Aggiornamento professionale nei settori Data Protection, AI, ICT e IP

n. 1 / 2024

DATA PROTECTION

30 aprile 2024 - Sentenza della Corte di Giustizia UE nella causa C-178/22 - Vita privata e perseguimento di reati gravi: il giudice incaricato di autorizzare l'accesso ai tabulati telefonici per identificare gli autori di un reato, per il cui perseguimento la legge nazionale prevede un tale accesso, deve poter rifiutare o limitare detto accesso.

---

30 aprile 2024 - Sentenza della Corte di Giustizia UE nella causa C-470/21- Lotta contro i reati e ingerenza nei diritti fondamentali: un'autorità pubblica nazionale incaricata della lotta contro le contraffazioni commesse online può accedere ai dati identificativi a partire da un indirizzo IP.

---

26 aprile 2024 – Approvato in via definitiva il Regolamento UE istitutivo dello Spazio europeo dei dati sanitari (EHDS Regulation).

---

22 aprile 2024 – Attivo dal 22 aprile al 30 giugno 2024 il servizio per opporsi all'alimentazione automatica del Fascicolo Sanitario Elettronico mediante caricamento dei dati sanitari antecedenti al 19 Maggio 2020.

---

23 aprile 2024 – Corte costituzionale: le Regioni non possono disciplinare autonomamente la materia del trattamento dei dati personali.

---

18 aprile 2024 - Il Comitato europeo per la protezione dei dati personali - EDPB stabilisce le priorità per il periodo 2024-2027 e chiarisce i meccanismi di ricorso del DPF.

---

17 aprile 2024 – Comitato europeo per la protezione dei dati personali: Opinion 8/2024 sul meccanismo on line "*Pay or Consent*".

FIVELEX
Studio Legale e Tributario
Via degli Omenoni 2
20121 Milano

Piazzale delle Belle Arti 6
0196 Roma

11 aprile 2024 – **Sentenza della Corte di Giustizia UE nella causa C-741/21 - Responsabilità del titolare del trattamento per danno causato a terzi dal proprio dipendente in violazione delle istruzioni impartite.**

---

7 aprile 2024 – Stati Uniti: presentato al Congresso l'American Privacy Rights Act.

INTELLIGENZA ARTIFICIALE.

24 aprile 2024 – Consiglio dei Ministri: approvato un disegno di legge per l'introduzione di disposizioni e la delega al Governo in materia di Intelligenza Artificiale.

---

19 aprile 20204 - L'Assemblea parlamentare del Consiglio d'Europa adotta il parere sul progetto di convenzione internazionale sull'Intelligenza Artificiale.

INFORMATION TECHNOLOGY

24 aprile 2024 - Il Parlamento europeo adotta la Direttiva sulle condizioni di lavoro dei lavoratori delle piattaforme elettroniche (Direttiva GIG Economy).

---

20 aprile 2024 – Firme digitali: negata la possibilità di sottoscrivere le liste elettorali con firma digitale ad un elettore con disabilità: questione rinviata alla Consulta.

MERCATI DIGITALI.

1° Maggio 2024 – Pubblicato nella Gazzetta Ufficiale dell'Unione Europea del 30 aprile 2024, il Regolamento (UE) 2024/1183 (c.d. Regolamento eIDAS2), che introduce un nuovo quadro per un'identità digitale europea (e-ID) e che a tal fine modifica il Regolamento (UE) n. 910/2014.

---

19 aprile 2024 - Commissione europea: Linee Guida pratiche per spiegare l'applicazione del Regolamento 2854/2023 - Data Act, e i suoi effetti.

REATI INFORMATICI

5 Aprile 2024 - Suprema Corte di Cassazione: frode informatica, il concetto di "identità digitale" trova applicazione anche nei casi di home banking.

TELECOMUNICAZIONI.

28 aprile 2024 - Decreto legislativo correttivo del Codice delle comunicazioni.

FIVELEX
Studio Legale e Tributario

Via degli Omenoni 2
20121 Milano

Piazzale delle Belle Arti 6
0196 Roma

DATA PROTECTION

30 aprile 2024 - Sentenza della Corte di Giustizia UE nella causa C-178/22 - Vita privata e perseguimento di reati gravi: il giudice incaricato di autorizzare l'accesso ai tabulati telefonici per identificare gli autori di un reato, per il cui perseguimento la legge nazionale prevede un tale accesso, deve poter rifiutare o limitare detto accesso.

Secondo la legge italiana, il delitto di furto aggravato fa parte dei reati che giustificano l'acquisizione di tabulati telefonici presso il fornitore di servizi di comunicazione elettronica, previa autorizzazione di un giudice. La Corte di giustizia UE ritiene che un accesso a tali tabulati possa essere concesso soltanto per i dati di persone sospettate di essere implicate in un reato grave, e precisa che spetta agli Stati membri definire i «*reati gravi*». Tuttavia, il giudice incaricato di autorizzare tale accesso deve poter rifiutare o limitare detto accesso qualora constati che l'ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali causata da un tale accesso è grave, mentre risulta manifestamente che il reato in questione non è grave alla luce delle condizioni sociali esistenti nello Stato membro interessato.

---

30 aprile 2024 - Sentenza della Corte di Giustizia UE nella causa C-470/21- Lotta contro i reati e ingerenza nei diritti fondamentali: un'autorità pubblica nazionale incaricata della lotta contro le contraffazioni commesse online può accedere ai dati identificativi a partire da un indirizzo IP.

Gli Stati membri possono imporre ai fornitori di accesso a Internet un obbligo di conservazione generalizzata e indifferenziata degli indirizzi IP per lottare contro i reati in generale, purché tale conservazione non consenta di trarre conclusioni precise sulla vita privata dell'interessato. Ciò implica che si deve vietare agli agenti che dispongono di tale accesso di divulgare informazioni sul contenuto degli archivi consultati, di effettuare un tracciamento del percorso di navigazione a partire dagli indirizzi IP e di utilizzare tali indirizzi IP a fini diversi dall'identificazione dei loro titolari ai fini dell'adozione di eventuali misure. Ciò può essere realizzato mediante modalità di conservazione che garantiscano una separazione effettivamente stagna degli indirizzi IP e delle altre categorie di dati personali, in particolare i dati relativi all'identità civile.

Gli Stati membri possono inoltre, a determinate condizioni, autorizzare l'autorità nazionale competente ad accedere ai dati relativi all'identità civile riferentisi a indirizzi IP. Quando l'accesso a dati relativi all'identità civile degli utenti dei mezzi di comunicazione elettronica ha il solo scopo di identificare l'utente interessato, non è indispensabile un previo controllo di tale accesso da parte di un giudice o di un ente amministrativo indipendente in quanto tale accesso comporta un'ingerenza nei diritti fondamentali che non può essere qualificata come grave. Detto controllo deve tuttavia essere previsto allorché le specificità di una procedura nazionale che disciplina un accesso siffatto possono, per il fatto di mettere in relazione i dati e le informazioni raccolti nel corso delle diverse fasi di tale procedura, consentire di trarre conclusioni precise sulla vita privata dell'interessato e, pertanto, comportare una grave ingerenza nei diritti fondamentali. In un caso del genere, tale controllo da parte di un giudice o di un ente amministrativo indipendente deve avvenire prima che abbia luogo tale messa in relazione, preservando al contempo l'efficacia di detta procedura, consentendo, in particolare, di individuare i casi di nuova possibile reiterazione del comportamento illecito di cui trattasi.

---

26 aprile 2024 – Approvato in via definitiva il Regolamento UE istitutivo dello Spazio europeo dei dati sanitari (EHDS Regulation).

Nella sua ultima sessione di legislatura il Parlamento europeo ha approvato in via definitiva - 445 voti a 142 - il Regolamento UE istitutivo dello Spazio europeo dei dati sanitari (European Health Data Space, EHDS) recependo l'accordo raggiunto con il Consiglio UE.

Lo Spazio europeo dei dati sanitari sarà un pilastro fondamentale dell'Unione europea della Salute ed è il primo spazio comune di dati dell'UE in un settore specifico a emergere dalla strategia europea per i dati. In sostanza è la prima *lex specialis* rispetto al *Data Governance Act* (Regolamento 2022/868 - DGA) che, come *lex generalis* fissa, le regole sulla circolazione intersettoriale di dati in Spazi Europei dei Dati.

L'EHDS consentirà ai cittadini-pazienti di assumere il pieno controllo dei propri dati sanitari, facilitandone lo scambio per la fornitura di assistenza sanitaria in tutta l'UE (il cosiddetto uso primario dei dati che circoleranno mediante una apposita piattaforma elettronica europea). Si promuove anche un vero e proprio mercato unico per i sistemi di cartelle cliniche elettroniche. Si attua inoltre un sistema coerente, affidabile ed efficiente per il riutilizzo dei dati sanitari a fini di ricerca, innovazione, sviluppo di medicina e app personalizzate, addestramento di algoritmi di IA, elaborazione di politiche e attività normative: il cosiddetto uso secondario dei dati, per cui sarà attivata una seconda e apposita piattaforma elettronica.

A questo punto si può affermare che questa Legislatura UE che si va a concludere è stata tra le più rilevanti quanto alla piena realizzazione del quadro normativo UE attuativo della Strategia dei Dati: dopo il GDPR, il DGA, il Data Act e l'EDHS, unitamente al quadro di cybersecurity (NIS 2, DORA, direttiva sulla resilienza dei sistemi critici, GPSR, CRA, TERREG).

---

22 aprile 2024 – Attivo dal 22 aprile al 30 giugno 2024 il servizio per opporsi all'alimentazione automatica del Fascicolo Sanitario Elettronico mediante caricamento dei dati sanitari antecedenti al 19 Maggio 2020.

Per incrementare l'alimentazione del Fascicolo sanitario elettronico - FSE, l'articolo 11 del decreto-legge n.34/2020 ha previsto che, a decorrere dalla data di pubblicazione del decreto (19 maggio 2020), il caricamento dei dati sul FSE avvenga in maniera automatica, con conseguente eliminazione del "consenso all'alimentazione" previsto dalla normativa precedente.

Per i dati e i documenti sanitari generati da eventi clinici antecedenti al 19 maggio 2020 l'assistito può esercitare il diritto di opporsi all'alimentazione del FSE tramite il servizio on line "*FSE - Opposizione al pregresso*" che consente all'assistito di opporsi al caricamento nel proprio FSE dei dati e documenti digitali sanitari generati da eventi clinici riferiti alle prestazioni erogate dal Servizio Sanitario Nazionale antecedenti al 19 maggio 2020. L'opposizione al caricamento di dati e documenti generati da eventi clinici riferiti alle prestazioni erogate dal Servizio Sanitario Nazionale antecedenti al 19 maggio 2020 va effettuata attraverso il portale Sistema Tessera Sanitaria all'indirizzo www.sistemats.it.

Il servizio on line "FSE - Opposizione al pregresso" è disponibile dal 22 aprile fino al 30 giugno 2024.

La scelta può essere revocata e nuovamente registrata nel Sistema Tessera Sanitaria più volte, fino al 30 giugno 2024. Il sistema selezionerà l'ultima indicazione caricata cronologicamente.

FIVELEX
Studio Legale e Tributario

Via degli Omenoni 2
20121 Milano

Piazzale delle Belle Arti 6
0196 Roma

Il mancato accesso al servizio on line "FSE - Opposizione al pregresso" o l'accesso al servizio senza registrare la propria opposizione comporterà il caricamento automatico dei propri dati e i documenti sanitari disponibili e antecedenti al 19 maggio 2020 nel FSE.

---

23 aprile 2024 – Corte costituzionale: le Regioni non possono disciplinare autonomamente la materia del trattamento dei dati personali.

È incostituzionale una disciplina regionale che regola il trattamento dei dati personali nella installazione degli impianti di videosorveglianza, in quanto vìola gli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea e invade le competenze legislative esclusive dello Stato nella materia «ordinamento civile». È quanto si legge nella sentenza n. 69/2024 con cui la Corte costituzionale ha dichiarato costituzionalmente illegittimo l'articolo 3 della legge della Regione Puglia n. 13 del 2023 per contrasto con l'art. 117, commi primo e secondo, della Costituzione. La Corte rileva che l'Unione europea, nell'esercizio della competenza fissata nell'art. 16 del Trattato sul funzionamento dell'Unione europea, detta una complessa disciplina in materia di trattamento dei dati personali, che «*trova completamento e integrazione nelle fonti nazionali*». Secondo i giudici delle leggi, la Regione non può regolare autonomamente la materia, né operare una selezione di fonti e di previsioni, «*che, all'interno dell'articolato plesso normativo contemplato sia dall'Unione europea sia dal legislatore statale, sono chiamate a disciplinare questa complessa e delicata materia*», poiché in tal modo «*non solo si sovrappone alle normative eurounitaria e statale, travalicando le proprie competenze, ma oltretutto effettua una arbitraria scelta, il cui contenuto precettivo equivale a ritenere vincolanti le sole regole individuate dal legislatore regionale e non anche le altre*», dettate dall'Unione europea e dal legislatore statale.

---

18 aprile 2024 - Il Comitato europeo per la protezione dei dati personali - EDPB stabilisce le priorità per il periodo 2024-2027 e chiarisce i meccanismi di ricorso del DPF.

Durante la sua ultima plenaria, l'EDPB ha adottato la sua **Strategia per il periodo 2024-2027.** La strategia definisce le priorità del Comitato europeo per la protezione dei dati, raggruppate attorno a quattro pilastri, nonché le azioni chiave per pilastro per contribuire al conseguimento di tali obiettivi. Questi quattro pilastri sono:

Pilastro 1 – Rafforzare l'armonizzazione e promuovere la conformità

Pilastro 2 – Rafforzare una cultura comune dell'applicazione delle norme e una cooperazione efficace

Pilastro 3 – Salvaguardare la protezione dei dati nel panorama digitale e transnormativo in via di sviluppo

Pilastro 4 – Contribuire al dialogo globale sulla protezione dei dati

Nei prossimi quattro anni, l'EDPB continuerà a promuovere il rispetto della legge sulla protezione dei dati elaborando orientamenti chiari, concisi e pratici su temi importanti e sviluppando materiali per un pubblico più ampio. Inoltre, la cooperazione in materia di applicazione delle norme rimarrà una priorità importante per il Comitato europeo per la protezione dei dati. Il comitato continuerà a basarsi sulla visione delineata nella sua cosiddetta dichiarazione di Vienna e svilupperà ulteriormente le iniziative del Comitato europeo per la protezione dei dati in questo settore, come le azioni di esecuzione coordinate.

Un nuovo aspetto della strategia è l'attenzione all'interazione con il nuovo quadro normativo digitale. Le nuove leggi digitali, come il DMA o il DSA, hanno un impatto

sulla protezione dei dati e sulla privacy. L'EDPB si adopererà per rafforzare la cooperazione con altre autorità di regolamentazione, al fine di integrare il diritto alla protezione dei dati nell'architettura normativa generale. Inoltre, l'EDPB continuerà a prestare particolare attenzione alle sfide poste dalle nuove tecnologie, come l'IA.

La strategia sarà integrata da due programmi di lavoro, che conterranno dettagli sulla sua attuazione.

Inoltre, per quanto riguarda il quadro UE-USA per la riservatezza dei dati, l'EDPB ha adottato un regolamento interno, una nota informativa al pubblico e modelli di moduli di reclamo per facilitare l'attuazione dei meccanismi di ricorso previsti dal DPF.

I documenti del Comitato europeo per la protezione dei dati si riferiscono a due meccanismi di ricorso del DPF creati per gestire le denunce presentate da cittadini dell'UE. I meccanismi di ricorso riguardano solo i reclami riguardanti la rispettiva competenza - sicurezza nazionale o scopi commerciali - e solo per i dati trasmessi dopo il 10 luglio 2023.

---

17 aprile 2024 – Comitato europeo per la protezione dei dati personali: Opinion 8/2024 sul meccanismo on line "*Pay or Consent*".

Con la *Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms*, il Comitato europeo per la protezione dei dati personali si è finalmente espresso sulla validità dei meccanismi "*pay or consent*".

In linea di principio l'EDPB non vieta né ritiene illecito il meccanismo, ma lo sottopone a prevedibili quanto stringenti requisiti di conformità, che possono essere riassunti di seguito:

(1) l'offerta di (solo) un'alternativa a pagamento al servizio che include il trattamento a fini di pubblicità comportamentale non è ammessa;

(2) dovrebbe essere offerta anche una ulteriore alternativa non a pagamento (come anche previsto nei Principi sui Cookies della Commissione UE), senza pubblicità comportamentale, ad esempio con una forma di pubblicità che comporti il trattamento di una quantità minore (o nulla) di dati personali.;

(3) qualsiasi tariffa imposta non può essere tale da inibire effettivamente gli interessati dal compiere una libera scelta o da determinare pregiudizio, come quando gli interessati non consenzienti non pagano un corrispettivo e rischiano quindi di essere esclusi da servizi importanti o decisivi per la partecipazione alla vita sociale;

(4) i titolari del trattamento devono valutare, caso per caso, una serie di fattori, quali: se esiste uno squilibrio di potere con l'interessato; la posizione della grande piattaforma online nel mercato; l'esistenza di effetti di lock-in o di rete; la misura in cui l'interessato fa affidamento sul servizio; il pubblico principale del servizio; se il consenso è richiesto per accedere a beni o servizi, se il trattamento non sia necessario per l'adempimento del contratto;

(5) i titolari del trattamento devono valutare una versione alternativa del servizio offerto che non implica il consenso al trattamento dei dati personali a fini di pubblicità comportamentale;

(6) quando viene presentato un modello "consenso o pagamento", l'interessato deve essere libero di scegliere quale finalità di trattamento accettare (il consenso deve essere specifico e granulare), piuttosto che trovarsi di fronte a una richiesta di consenso che raggruppa diverse finalità. Il consenso va inoltre riconfermato ad intervalli di tempo.

11 aprile 2024 – **Sentenza della Corte di Giustizia UE nella causa C-741/21 - Responsabilità del titolare del trattamento per danno causato a terzi dal proprio dipendente in violazione delle istruzioni impartite.**

La Corte di Giustizia UE ha fornito le corrette interpretazioni degli articoli 82, 83 e 29 del GDPR nel caso di avvocato tedesco che aveva lamentato presso una società la continua ricezione di comunicazioni a scopi marketing anche a seguito della avvenuta revoca dei consensi. L'interessato ha dunque avviato una causa di risarcimento del danno da trattamento dei dati personali nella quale la società ha sostenuto che la violazione era imputabile a un dipendente che aveva violato il rigoroso sistema di tutela implementato dalla società per evitare le chiamate indesiderate e le istruzioni sul trattamento impartite ai sensi dell'articolo 29 del GDPR. Investita dal giudice nazionale tedesco, che ha richiesto la interpretazione dell'articolo 82 del GDPR in tema di esonero della responsabilità del titolare del trattamento, la CGUE sul punto ha risposto che l'articolo 82 del GDPR deve essere interpretato nel senso che non può essere sufficiente che il titolare del trattamento, per essere esonerato dalla sua responsabilità ai sensi del paragrafo 3 di detto articolo (che recita: "*Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile*»), faccia valere che il danno di cui trattasi è stato causato dall'errore di una persona che agisce sotto la sua autorità, a norma dell'articolo 29 di tale regolamento. Se così fosse, il danneggiato dovrebbe agire nei confronti diretti dell'autore della violazione, depotenziando il suo diritto al risarcimento del danno. La Corte precisa che le circostanze dell'esonero da responsabilità di cui all'articolo 82, paragrafo 3, del RGPD devono essere strettamente limitate a quelle in cui il titolare del trattamento è in grado di dimostrare, da parte sua, la mancanza di imputabilità del danno. Pertanto, in caso di violazione di dati personali commessa da una persona che agisce sotto la sua autorità, detto titolare può beneficiare di tale esonero unicamente se prova che non sussiste alcun nesso di causalità tra l'eventuale violazione dell'obbligo di protezione dei dati e il danno subito dall'interessato (in altri termini: la violazione da parte del dipendente deve essere finalizzata al perseguimento di scopi suoi propri ed estranei alle mansioni e alle istruzioni cui egli è tenuto).

La Corte UE enuncia anche ulteriori e importanti principi in tema di risarcimento del danno da trattamento, tra i quali i seguenti: (1) una violazione di disposizioni del GDPR che conferiscono diritti alla persona interessata non è di per sé sufficiente a costituire un «danno immateriale», indipendentemente dal grado di gravità del danno subito da tale persona e dalla prova di tale danno; (2) per determinare l'importo dovuto a titolo di risarcimento di un danno fondato sull'articolo 82 del GDPR, da un lato, non si devono applicare *mutatis mutandis* i criteri di fissazione dell'importo delle sanzioni amministrative pecuniarie previsti dall'articolo 83 del GDPR e, dall'altro, non si deve tener conto – come aggravante che invece si applica all'applicazione delle sanzioni amministrative - del fatto che più violazioni del GDPR riconducibili ad una stessa operazione di trattamento riguardino la persona che richiede il risarcimento.

7 aprile 2024 – Stati Uniti: presentato al Congresso l'American Privacy Rights Act.

Dopo la mancata approvazione dell'American Data Privacy & Protection Act – DPPA nel 2022, gli Stati Uniti provano nuovamente la strada di una legge federale sulla protezione dei dati. Il 7 aprile 2024 è stato introdotto al Congresso l'*American Privacy Rights Act - APRA*, un progetto di legge bipartisan e bicamerale finalizzato a introdurre in USA uno standard nazionale per la protezione dei dati personali. Rispetto al testo precedente non vi sono grandi novità: l'approccio del Legislatore USA è ben diverso dal rigoroso regime di tutele del GDPR europeo; il concetto di

"*covered data*" tutelato esclude importanti categorie di interessati (es: i lavoratori); le tutele rispetto ad attività marketing (es: pubblicità mirata) e profilazione sono basate su meccanismi di opt-out; prevale una prospettiva commerciale, quella delle tematiche di protezione dei dati inserite nell'ambito dei rapporti con i consumatori (ne è esempio il meccanismo del *"do-not-sell*" con il quale l'interessato può opporsi anticipatamente alla vendita dei suoi dati). Certamente apprezzabili sono i principi di diretta derivazione dal GDPR: dagli obblighi di trasparenza al principio di minimizzazione; dal catalogo dei diritti per gli interessati fino alle norme su sicurezza e data breach. Tuttavia, divergono parecchio le scelte regolatorie del Legislatore USA rispetto a quello UE. Come anche già previsto nel precedente disegno di legge ADPPA, interessante la riproposizione della sezione sui trattamenti basati sugli algoritmi, con regole molto simili a quelle dell'AI Act europeo.

INTELLIGENZA ARTIFICIALE.

24 aprile 2024 – Consiglio dei Ministri: approvato un disegno di legge per l'introduzione di disposizioni e la delega al Governo in materia di Intelligenza Artificiale.

Il Consiglio dei ministri ha approvato, con la previsione della richiesta alle Camere di sollecita calendarizzazione nel rispetto dei regolamenti dei due rami del Parlamento, un disegno di legge per l'introduzione di disposizioni e la delega al Governo in materia di intelligenza artificiale.

Il disegno di introduce norme di principio e disposizioni di settore che nelle intenzioni del Legislatore non si sovrappongono al Regolamento europeo sull'intelligenza artificiale approvato lo scorso 13 marzo dal Parlamento Europeo, di prossima emanazione, ma ne accompagnano il quadro regolatorio in settori di diritto interno. Le norme intervengono infatti in cinque ambiti: la strategia nazionale, le autorità nazionali, le azioni di promozione, la tutela del diritto di autore, le sanzioni penali. Si prevede, inoltre, una delega al governo per adeguare l'ordinamento nazionale al Regolamento UE in materie come l'alfabetizzazione dei cittadini in materia di IA (sia nei percorsi scolastici che in quelli universitari) e la formazione da parte degli ordini professionali per professionisti e operatori. La delega riguarda anche il riordino in materia penale per adeguare reati e sanzioni all'uso illecito dei sistemi di IA.

---

19 aprile 20204 - L'Assemblea parlamentare del Consiglio d'Europa adotta il parere sul progetto di convenzione internazionale sull'Intelligenza Artificiale.

L'Assemblea parlamentare del Consiglio d'Europa (CoE) ha pubblicato il suo parere 303 (2024) sul *Framework on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law by the Committee on Artificial Intelligence.*

L'Assemblea deve esprimere il proprio parere sul progetto di quadro prima che sia adottato dal Comitato dei Ministri, dopodiché può essere firmato e ratificato.

In particolare, l'Assemblea ha previsto che gli Stati membri del Consiglio d'Europa, al momento della ratifica del progetto di quadro, dovrebbero scegliere di applicarne pienamente le disposizioni alle attività degli attori privati. In particolare, l'Assemblea ha stabilito che il progetto di quadro non affronta i rischi e gli impatti derivanti dall'uso dell'intelligenza artificiale (IA) da parte di attori privati e che un approccio differenziato per il settore privato crea una scappatoia significativa.

Inoltre, l'Assemblea ha proposto modifiche alle disposizioni in materia di sicurezza nazionale, proponendo che le attività di IA necessarie per proteggere la sicurezza

nazionale siano possibili solo se le attività sono in linea con il diritto internazionale in materia di diritti umani. L'Assemblea ha inoltre proposto che gli Stati membri istituiscano meccanismi per vietare o limitare determinati usi dei sistemi di IA qualora tali casi d'uso siano considerati incompatibili con il rispetto dei diritti umani, il funzionamento della democrazia e lo Stato di diritto.

Ulteriori proposte dell'Assemblea includono l'aggiunta di misure adeguate per garantire la protezione degli informatori in relazione alle attività nell'ambito dei sistemi del ciclo di vita dell'IA.

INFORMATION TECHNOLOGY

24 aprile 2024 - Il Parlamento europeo adotta la Direttiva sulle condizioni di lavoro dei lavoratori delle piattaforme elettroniche (Direttiva GIG Economy).

Il Parlamento europeo ha approvato definitivamente le nuove norme volte a migliorare le condizioni di lavoro dei lavoratori delle piattaforme elettroniche. Le nuove norme, concordate dal Parlamento e dal Consiglio dell'UE a febbraio e adottate con 554 voti a favore, 56 contrari e 24 astensioni, mirano a garantire che i lavoratori delle piattaforme elettroniche abbiano il loro status occupazionale classificato correttamente e a combattere scenari di falso lavoro autonomo. Inoltre, per la prima volta nell'UE, si regolamenta l'uso degli algoritmi sul posto di lavoro.

La nuova legge introduce una presunzione di rapporto di lavoro subordinato (in contrapposizione al lavoro autonomo) che scatta in presenza di fattori che indicano controllo e direzione, in base alla legge nazionale e ai contratti collettivi, e tenendo conto della giurisprudenza dell'UE.

La direttiva obbliga i Paesi dell'UE a stabilire una presunzione legale di lavoro subordinato a livello nazionale, con l'obiettivo di correggere lo squilibrio di potere tra la piattaforma di lavoro digitale e la persona che svolge il lavoro sulla piattaforma. L'onere della prova spetta alla piattaforma, il che significa che spetta a quest'ultima dimostrare l'assenza di un rapporto di lavoro.

Sono previste anche nuove regole sulla gestione algoritmica. Le nuove norme assicurano che una persona che svolge il lavoro su piattaforma non possa essere licenziata o allontanata sulla base di una decisione presa da un algoritmo o da un sistema decisionale automatizzato. Le piattaforme di lavoro digitale devono invece garantire una supervisione umana sulle decisioni importanti che riguardano direttamente le persone che svolgono il lavoro sulla piattaforma.

I diritti di trasparenza e di protezione dei dati sono ulteriormente rafforzati. La direttiva introduce norme che proteggono in modo più solido i dati dei lavoratori delle piattaforme. Alle piattaforme di lavoro digitale sarà vietato trattare alcuni tipi di dati personali, come quelli sullo stato emotivo o psicologico di una persona e sulle sue convinzioni personali.

Il testo concordato dovrà ora essere adottato formalmente anche dal Consiglio. Dopo la pubblicazione nella Gazzetta ufficiale dell'UE, gli Stati membri avranno due anni di tempo per incorporare le disposizioni della direttiva nella loro legislazione nazionale.

20 aprile 2024 – Firme digitali: negata la possibilità di sottoscrivere le liste elettorali con firma digitale ad un elettore con disabilità: questione rinviata alla Consulta.

Il Tribunale di Civitavecchia solleva questione di legittimità costituzionale in merito alla preclusione, per le persone con disabilità impossibilitate a firmare, di sottoscrivere una lista di candidati per la presentazione alle elezioni regionali ex art. 9 L. n. 108/1968 con firma digitale.

Un cittadino italiano con disabilità intendeva esercitare il proprio diritto di sottoscrizione delle liste elettorali per l'elezione del Consiglio regionale, in base all'art. 9 della Legge 17 febbraio 1968, n. 108. Egli, impossibilitato ad apporre una firma autografa per le sue condizioni di salute, si era dotato di una firma digitale in grado di usare autonomamente.

Il gruppo politico al quale questi si rivolgeva gli rappresentava che l'art. 9 delle L. n. 108/1968, secondo l'interpretazione adottata dai competenti Uffici elettorali, escludeva la possibilità di apporre le firme in formato digitale e che tale preclusione derivava anche dall'art. 2, comma 6, del Decreto Legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale).

Il cittadino si rivolgeva, quindi, alla Regione Lazio, invitandola formalmente a dichiarare espressamente la possibilità di apporre la sottoscrizione prevista dall'art. 9, L. n. 108/1968 con firma digitale.

La richiesta presentata dal cittadino rimaneva priva di riscontro, mentre la medesima richiesta – presentata da parte di un'Associazione – trovava la conferma, da parte della Regione, dell'impossibilità di raccogliere la sottoscrizione attraverso firma digitale.

Il cittadino, dunque, si rivolgeva al Tribunale di Civitavecchia chiedendo di «accertare e dichiarare il diritto del ricorrente di sottoscrivere una lista di candidati per la presentazione alle elezioni regionali, ai sensi dell'art. 9, L. n. 108/1968, con la propria firma digitale» e, in via subordinata, «accogliere le conclusioni che precedono […] previa sospensione del giudizio e rimessione alla Corte costituzionale della questione pregiudiziale di legittimità costituzionale, ritenuta rilevante e non manifestamente infondata, dell'art. 9, della L. n. 108/1968 e dell'art. 2, comma 6, del D.Lgs. 82/2005, per violazione degli artt. 2, 3, 48,49 della Costituzione».

MERCATI DIGITALI.

1° Maggio 2024 – Pubblicato nella Gazzetta Ufficiale dell'Unione Europea del 30 aprile 2024, il Regolamento (UE) 2024/1183 (c.d. Regolamento eIDAS2), che introduce un nuovo quadro per un'identità digitale europea (e-ID) e che a tal fine modifica il Regolamento (UE) n. 910/2014.

A 3 anni dalla sua proposta iniziale nel giugno 2021, il Regolamento europeo noto come eIDAS 2.0 è stato pubblicato nella Gazzetta ufficiale dell'Unione europea (Regolamento UE 2024/1183) e segna un'evoluzione significativa nel quadro digitale dell'UE. Entrerà in vigore il 20 maggio 2024, ma sarà applicabile – a seconda dei casi – a maggio 2026 o a maggio 2027.

I punti salienti del Regolamento (che integra e aggiorna il precedente regolamento 910/2014) sono:

l'introduzione del portafoglio comune di identità digitale dell'UE (EUDIW), che sarà rilasciato gratuitamente (i componenti software per le applicazioni dei portafogli saranno open source) e consentirà ai cittadini dell'UE (sulla base di una scelta

volontaria e senza discriminazioni nel caso si scelga di non aderire) di archiviare e gestire in modo sicuro i propri dati e documenti ufficiali (come carte d'identità, patenti di guida, diplomi, coordinate bancarie, carte di viaggio, ecc.) e di facilitare le interazioni online con le autorità, le imprese e i cittadini in tutti gli Stati membri dell'UE;

- si introducono una maggiore interoperabilità dei sistemi di identificazione digitale tra gli Stati membri e misure di sicurezza più rigorose, con l'introduzione di metodi di autenticazione più rigorosi e di standard di sicurezza rafforzati per aumentare la fiducia nelle transazioni digitali e a promuovere un mercato digitale più sicuro nell'UE;

- si introducono nuovi servizi fiduciari come l'attestazione elettronica degli attributi, l'archiviazione elettronica o la registrazione dei registri elettronici. La Commissione stabilirà un elenco di norme da utilizzare entro la fine del 2024;

- viene precisato l'ambito di applicazione dei certificati qualificati di autenticazione di siti web, per consentire agli utenti di verificare in modo certificato chi amministra sirti web e piattaforme (tali certificati erano già previsti del Regolamento eIDAS del 2014).

---

19 aprile 2024 - Commissione europea: Linee Guida pratiche per spiegare l'applicazione del Regolamento 2854/2023 - Data Act, e i suoi effetti.

Il Regolamento UE 2854/2023 (Data Act) è entrato ufficialmente in vigore l'11 gennaio 2024. Introduce regole armonizzate sull'accesso e l'uso equo dei dati, in particolare per quanto riguarda i dispositivi connessi. Diventerà operativo il 12 settembre 2025.

La Commissione europea ha pubblicato un set di Linee guida pratiche sul funzionamento, la portata e gli effetti applicativi del Data Act, con particolare riferimento ai seguenti otto scenari: (1) condivisione dei dati tra imprese e consumatori nel contesto dell'IoT; (2) condivisione dei dati tra imprese; (3) clausole contrattuali abusive; (4) condivisione dei dati tra imprese e pubblica amministrazione; (5) passaggio da un fornitore di servizi cloud ad un altro; (6) accesso illegale ai dati da parte di governi di Paesi terzi; (7) interoperabilità; e (8) applicazione.

Come ulteriore sviluppo, la Commissione UE ha anticipato una serie di clausole contrattuali modello per aiutare le imprese a concludere contratti di condivisione dei dati che siano equi, ragionevoli e non discriminatori. Questi termini forniranno anche indicazioni su un compenso ragionevole e sulla protezione dei segreti commerciali.

Per quanto riguarda il cloud, la Commissione UE adotterà e renderà pubbliche anche una serie di clausole contrattuali standard non vincolanti per i contratti di cloud computing tra utenti e fornitori di servizi cloud. A tale scopo, è già stato istituito un gruppo di esperti per supportare la Commissione nella redazione di tali termini e clausole entro l'autunno del 2025.

REATI INFORMATICI

5 Aprile 2024 - Suprema Corte di Cassazione: frode informatica, il concetto di "identità digitale" trova applicazione anche nei casi di home banking.

La nozione di identità digitale, che integra l'aggravante ex art. 640-ter, comma terzo, c.p., non presuppone una procedura di validazione adottata dalla PA, ma trova applicazione anche nei casi di utilizzo di credenziali di accesso a sistemi informatici privati.

L'imputato veniva condannato dal Tribunale in ordine al reato di riciclaggio, per aver messo a disposizione di ignoti il proprio conto corrente ove era confluito denaro proveniente dai delitti di accesso abusivo ad un sistema informatico e frode informatica. La Corte d'Appello, parzialmente riformando la sentenza di primo grado, qualificava il fatto ai sensi dell' art. 640-ter c.p. e rideterminava la pena in senso favorevole all'uomo.

L'imputato ricorre così in Cassazione, lamentando violazione di legge e vizio di motivazione in ordine alla ritenuta sussistenza dell'aggravante ex comma 3, art. 640-ter cit.. Evidenzia egli che le risultanze processuali non proverebbero la sussistenza del furto o dell'indebito utilizzo dell'identità digitale, concetto non adattabile al caso in esame, nel quale, per accedere al conto corrente della vittima, ci si era serviti di una chiavetta elettronica idonea a comunicare il codice di accesso da utilizzare di volta in volta.

Con sentenza n. 13559 del 3 aprile, la Seconda sezione Penale rigetta il ricorso.

La nozione di identità digitale, che integra l'aggravante in questione, non è circostanziata alle procedure di validazione adottate dalla PA, ma trova applicazione anche nel caso di utilizzo di credenziali di accesso a sistemi informatici gestiti da privati.

Il Legislatore non ha infatti fornito alcuna definizione di identità digitale.

La dottrina ha evidenziato che la traslazione in sede penale di definizioni tratte da fonti esterne trova un evidente ostacolo nel fatto che si tratta di concettualizzazioni o indicazioni metodologiche funzionali agli specifici provvedimenti cui ineriscono.

L'Ufficio del Massimario ha affermato che «l'identità digitale è comunemente intesa come l'insieme delle informazioni e delle risorse concesse da un sistema informatico ad un particolare utilizzatore del suddetto sotto un processo di identificazione (..)».

Sebbene si tratti, quindi, di un concetto destinato ad una futura perimetrazione, non può essere accolta la tesi difensiva che pretende di limitare l'identità digitale alle sole procedure di validazione adottate dalla PA debitamente certificate, escludendo le procedure di accesso mediante credenziali a sistemi informatici a gestione privatistica quale i servizi di home banking o le piattaforme di vendita online.

E tali indicazioni, espresse a proposito dell'utilizzo di credenziali personali per l'accesso a sistemi cosiddetti di home banking o simili, possono essere applicati anche all'uso illegittimo dei cosiddetti PIN e di chiavette elettroniche che producono di volta in volta un codice per effettuare l'operazione bancaria, dal momento che, in tutti i casi, quel che rileva è che «i dati di accesso al sistema informatico di volta in volta compulsato dall'agente direttamente o attraverso l'uso di dispositivi elettronici, individuino in modo esclusivo ed univoco una determinata persona attraverso numeri o lettere secondo una sequenza unica destinata ad essere utilizzata (..) solo dal titolare o da soggetto da questi autorizzato».

FIVELEX
Studio Legale e Tributario

Via degli Omenoni 2
20121 Milano

Piazzale delle Belle Arti 6
0196 Roma

Venendo al caso di specie, si può confermare che l'aver utilizzato, carpendola senza autorizzazione, la chiavetta elettronica appartenente al titolare del conto, integra l'aggravante contestata e presuppone, comunque, a monte, un uso non autorizzato delle credenziali di accesso al conto inerenti alla persona del suo titolare.

TELECOMUNICAZIONI.

28 aprile 2024 - Decreto legislativo correttivo del Codice delle comunicazioni. Il 28 aprile 2024 è entrato in vigore il decreto legislativo 48/2024 correttivo del Codice delle Comunicazioni Elettroniche (d.lgs. 259/03). L'intervento correttivo (8 articoli e 2 allegati) mira ad aggiornare il testo alla innovazione tecnologica (anche con l'introduzione di nuove definizioni, come quella di "access point" o "MAC Address") e ad uniformare e semplificare la disciplina in vari ambiti (dalla procedura di SCIA, alla mappatura delle infrastrutture di comunicazione elettronica fino alle procedure di installazione di impianti). Interessanti le modifiche apportate all'articolo 98-*decies* del Codice, con la previsione della possibilità per AGCOM di imporre limitazioni per bloccare comunicazioni provenienti dall'estero che illegittimamente usano numerazione nazionale per identificarne l'origine, come i call center, o per bloccare siti che forniscono APP, sistemi software o servizi illegittimi, ad esempio cashfor sms (remunerazione illegittima degli utenti finali di altri operatori), creazione di reti parallele (dark web) che possono anche essere utilizzare per attività illecite (violazione dei diritti d'autore, violazione della privacy, pedopornografia, furto d'identità).