

## Regulatory update Data protection, AI, IT and IP

No. 13 / 2024

### DATA PROTECTION.

22 October 2024 – Italian Data Protection Authority: systematic retention of employees' e-mails and access logs for disproportionate periods of time is unlawful.

---

### ARTIFICIAL INTELLIGENCE.

18 October 2024 – Regulatory perspectives of the proposal for a Directive on civil liability for damage caused by Artificial Intelligence.

---

### DIGITAL MARKETS

24 October 2024 – EU Commission: draft regulation on VLOP and VLOSE data access under DSA.

---

18 October 2024 – Italian Communications Authority: new web platform to send on line reports for relevant breaches of the electronic communication laws.

---

### INFORMATION TECHNOLOGY

17 October 2024 – EU Commission: NIS 2, adopted the first implementing rules of the Network Security Directive.

---

16 October 2024 – National Cybersecurity Agency: the *road map* for the gradual implementation of the obligations provided for by the NIS 2 Directive and the transposing legislative decree has been published.

---

16 October 2024 – Supreme Court of Cassation: it is not defamation if the sender is unaware that the Messenger account is accessed by several people.

---

### INTELLECTUAL AND INDUSTRIAL PROPERTY

25 October 2024 - Ministry of Made in Italy: opening from Oct. 29 of the counter to access funding from the Patents+ 2024 program.

---



**22 October 2024 - Ministry of Made in Italy: anti-counterfeiting report, in 9 months over 2,300 applications of the new Made in Italy Law.**

---



## DATA PROTECTION

### **22 October 2024 – Italian Data Protection Authority: systematic retention of employees' e-mails and access logs for disproportionate periods of time is unlawful.**

The systematic storage of employees' e-mails - carried out for a considerable period of time (amounting to three years following the termination of the labour relationship) - and the systematic storage of access logs to e-mail and management software used by the employees is disproportionate and not necessary to achieve the employer's stated purposes, namely those of ensuring the security of the computer network and the continuity of the company's business.

This was established by the Italian Data Protection Authority by fining a company for 80 thousand euros.

For such disproportionate purposes, the employer may not access the employee's or collaborator's e-mail or use software to keep a copy of messages. Such processing of personal data, in addition to constituting a violation of data protection regulations, is likely to carry out unlawful monitoring of the employee.

The Italian Data Protection Authority, which intervened following a complaint filed by a commercial agent, found that the company in the course of the employment relationship, through software, had made a backup of the e-mail, preserving both the contents and the access logs to the e-mail and the company's management system. The information collected had then been used by the company in litigation.

The Authority also ascertained the unsuitability and deficiency of the information given to workers. In fact, the document provided for the possibility for the employer to access the e-mail of its employees and collaborators to ensure the continuity of the company's business, in case of their absence or termination, without mentioning, among other things, the making of the backup and the related retention time.

This, moreover, had allowed the company to reconstruct, in minute detail, the activity of the employee, thus incurring a form of control prohibited by the Workers' Statute (Law of May 20, 1970 no. 300).

Finally, with regard to the use of data in court, the Italian Data Protection Authority recalls that the processing carried out by accessing the employee's e-mail for purposes of protection in the judicial sphere refers to litigation already in progress, not to abstract and indeterminate hypotheses of protection as in this case.

In addition to the sanction, the Authority ordered a ban on further processing of data through the software used to back up e-mail.

---

## ARTIFICIAL INTELLIGENCE.

### **18 October 2024 – Regulatory perspectives of the proposal for a Directive on civil liability for damage caused by Artificial Intelligence.**

In September 2022, the European Commission presented a proposal for a directive on the adaptation of non-contractual civil liability rules to artificial intelligence (AILD). While the European Parliament and the Council informally agreed on the text of the proposal in December 2023, it is expected that the text will change on the basis of a complementary impact assessment published by the European Parliamentary Research Service at the end of September 2024 and which identified the main shortcomings and proposed that the Directive extend its scope to include general-purpose AI systems and other "AI systems". *high-impact AI*, as well as software. It also discusses a mixed liability framework that balances fault-based liability and strict liability.

The EU Parliament's latest impact assessment recommends a transition from an AI-focused directive to a software liability regulation, to prevent market fragmentation and improve clarity across the EU.

The European Parliament's Legal Affairs Committee (JURI), which is responsible for adopting legislation on AI liability, is expected to decide in the coming weeks whether to follow the impact assessment's



suggestion to abandon the current proposal for a directive and recommend to the European Commission to propose a regulation on AI liability.

In the meantime, the EU Council has sent questions to the governments of the Member States on: (i) the steps that applicants should take to identify the person potentially responsible for the damage; and (ii) the rebuttable presumption of a causal link between the AI system and the harm in certain circumstances.

---

## DIGITAL MARKETS

### **24 October 2024 – EU Commission: draft regulation on VLOP and VLOSE data access under DSA.**

The European Commission opened a public consultation on a draft regulation for data access under the Digital Services Act (DSA), which mandates Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) to provide data for regulatory, research, and risk mitigation assessment purposes.

The draft introduces the DSA data access portal as a centralized information exchange, requiring registration and detailing personal data processing rules. It outlines the roles of the Commission as a processor and the Digital Services Coordinator in assessing reasoned access requests, considering data sensitivity and the rights of data providers.

The regulation also specifies conditions for providing data to vetted researchers and the prohibition of imposing certain requirements that could obstruct research, while allowing limitations on analytical tool use as stated in the access request. The consultation period ends on November 26, 2024.

---

### **18 October 2024 – Italian Communications Authority: new web platform to send on line reports for relevant breaches of the electronic communication laws.**

On October 15, 2024, the Italian Communications Authority's (AGCOM) [Portal of Reports](#) went live. Through this new online portal users and consumers will be able to send reports to the Authority in a simple and intuitive way: these are the reports currently submitted to Agcom through Forms D and P for contractual and legal violations committed by providers of electronic communications services; audiovisual media, pay-tv and postal services.

To access the system and submit the report, it is necessary to authenticate through SPID, CIE, CNS or eIDAS, and fill out the new electronic forms.

---

## INFORMATION TECHNOLOGY

### **17 October 2024 – EU Commission: NIS 2, adopted the first implementing rules of the Network Security Directive.**

The EU Commission has adopted the first implementing rules on the cybersecurity of critical entities and networks under the Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive).

The implementing regulation specifies cybersecurity risk management measures, as well as when an incident should be considered significant, to whom companies providing digital services must report it and in what timeframe. The implementing regulation will apply to specific categories of companies providing digital services, such as cloud computing service providers, data center service providers, online marketplaces, online search engines and social networking platforms. For each category of service providers, it is specified when an incident is considered significant, to whom it must be reported and in what time frame.



**16 October 2024 – National Cybersecurity Agency: the *road map* for the gradual implementation of the obligations provided for by the NIS 2 Directive and the transposing legislative decree has been published.**

IT security is increasingly important for companies and public administrations. From 16 October 2024, the new Italian legislation on *Network and Information Security (NIS 2)* is applicable. The fields of application of the legislation are increasing. The sectors involved become 18, of which 11 are highly critical and 7 critical, involving over 80 types of subjects, distinguishing them between essential and important in relation to the level of criticality of the activities carried out and the sector in which they operate. The National Cybersecurity Agency (ACN) is the competent authority for the application of NIS 2 and a single point of contact and has outlined a gradual and sustainable path to allow public and private organizations to comply with the new legal obligations.

This is considering the increased requirements for security measures and incident notification and the increased supervisory power given to the ACN and the bodies responsible for incident response and crisis management. New tools for cybersecurity are also planned, such as the coordinated disclosure of vulnerabilities, to be achieved through cooperation and information sharing at national and European level.

Compliance with the NIS regulations provides for a sustainable path with a gradual implementation of the obligations.

The first step for interested parties is to [register on the ACN portal](#). There is time from 1 December 2024 until 28 February 2025 for medium and large companies and, in some cases, also for small and micro enterprises.

To facilitate the implementation of incident notification obligations and safety measures, they will be defined progressively and following consultations within the sectoral tables following the decisions of the Director General of ACN which will be adopted by the first quarter of 2025.

There is also a differentiated implementation time window: 9 months for notifications and 18 months for security measures, starting from the date of consolidation of the list of NIS entities (end of March 2025). From April 2025, a shared path to strengthen national and European cybersecurity will therefore start.

To make it easier to understand the news, the ACN has published [a video](#) and [information pages](#).

---

**16 October 2024 – Supreme Court of Cassation: it is not defamation if the sender is unaware that the Messenger account is accessed by several people.**

The sending of defamatory messages through the Messenger platform does not constitute the crime of (aggravated) defamation *when* the use of this channel - in the belief of the agent - is not public but it is believed to interact with a private messaging application and to speak directly. The defendant had circulated a letter with harmful and defamatory content to the recipient, without being aware that other subjects also had access to the device (all belonging to an association to which the victim also belonged, as President). This circumstance makes the intent absent since there is a lack - according to the Supreme Court, which ruled so in its judgment no. 36217/2024 - of the awareness of communication "*with several persons*" required by the incriminating provision for the purposes of the existence of the intent of defamation.

## **INTELLECTUAL AND INDUSTRIAL PROPERTY**

**25 October 2024 - Ministry of Made in Italy: opening from Oct. 29 of the counter to access funding from the Patents+ 2024 program.**

As of 12 noon on Oct. 29, micro, small and medium-sized enterprises will be able to send applications to access the Brevetti+ 2024 incentives, the intervention promoted by the Ministry of Business and Made in Italy for the economic valorisation of patents, with a budget of 20 million euros.



The incentives, consisting of a non-repayable grant of up to a maximum of 140,000 euros and no more than 80 percent of eligible costs, will also be granted, on a de minimis basis, to newly established SMEs with registered and operational headquarters in Italy that meet at least one of the following requirements:

- be holders or licensees of a patent for industrial invention granted in Italy after January 1, 2023
- be holders of a national application for a patent for industrial invention filed after January 1, 2022 with a search report with a “non-negative” outcome
- be the holder of a patent granted by the EPO and validated in Italy after January 1, 2023
- be the owner of a European patent application or an international patent application filed after January 1, 2022, with a search report with a “non-negative” outcome claiming priority to a previous national patent application.

The subsidy will be up to 85 percent of eligible costs in the case of companies in possession of gender parity certification, and 100 percent for beneficiary companies that at the time of submission of the application are co-owners, with a public research organization, of the application for a patent or issued patent, or holders of an exclusive license having as its object a patent issued to one of the aforementioned public organizations, already transcribed at the UIBM, without territorial extension constraints.

The grant is for the purchase of the following specialized services:

- design, engineering and industrialization
- organization and development
- technology transfer.

The measure is managed by Invitalia on behalf of the Ministry of Made in Italy.

---

## **22 October 2024 - Ministry of Made in Italy: anti-counterfeiting report, in 9 months over 2,300 applications of the new Made in Italy Law.**

Nine months after the entry into force of the “Made in Italy” Law, there are 2,357 concrete cases of application of the new anti-counterfeiting regulatory provisions. Specifically, about 100 are the cases in which the provision regarding the destruction of seized counterfeit goods has been applied, and more than 2,200 are the cases in which the new fines have been applied, which have increased compared to the past.

Regarding enforcement actions, nearly 9,000 seizure operations were carried out in the first half of 2024. In particular, there were more than 2,700 operations carried out by the Guardia di Finanza and more than 4,000 by the Customs and Monopolies Agency. The Criminal Analysis Service of the Ministry of the Interior detected more than 400 seizures of counterfeit branded goods made by State Police, Carabinieri and Local Police.

This is the finding of the Cnalcis Report, produced by the General Directorate for Industrial Property - Italian Patent and Trademark Office of Mimit, on the activities carried out to combat counterfeiting by the relevant administrations. The data were presented at the launch of the ninth edition of Anti-Counterfeiting Week 2024.

“With the new legislation of tightens the grip on the serious phenomenon of counterfeiting. We are on the right track but we must not give up. In fact, the risks are growing with the spread of new technologies and e-commerce, so maximum attention to protect Made in Italy, a priority of our government,” said Minister Urso.

In the Law, in fact, measures have been introduced for the protection of Italian brands and excellence, through the strengthening of sanctions and the expansion of the tools available to the competent authorities.

At the sectoral level, the report continues, agribusiness was affected by about 300 interventions by the MASAF-ICQRF and 35 by the Carabinieri (Command for the Protection of Agribusiness), of which 26 were for protected PDO and PGI trademarks, 7 for plant privatives and 2 related to Made in Italy. Health

protection saw, by the Carabinieri - NAS, nearly 200 blackouts of websites selling fake health products. Finally, 1,200 operations were carried out by the Carabinieri for the protection of cultural heritage.

Also important is the institutional commitment to prevent and counter the spread of the online fake market: 7 are the web platforms with which the network of public-private collaboration has been consolidated, with the sharing of common intentions for remedial actions and tools.

Numerous actions to raise awareness among consumers, especially young people: more than 3,000 students involved this year in the fourth edition of the "Anti-Counterfeiting Day for Students"; various training activities carried out, including through webinars, to reach the largest number of people; 2 anti-counterfeiting campaigns and 6 events during the Anti-Counterfeiting Week 2024.

Another central target in actions to protect, including abroad, Industrial Property are businesses: the dedicated Anticounterfeiting Hotline collected 447 reports of possible infringements of Industrial Property rights.

Also for 2023, Mimit's Italian Patent and Trademark Office processed more than 500 thousand data in the IPERICO database, received from the various databases of Italian enforcement authorities. The main evidences that emerged for 2023 record that the product categories most seized for counterfeiting were clothing (43.2 percent), clothing accessories (23 percent) and footwear (10.5 percent), all sectors historically affected by illegal business and representing some of the manufacturing and Made in Italy products of excellence. As for the origin of fake items, China appears to prevail, followed by Turkey, Morocco and Pakistan.

Between 2008 and 2023, there were almost 241,000 seizures and 699.5 million counterfeit items seized, for an estimated economic value of the seized goods of more than 6.14 billion euros removed from the illegal circuit.

---