf of the Ministry.

The facilitations to companies will be granted in the form of a non-repayable contribution, up to a maximum of 50 per cent of eligible expenses and a maximum limit of EUR 60,000, for the acquisition of specialist services, such as training activities for the company's employees, implementation of one or more enabling technologies aimed at fostering the development of business processes or innovative products (cloud computing big data and analytics, artificial intelligence, blockchain, advanced and collaborative robotics, additive manufacturing and 3D printing, Internet of Things, augmented reality, advanced manufacturing solutions, digital platforms for sharing skills, digital traceability systems of the production chain), obtaining environmental sustainability certifications, Life Cycle Assessment (LCA) analysis services.

---

8 November 2024 – European Court of Justice: Member States are required to protect works of art in the European Union, irrespective of the country of origin of those works or the nationality of their author.

Vitra, a Swiss company that manufactures designer furniture, holds intellectual property rights over chairs designed by the since-deceased spouses, Charles and Ray Eames, who were nationals of the United States of America. That furniture included the Dining Sidechair Wood, which was created as part of a furniture design competition organised by the Museum of Modern Art in New York (United States) and exhibited in that museum from 1950.

The company Kwantum, which operates a chain of interior furnishing shops in the Netherlands and in Belgium, marketed a chair called the ‘Paris chair’, allegedly in breach of Vitra’s copyright in the Dining Sidechair Wood. Vitra brought proceedings before the Netherlands courts with the aim, inter alia, of putting an end to that marketing. In that context, the Supreme Court of the Netherlands decided to refer questions to the Court of Justice for a preliminary ruling relating to the protection which, under Directive 2001/29 and Article 17(2) and Article 52(1) of the Charter of Fundamental Rights of the European Union (‘the

Charter'), may be granted in the European Union to a work of applied art originating in a third country and the author of which is not a national of a Member State.

In international law, the Berne Convention provides that authors who are nationals of the signatory countries enjoy in the other signatory countries, in principle, the same rights as national authors. However, the protection of works of applied art constitutes an exception to that principle. In that regard, the contracting parties have laid down a material reciprocity clause according to which works of applied art originating in countries in which such works are protected solely as designs and models are not entitled, in the other signatory countries, to such protection in addition to copyright protection. In this respect, the question referred to the Court of Justice by the Supreme Court of the Netherlands seeks to ascertain whether the Member States are still free to apply the material reciprocity clause contained in the Berne Convention to works of applied art originating in third countries which protect those works solely under a special regime, even though the EU legislature has not provided for such a limitation.

In its judgment, the Court of Justice answers in the negative: within the scope of Directive 2001/29, the Member States are no longer competent to implement the relevant stipulations of the Berne Convention.

First of all, the Court clarifies in that regard that a situation in which a company claims copyright protection for a subject matter of applied art marketed in a Member State, provided that such subject matter may be classified as a 'work' within the meaning of Directive 2001/29, falls within the material scope of EU law.

Next, the Court finds that the EU legislature, in adopting that directive, necessarily took into account all the works for which protection is sought in the territory of the European Union; moreover, that directive does not lay down any criterion relating to the country of origin of those works or to the nationality of their author. The Court adds that the application of the material reciprocity clause contained in the Berne Convention would undermine the objective of Directive 2001/29, which consists in the harmonisation of copyright in the internal market, since, under that clause, works of applied art originating in third countries might be treated differently in different Member States.

Lastly, the Court points out that, since the intellectual property rights in question are protected under Article 17(2) of the Charter, any limitation of those rights must, in accordance with Article 52(1) of the Charter, be provided for by law. It is for the EU legislature alone to determine whether the grant in the European Union of the rights laid down in Directive 2001/29 should be limited. In those circumstances, a Member State cannot rely on the Berne Convention in order to exempt itself from the obligations arising from that directive. Therefore, a Member State may not, by way of derogation from the provisions of EU law, apply the material reciprocity clause contained in the Berne Convention in respect of a work the country of origin of which is the United States of America.

---

8 November 2024 – European Court of Justice: the directive on the legal protection of computer programs does not allow the holder of that protection to prohibit the marketing by a third party of software which merely changes variables transferred temporarily to a game console's RAM.

Sony markets PlayStation video game consoles as well as games for those consoles. Until 2014, it offered for sale, among other products, the PlayStation Portable console and the game 'MotorStorm: Arctic Edge'.

Sony brought an action before the German courts against the undertaking Datel, which offers software and a device that are compatible with that PlayStation and presents the user with game options not provided at that stage of the game by Sony. Sony is of the view that those Datel products have the effect of altering the software which underpins its game and thereby infringe its exclusive right to authorise such alterations. It therefore requested those courts to prohibit Data from marketing the products in question and to order it to pay compensation for the loss allegedly suffered. The German Federal Court of Justice (BGH) has requested the Court of Justice to interpret the Directive on the legal protection of computer programs.

The BGH observes that Datel's software is installed by the user on the PlayStation and runs at the same time as the game software. It does not change or reproduce either the object code, the source code or the internal structure and organisation of Sony's software. It merely changes the content of the variables

temporarily transferred by Sony's games to the console's RAM, which are used during the running of the game. Thus, the game runs on the basis of those variables to the changed content.

The Court finds that the content of the variable data transferred by a computer program to the RAM of a computer and used by that program in its running does not fall within the protection specifically conferred by that directive, in so far as that content does not enable such a program to be reproduced or subsequently created. The directive protects only the intellectual creation as it is reflected in the text of the computer program's source code and object code. On the other hand, the directive does not protect the functionalities of the program or the elements by means of which users make use of such functionalities, unless they allow that program to be reproduced or subsequent created.
