

Aggiornamento Data protection, AI, IT e IP

n. 10 / 2024

DATA PROTECTION

16 settembre 2024 – Garante privacy: parere favorevole sullo schema di decreto legislativo di recepimento della Direttiva UE 2022/2557 sulla resilienza dei soggetti critici.

12 settembre 2024 – Corte di Giustizia dell'Unione Europea: interpretazione della base di legittimità del trattamento rappresentata dall'adempimento di un contratto, o di un obbligo legale e dal perseguimento del legittimo interesse nel caso di divulgazione dei dati personali dei soci di fondi di investimento.

11 settembre 2024 - La Commissione UE annuncia una consultazione pubblica sulle clausole contrattuali standard (SCC) per il trasferimento di dati a Titolari e Responsabili del trattamento di Paesi terzi soggetti al GDPR.

10 settembre 2024 - L'EDPB collaborerà con la Commissione europea per sviluppare linee guida sull'interazione tra GDPR e DMA.

INTELLIGENZA ARTIFICIALE.

5 settembre 2024 - Il Consiglio d'Europa apre alla firma il primo trattato globale sull'intelligenza artificiale.

5 settembre 2024 - Il Consiglio d'Europa pubblica un rapporto sugli approcci normativi all'intelligenza artificiale nella Finanza.

MERCATI DIGITALI

16 Settembre 2024 – Pubblicato in Gazzetta Ufficiale il decreto legislativo n. 129/2024, di adeguamento della normativa nazionale al Regolamento (UE) 2023/1114 relativo ai mercati delle criptoattività (Regolamento MiCAR).

6 Settembre 2024 – Commissione UE: rilasciate le FAQ esplicative del Regolamento 2054/2023 (Data Act).



INFORMATION TECHNOLOGY

10 Settembre 2024 – Corte di Cassazione: La notifica telematica si perfeziona quando è generata la ricevuta di accettazione.

CYBERSECURITY

6 Settembre 2024 - Agenzia Nazionale per la Cybersicurezza: pubblicato il DPCM per la ripartizione dei fondi nel triennio 2024 – 2026 nell’ambito della Strategia nazionale di cybersicurezza.

DATA PROTECTION

16 Settembre 2024 – Garante privacy: parere favorevole sullo schema di decreto legislativo di recepimento della Direttiva UE 2022/2557 sulla resilienza dei soggetti critici.

[Parere favorevole](#) del Garante Privacy sullo schema di decreto legislativo che recepisce la direttiva europea sulla resilienza dei soggetti critici (direttiva CER - *critical entities resilience*), operativi in settori particolarmente delicati (energia, sanità, infrastrutture digitali, PA).

Lo schema di decreto legislativo prevede, tra l'altro, l'introduzione di misure, criteri, obblighi, sanzioni e disposizioni volti a garantire l'erogazione dei servizi essenziali per il mantenimento di funzioni vitali della società o di attività economiche, della salute e della sicurezza pubbliche o dell'ambiente.

Nel rendere il parere al Governo, il Garante ha ritenuto che lo schema di decreto legislativo, pur non presentando particolari criticità sotto il profilo della protezione dati, necessiti di alcune integrazioni in merito alla verifica dei precedenti penali per quanti ricoprono ruoli sensibili all'interno delle strutture.

In particolare, l'Autorità ha chiesto di precisare quali siano le categorie di precedenti (essenzialmente penali) ritenuti "rilevanti" e di disciplinare le modalità e i tempi di conservazione dei certificati del casellario giudiziale europeo acquisiti, demandando eventualmente anche alla fonte regolamentare.

Occorre poi valutare, secondo il Garante, l'opportunità di integrare lo schema richiamando gli adempimenti previsti nei casi in cui particolari eventi o incidenti implicino violazioni di dati personali.

12 Settembre 2024 – Corte di Giustizia dell'Unione Europea: interpretazione della base di legittimità del trattamento rappresentata dall'adempimento di un contratto, o di un obbligo legale e dal perseguimento del legittimo interesse nel caso di divulgazione dei dati personali dei soci di fondi di investimento.

La Corte di Giustizia UE ha emesso una importante sentenza pregiudiziale ([2024/738](#)) sulla corretta applicazione degli articoli 6, comma 1, lettera (b), 6, comma 1, lettera (c) e 6, comma 1, lettera (f) del Regolamento UE 679/2016 sulla tutela dei dati personali. Come è noto, si tratta delle basi di liceità del trattamento rappresentate dall'adempimento di obbligazioni contrattuali, di un obbligo legale e dal perseguimento del legittimo interesse, proprio o di un terzo.

Il caso: su richiesta di un socio di un fondo di investimento, costituito sotto forma di società di persone ad azionariato diffuso, era stato richiesto al fondo di divulgare informazioni su tutti i soci che detenevano partecipazioni indirette in tale fondo, tramite società fiduciarie, indipendentemente dall'entità della loro partecipazione al capitale di detto fondo, al fine di entrare in contatto e negoziare con loro il riacquisto delle loro quote sociali, o - ancora - di coordinarsi con questi ultimi al fine di formare una volontà comune nell'ambito di decisioni dei soci.

La Corte UE ha ritenuto che il trattamento rappresentato dalla divulgazione dei dati personali dei soci può essere considerato necessario alla esecuzione del contratto in forza del quale tali soci hanno acquistato tali partecipazioni, ai sensi dell'articolo 6, comma 1, lettera (b) del GDPR, soltanto a condizione che tale trattamento sia oggettivamente indispensabile per realizzare una finalità che è parte integrante della prestazione contrattuale destinata a questi stessi soci, di modo che l'oggetto principale del contratto non potrebbe essere conseguito in assenza di tale trattamento. Ciò non si verifica se tale contratto esclude espressamente la divulgazione di tali dati personali ad altri detentori di partecipazioni.



Quanto al perseguimento del legittimo interesse ai sensi dell'articolo 6, comma 1, lettera (f) del GDPR, la CGUE ha ritenuto che il trattamento rappresentato dalla divulgazione dei dati personali dei soci può essere considerato necessario per il perseguimento del legittimo interesse di terzi, ai sensi di tale disposizione, solo a condizione che detto trattamento sia strettamente necessario per la realizzazione di un simile legittimo interesse e, alla luce di tutte le circostanze pertinenti, gli interessi o le libertà e i diritti fondamentali di detti soci non prevalgano su tale interesse legittimo.

Quanto all'adempimento di un obbligo legale ai sensi dell'articolo 6, comma 1, lettera (c) del GDPR, la CGUE ha ritenuto che il trattamento rappresentato dalla divulgazione dei dati personali dei soci può essere considerato giustificato, ai sensi di tale disposizione, quando è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento, in virtù del diritto dello Stato membro interessato, come precisato dalla giurisprudenza di tale Stato membro, a condizione che tale giurisprudenza sia chiara e precisa, che la sua applicazione sia prevedibile per le persone che vi sono sottoposte e che risponda a un obiettivo di interesse pubblico e sia proporzionata a quest'ultimo.

11 settembre 2024 - La Commissione UE annuncia una consultazione pubblica sulle clausole contrattuali standard (SCC) per il trasferimento di dati a Titolari e Responsabili del trattamento di Paesi terzi soggetti al GDPR.

La Commissione europea ha annunciato il prossimo avvio, prima della fine del 2024 di una consultazione pubblica sulle clausole contrattuali standard (SCC) ai sensi del Capo V dal Regolamento generale sulla protezione dei dati (GDPR).

Le clausole contrattuali standard sono disposizioni tipo sulla protezione dei dati personali che gli esportatori di dati dell'UE possono incorporare nei loro contratti per trasferire dati personali a importatori di dati situati in paesi terzi, in linea con i requisiti del Regolamento generale sulla protezione dei dati (GDPR). La consultazione pubblica verterà in particolare sulle clausole utilizzate nel caso specifico dell'importatore di dati situato in un Paese terzo ma sia direttamente soggetto al GDPR (cfr. art. 3, comma 2, del GDPR). Esse integrano le clausole esistenti per i trasferimenti di dati a importatori di Paesi terzi non soggetti al GDPR.

E possibile partecipare – una volta indetta – alla consultazione pubblica consultando [questa pagina](#).

10 settembre 2024 - L'EDPB collaborerà con la Commissione europea per sviluppare linee guida sull'interazione tra GDPR e DMA.

I servizi della Commissione incaricati dell'applicazione della legge sui mercati digitali (DMA) e il Comitato europeo per la protezione dei dati (EDPB) hanno deciso di collaborare per chiarire e fornire orientamenti sull'interazione tra la DMA e il GDPR.

Questo dialogo rafforzato tra i servizi della Commissione e l'EDPB si concentrerà sugli obblighi applicabili ai *gatekeeper* digitali ai sensi della DMA, che presentano una forte interazione con il GDPR, in quanto è necessario garantire l'applicazione coerente ai *gatekeeper* digitali dei quadri normativi applicabili.

Lo sviluppo di un'interpretazione coerente del DMA e del GDPR, nel rispetto delle competenze di ciascuna autorità di regolamentazione nelle aree in cui il GDPR si applica e viene citato nel DMA, è fondamentale per attuare efficacemente i due quadri normativi e raggiungere i loro obiettivi rispettivi e complementari.

Il DMA ha istituito un gruppo di alto livello per fornire alla Commissione consulenza ed esperienza al fine di garantire che il DMA e le altre normative settoriali applicabili ai *gatekeeper* siano attuate in modo coerente e complementare. La Commissione e i rappresentanti di EDPB e EDPS erano già impegnati nel

gruppo di alto livello per quanto riguarda gli obblighi relativi ai dati e all'interoperabilità. Questo nuovo progetto nasce dal precedente impegno e approfondisce la cooperazione in relazione ai due quadri normativi specifici.

INTELLIGENZA ARTIFICIALE.

10 Settembre 2024 – Il Board per l'AI previsto dal Regolamento 2024/1689 (AI Act) avvia i lavori sull'attuazione dell'AI Act.

La Commissione ospita la prima riunione ufficiale del [Consiglio sull'intelligenza artificiale \(IA\)](#), dopo l'entrata in vigore del Regolamento 2024/1689 (AI Act) lo scorso 1° agosto.

La sessione inaugurale, che si tiene a Bruxelles, segna un passo importante nell'impegno dell'UE nel definire un quadro solido per la *governance* dell'intelligenza artificiale.

L'AI Board è composto da rappresentanti di alto livello della Commissione e di tutti gli Stati membri dell'UE e sta discutendo su come migliorare lo sviluppo e l'adozione dell'IA nell'UE e sui prossimi passi nell'implementazione del Regolamento. Il Garante europeo della protezione dei dati (EDPS) e i rappresentanti SEE/EFTA di Norvegia, Liechtenstein e Islanda partecipano come osservatori.

La riunione ha affrontato i seguenti ambiti chiave: l'organizzazione del Consiglio per l'intelligenza artificiale e l'adozione del suo regolamento interno; la politica dell'UE in materia di intelligenza artificiale, tra cui l'iniziativa GenAI4EU e le attività internazionali in materia di intelligenza artificiale; l'analisi dei primi risultati della Commissione UE relativi all'attuazione dell'AI Act; lo scambio di buone pratiche per gli approcci nazionali alla *governance* dell'intelligenza artificiale e all'attuazione del Regolamento 2024/1689.

5 settembre 2024 - Il Consiglio d'Europa apre alla firma il primo trattato globale sull'intelligenza artificiale.

La Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale e i diritti umani, la democrazia e lo stato di diritto ([CETS n. 225](#)) è stata aperta alla firma durante una conferenza dei ministri della Giustizia del Consiglio d'Europa a Vilnius. Si tratta del primo trattato internazionale giuridicamente vincolante volto a garantire che l'uso dei sistemi di intelligenza artificiale sia pienamente coerente con i diritti umani, la democrazia e lo Stato di diritto.

La Convenzione quadro è stata firmata da Andorra, Georgia, Islanda, Norvegia, Repubblica di Moldova, San Marino, Regno Unito, Israele, Stati Uniti d'America e Unione Europea.

Il trattato fornisce un quadro giuridico che copre l'intero ciclo di vita dei sistemi di IA. Promuove il progresso e l'innovazione dell'IA, gestendo al contempo i rischi che essa può comportare per i diritti umani, la democrazia e lo Stato di diritto. Per resistere alla prova del tempo, è neutrale dal punto di vista tecnologico.

La Convenzione quadro è stata adottata dal Comitato dei Ministri del Consiglio d'Europa il 17 maggio 2024. Il trattato è stato negoziato dai 46 Stati membri del Consiglio d'Europa, dall'Unione Europea e da 11 Stati non membri (Argentina, Australia, Canada, Costa Rica, Santa Sede, Israele, Giappone, Messico, Perù, Stati Uniti d'America e Uruguay). Rappresentanti del settore privato, della società civile e del mondo accademico hanno contribuito come osservatori.

Il trattato entrerà in vigore il primo giorno del mese successivo alla scadenza di un periodo di tre mesi dalla data in cui cinque firmatari, tra cui almeno tre Stati membri del Consiglio d'Europa, lo avranno ratificato. I Paesi di tutto il mondo potranno aderire al trattato e impegnarsi a rispettarne le disposizioni.

5 settembre 2024 - Il Consiglio d'Europa pubblica un rapporto sugli approcci normativi all'intelligenza artificiale nella Finanza.

L'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) ha annunciato la pubblicazione di un [rapporto-indagine](#) sugli approcci normativi all'intelligenza artificiale (IA) nella Finanza. Il rapporto analizza, tra l'altro, i diversi approcci normativi all'uso dell'IA nella finanza in 49 giurisdizioni OCSE e non OCSE.

La stragrande maggioranza degli intervistati ha dichiarato di disporre di una regolamentazione adeguata, pur riconoscendo che potrebbero esserci delle lacune e che potrebbero essere utili indicazioni più generali. L'assenza di una regolamentazione settoriale esplicita per l'IA nella Finanza nella maggior parte delle giurisdizioni intervistate potrebbe essere (almeno in parte) spiegata dal fatto che la regolamentazione, le leggi e le linee guida finanziarie esistenti si applicano alle attività finanziarie indipendentemente dalla tecnologia utilizzata.

Gli intervistati hanno dichiarato inoltre che, quando l'IA viene utilizzata in settori per applicazioni coperte da norme o linee guida esistenti, tali norme o linee guida dovrebbero essere generalmente applicate indipendentemente dal fatto che la decisione sia stata presa dall'IA (con o senza intervento umano), da modelli tradizionali o da esseri umani. Ciò include, ad esempio, le norme generali sulla prudenza aziendale, le leggi e i regolamenti sulla protezione dei consumatori/investitori, le linee guida sulla gestione del rischio, i requisiti di divulgazione, i manuali relativi alla *governance* informatica e le leggi e i regolamenti sulla sicurezza informatica e sulla resilienza operativa che continuano ad applicarsi indipendentemente dalla tecnologia utilizzata. I progressi tecnologici non rendono inapplicabili gli standard di sicurezza e solidità e i requisiti di conformità esistenti. Il rapporto evidenzia che molti dei rischi legati all'IA non sono necessariamente nuovi o unici per l'innovazione dell'IA, ma piuttosto amplificati e amplificati dall'uso di tale innovazione - o si manifestano in modi diversi.

Il rapporto si basa su 49 risposte all'Indagine OCSE sugli approcci normativi all'IA in ambito finanziario da parte di 38 Paesi OCSE (ad es. Australia, Austria, Belgio, Canada, Cile, Colombia, Costa Rica, Repubblica Ceca, Danimarca, Estonia, Finlandia, Francia, Germania, Grecia, Ungheria, Islanda, Irlanda, Israele, Italia, Giappone, Corea, Lettonia, Lituania, Lussemburgo, Messico, Paesi Bassi, Nuova Zelanda, Norvegia, Polonia, Portogallo, Repubblica Slovacca, Slovenia, Spagna, Svezia, Svizzera, Turchia, Regno Unito, Stati Uniti) e da 6 Paesi candidati all'adesione all'OCSE (Argentina, Brasile, Bulgaria, Italia e Stati Uniti). Argentina, Brasile, Bulgaria, Croazia, Perù, Romania) e da 4 giurisdizioni non appartenenti all'OCSE (Hong Kong, Cina, Indonesia, Singapore, Sudafrica), nonché da una risposta consolidata fornita dalle istituzioni dell'UE (CE, EBA, EIOPA, ESMA) ed è stata condotta nel primo trimestre del 2024.

La stragrande maggioranza delle giurisdizioni ha introdotto una qualche forma di politica che copre l'IA in (parti della) Finanza, anche se in forme diverse: legislazione intersettoriale che copre parte dell'attività finanziaria; norme o proposte vincolanti emesse dalle autorità di regolamentazione finanziaria e orientamenti o chiarimenti non vincolanti rilasciati dalle autorità di regolamentazione finanziaria/supervisione. È importante notare che questi approcci non si escludono a vicenda. Ad esempio, nelle giurisdizioni con una legislazione vincolante, la normativa settoriale esistente continua ad essere applicata senza necessariamente fare riferimento esplicito all'IA e dato l'approccio tecnologicamente neutrale dei Paesi membri dell'OCSE. In particolare, alcuni Paesi hanno introdotto (o sono in procinto di farlo) una legislazione relativa esclusivamente all'IA, come ad esempio Brasile, Cile, Colombia e Perù. Queste legislazioni sono intersettoriali e, nel caso della legge europea sull'IA, contengono disposizioni esplicite per parti specifiche del settore finanziario. Ad esempio, l'EU AI Act regola le valutazioni del merito di credito basate sull'IA da parte delle banche, nonché la determinazione dei prezzi e la valutazione del rischio nelle assicurazioni sulla vita e sulla salute, con requisiti più severi applicabili a queste applicazioni finanziarie basate sull'IA in quanto considerate casi d'uso ad alto rischio. Un piccolo numero di norme o proposte di norme sono state introdotte dai regolatori finanziari per settori o parti specifiche delle attività.

Orientamenti politici non vincolanti (ad esempio principi, linee guida, libri bianchi) sull'uso dell'IA sono stati segnalati in diverse giurisdizioni e sono esplicitamente rivolti alle attività finanziarie o sono trasversali e comprensivi delle attività finanziarie. Tali orientamenti possono essere guidati dai governi, con progetti o libri bianchi che coprono tutti i settori dell'attività economica, compresa la finanza (ad esempio, l'ordine esecutivo del presidente degli Stati Uniti Biden sullo sviluppo e l'uso sicuro e affidabile dell'intelligenza

artificiale; o il libro bianco del governo britannico “*A pro-innovation approach to AI Regulation*”). Tali orientamenti incoraggiano inoltre le autorità di regolamentazione finanziaria a considerare l'utilizzo di tutte le loro autorità per proteggere i consumatori e gli investitori dai rischi che possono derivare dall'uso dell'IA (ad esempio negli Stati Uniti).

In alcune giurisdizioni le autorità di regolamentazione finanziaria hanno emanato anche linee guida non vincolanti che forniscono raccomandazioni generali per l'uso dell'IA nella finanza o si concentrano su aree specifiche di attività (ad esempio, servizi di *robo-advisory*, valutazione del merito di credito). Solo una minoranza di autorità di regolamentazione finanziaria/vigilanza nelle giurisdizioni intervistate ha emesso specifiche aspettative di vigilanza o chiarimenti sull'uso dell'IA nella finanza.

Alcuni intervistati hanno riferito che, a livello di attuazione pratica, potrebbero essere necessarie ulteriori linee guida di regolamentazione/vigilanza per assistere le entità autorizzate/vigilate nella loro conformità, date le questioni uniche che emergono nell'impiego dell'innovazione dell'IA, a seconda dei casi. Infine, la maggior parte di coloro che hanno risposto all'indagine non prevede di introdurre nuove norme sull'IA nella finanza nel prossimo futuro.

MERCATI DIGITALI

16 Settembre 2024 – Pubblicato in Gazzetta Ufficiale il decreto legislativo n. 129/2024, di adeguamento della normativa nazionale al Regolamento (UE) 2023/1114 relativo ai mercati delle cryptoattività (Regolamento MiCAR).

Publicato in Gazzetta Ufficiale, Serie Generale n. 215 del 13 settembre 2024, il Decreto Legislativo n. 129 del 5 settembre 2024, di adeguamento della normativa nazionale al [Regolamento \(UE\) 2023/1114](#) (anche noto come MiCAR), relativo ai mercati delle cryptoattività.

Gli articoli 93 e 94 del [Regolamento \(UE\) 2023/1114](#) richiedono agli Stati membri di designare le autorità competenti (dotate dei necessari poteri di vigilanza) incaricate di svolgere le funzioni e i compiti ivi previsti, comunicando tale designazione alle competenti autorità (EBA ed ESMA).

Il [Decreto Legislativo n. 129 del 5 settembre 2024](#) è dunque la normativa nazionale di coordinamento al Regolamento MiCAR che assolve a tali compiti individuando nella Banca d'Italia e nella CONSOB le autorità nazionali competenti ai sensi dell'art. 93. Tra i poteri loro conferiti dal decreto legislativo vi è anche quello di emanare disposizioni di attuazione del decreto (sempre in conformità agli orientamenti adottati dall'ESMA e dall'EBA), nonché disposizioni riguardanti le modalità d'esercizio dei poteri di vigilanza.

Il decreto 129/2024 disciplina poi le modalità di esercizio dei poteri di vigilanza e di autorizzazione a seconda delle cryptoattività (token collegati ad attività -o ART, nel Capo II; token di moneta elettronica, o EMT, nel Capo III; crypto-attività diverse dai token collegati ad attività o dai token di moneta elettronica, nel Capo IV), regola i profili autorizzatori e di vigilanza sui prestatori di servizi per le crypto-attività (o CASP, nel Capo V e fissa norme in materia di prevenzione e vigilanza sugli abusi di mercato.

Infine, il decreto di coordinamento al MiCAR introduce anche le prime norme nazionali specifiche sui token collegati ad attività e sui prestatori di servizi per le crypto-attività e specifica competenze e poteri della CONSOB circa il controllo degli obblighi da parte degli emittenti, degli offerenti e delle persone che chiedono l'ammissione alla negoziazione di crypto-attività di comunicare al pubblico le informazioni privilegiate che li riguardano.



6 Settembre 2024 – Commissione UE: rilasciate le FAQ esplicative del Regolamento 2054/2023 (Data Act).

La Commissione UE ha rilasciato un interessante documento esplicativo in forma di [FAQ](#) relativo al Regolamento 2054/2023 – anche noto come Normativa sui Dati o Data Act – che sarà applicabile a partire dal 12 Settembre 2025.

Il [Data Act](#) stabilisce un insieme orizzontale di norme sull'accesso e l'uso dei dati che rispetta la protezione dei diritti fondamentali e apporta benefici ad ampio raggio all'economia e alla società europee. Aumenta la disponibilità dei dati, in particolare quelli industriali, e incoraggia l'innovazione basata sui dati, garantendo nel contempo l'equità nell'allocatione del valore dei dati tra tutti gli attori dell'economia dei dati.

Le FAQ supportano l'applicazione pratica del Data Act e chiariscono aspetti quali: l'interazione con altre normative della UE (come ad esempio il GDPR, o il DMA, etc), l'accesso ai dati e il loro uso nel contesto dell'IoT (*Internet of Things*), le pratiche commerciali nell'ambito del *data sharing*; le condizioni di accesso ai dati delle imprese da parte delle autorità pubbliche in caso di urgenze, i meccanismi di risoluzione alternative delle controversie e gli aspetti risarcitori nonché le condizioni per il passaggio da un fornitore di un servizio di trattamento dei dati (es: cloud) a un altro, gli aspetti di interoperabilità e le prospettive future.

INFORMATION TECHNOLOGY

10 Settembre 2024 – Corte di Cassazione: La notifica telematica si perfeziona quando è generata la ricevuta di accettazione.

In un giudizio avente ad oggetto la domanda di inefficacia di un provvedimento ingiuntivo, la Cassazione rileva in via preliminare l'inammissibilità del ricorso per mancata prova della sua notificazione. Nello specifico, non risultano depositate la ricevuta di accettazione e la ricevuta di avvenuta consegna, cd. RAC, né nel fascicolo telematico né sono state rinvenute altrove dalla Cancelleria.

Nelle sue argomentazioni, la Corte ribadisce che *«In tema di notifica a mezzo PEC (...) la prova dell'avvenuta notificazione è costituita dalla cd. ricevuta di avvenuta consegna (RAC), che costituisce il documento idoneo a dimostrare, fino a prova del contrario, che il messaggio informatico è pervenuto nella casella di posta elettronica del destinatario»*.

Tale principio è stato precisato anche dalla Consulta, la quale ha dichiarato l'illegittimità costituzionale dell'art. 16-*septies* D.L. n. 179/2012, nella parte in cui prevede che *«la notifica eseguita con modalità telematiche la cui ricevuta di accettazione è generata dopo le ore 21 ed entro le ore 24 si perfeziona per il notificante alle ore 7 del giorno successivo, anziché al momento di generazione della predetta ricevuta»*.

Pertanto, ai fini della determinazione del momento di perfezione della notifica telematica, non rileva né il momento della spedizione del messaggio PEC né quello in cui è generato il messaggio di avvenuta consegna.

Con ordinanza n. 24010 del 6 settembre 2024, la Cassazione dichiara il ricorso inammissibile.

CYBERSECURITY

6 Settembre 2024 - Agenzia Nazionale per la Cybersicurezza: pubblicato il DPCM per la ripartizione dei fondi nel triennio 2024 – 2026 nell'ambito della Strategia nazionale di cybersicurezza.

È stato pubblicato nella [Gazzetta Ufficiale n. 207 del 4 settembre 2024](#) il DPCM per la ripartizione dei fondi necessari all'attuazione della [Strategia nazionale di cybersicurezza 2024-26](#). Nel triennio di riferimento, il provvedimento assegna circa 347 milioni di euro alle Amministrazioni individuate dal Piano di implementazione.



Il Fondo per l'attuazione della Strategia nazionale di cybersicurezza e il Fondo per la gestione della cybersicurezza sono stati istituiti dall'articolo 1, comma 899, della legge 197/2022. Il primo Fondo serve a finanziare investimenti volti al conseguimento dell'autonomia tecnologica in ambito digitale e l'innalzamento dei livelli di cybersicurezza dei sistemi informativi nazionali. Il secondo è destinato a supportare le attività di gestione operativa di tali progetti.

Assieme ai fondi del PNRR e alle risorse proprie delle Amministrazioni sono il principale strumento per l'attuazione della Strategia nazionale di cybersicurezza 2022 – 2026 e l'innalzamento della resilienza cibernetica del nostro Paese.