FIVERS

Aggiornamento
Data protection, AI, IT e IP

n. 5 / 2024

DATA PROTECTION

1° Luglio 2024 – Corte di Giustizia UE: in caso di furto di dati personali (anche non utilizzati illecitamente) devono risarcire il danno anche i soggetti – privati o pubblici – detentori dei dati.

---

27 Giugno 2024 – Garante privacy: al via procedimenti nei confronti di 18 Regioni e 2 Province autonome per azioni correttive in materia di Fascicolo Sanitario Elettronico – FSE 2.0.

---

20 Giugno 2024 – Corte di Giustizia UE: la condanna al risarcimento del danno da trattamento ai sensi dell'articolo 82 del GDPR non deve necessariamente essere aggravata per contestuale violazione di altre normative (come quelle sull'ordinamento professionale), pur restando libero il giudice di decidere discrezionalmente caso per caso.

INTELLIGENZA ARTIFICIALE.

25 Giugno 2024 - L'ESMA fornisce orientamenti alle imprese che utilizzano l'intelligenza artificiale nei servizi di investimento.

---

21 giugno 2024 - La Commissione europea ospita la prima riunione di alto livello per il prossimo Consiglio dell'UE sull'IA, per impostare l'attuazione dell'AI Act.

---

20 Giugno 2024 – Commissione UE: Avviata una consultazione pubblica mirata sull'Intelligenza Artificiale nel settore finanziario.

MERCATI DIGITALI.

3 Luglio 2024 – Per la Commissione UE il modello "Pay or consent" adottato da Meta vìola il Digital Markets Act.

---

24 Giugno 2024 – Commissione UE contro Apple, App Store viola il Digital Markets Act (Regolamento UE 2022/1925).

---

18 Giugno 2024 – Commissione UE: pubblicato il rapporto sullo stato di attuazione negli Stati Membri della Direttiva 2019/2161 sulla modernizzazione e il rafforzamento della protezione dei consumatori on line.

INFORMATION TECHNOLOGY

2 Luglio 2024 – Corte Suprema di Cassazione: i messaggi WhatsApp costituiscono corrispondenza anche se già letti e conservati dal destinatario e ad essi si applica la disciplina del sequestro di corrispondenza.

---

25 Giugno 2024 – Sezioni Unite della Cassazione: principi chiarificatori in materia di acquisizione come prova attraverso un ordine europeo di indagine presso un'autorità giudiziaria straniera di dati tratti da criptofonini.

CYBERSECURITY

3 Luglio 2024 – Pubblicata nella Gazzetta Ufficiale la legge 90/2024 sulla cybersicurezza nazionale.

---

3 Luglio 2024 – Adottato dall'Agenzia Nazionale per la Cybersicurezza il Regolamento Unico per il Cloud delle PA e la qualificazione dei software e dei servizi: il nuovo regime è in vigore dal 1° agosto 2024.

---

27 Giugno 2024 – Pubblicati nella Gazzetta Ufficiale della UE i Regolamenti delegati della Commissione UE attuativi di alcuni obblighi del Regolamento DORA.

REATI INFORMATICI

21 Giugno 2024 – *Revenge porn*: la diffusione del materiale deve essere realizzata solo da chi ha fatto le riprese o se ne è indebitamente impossessato.

DATA PROTECTION

1° Luglio 2024 – Corte di Giustizia UE: in caso di furto di dati personali (anche non utilizzati illecitamente) devono risarcire il danno anche i soggetti – privati o pubblici – detentori dei dati.

La Scalable Capital, una società di diritto tedesco, gestisce una «trading app» nella quale i ricorrenti avevano aperto un conto. A tal fine, questi ultimi hanno salvato alcuni dati personali sui loro rispettivi conti, in particolare il loro nome, la loro data di nascita, il loro indirizzo postale, il loro indirizzo di posta elettronica nonché una copia digitale della loro carta d'identità, versando poi un importo necessario all'apertura di tali conti di diverse migliaia di euro.

I dati personali nonché i dati relativi al portafoglio di titoli dei ricorrenti sono stati poi oggetto di furto da parte di terzi la cui identità è rimasta sconosciuta. Inoltre, non è stato accertato se i suddetti dati personali siano stati oggetto o meno di un uso fraudolento.

In tale contesto, i ricorrenti hanno adito l'Amtsgericht München (Tribunale circoscrizionale, Monaco di Baviera, Germania), giudice del rinvio, con un ricorso volto ad ottenere il risarcimento del danno immateriale che essi affermano di aver subito a causa del furto dei loro dati personali.

La Corte di Giustizia UE ha fornito nuovi criteri interpretativi e applicativi dell'articolo 82 del GDPR sul risarcimento del danno, confermando in priamo luogo che il diritto al risarcimento previsto da tale disposizione svolge una funzione esclusivamente compensativa e il risarcimento pecuniario fondato su detta disposizione deve consentire di compensare integralmente il danno subito.

La Corte chiarisce anche che per configurarsi e far sorgere il diritto al risarcimento del danno immateriale ai sensi dell'art. 82 del GDPR, la nozione di «furto d'identità» implica che l'identità di una persona interessata dal furto di dati personali sia effettivamente usurpata da un terzo. Tuttavia, il risarcimento di un danno immateriale causato dal furto di dati personali non può essere limitato ai casi in cui è dimostrato che un siffatto furto di dati ha successivamente dato luogo a un furto o a un'usurpazione d'identità. Sono dunque risarcibili anche i furti di dati non ancora usati per sostituirsi effettivamente all'interessato.

Sulla base dei principi forniti dalla Corte UE, inoltre, sono tenuti a risarcire il danno non solo gli autori del furto dei dati, ma anche i soggetti privati pubblici che hanno subito la violazione dei dati e l'esfiltrazione e tale ampliamento soggettivo della platea dei soggetti tenuti implica forti impatti finanziari. Se è vero, infatti, che la Corte ricorda che la condanna al risarcimento non deve assumere carattere punitivo o esemplare, è altrettanto vero che nell'ambito della determinazione dell'importo dovuto a titolo di risarcimento di un danno immateriale il danno causato da una violazione di dati personali non è, per sua natura, meno grave di una lesione personale.

---

27 Giugno 2024 – Garante privacy: al via procedimenti nei confronti di 18 Regioni e 2 Province autonome per azioni correttive in materia di Fascilo Sanitario Elettronico – FSE 2.0.

È urgente intervenire per tutelare i diritti di tutti gli assistiti italiani coinvolti nel trattamento dei dati sulla salute effettuato attraverso il Fascicolo Sanitario Elettronico 2.0.

Con questa motivazione il Garante Privacy ha notificato a 18 Regioni e alle Province autonome di Bolzano e Trento l'avvio di procedimenti correttivi e sanzionatori per le numerose violazioni riscontrate nell'attuazione della nuova disciplina sul FSE 2.0, introdotta con il decreto del Ministero della salute del 7 settembre 2023.

Nei giorni precedenti la grave situazione e l'urgenza di interventi correttivi era stata segnalata al Presidente del Consiglio dei Ministri e al Ministro della salute.

Gli esiti dell'attività istruttoria sul FSE, avviata alla fine di gennaio, hanno mostrato che 18 Regioni e le due Province autonome del Trentino Alto Adige - non essendo in linea con quanto contenuto nel decreto del 7 settembre 2023 - hanno modificato, anche significativamente, il modello di informativa predisposto dal Ministero, previo parere del Garante, che avrebbe dovuto essere adottato su tutto il territorio nazionale.

Le difformità riscontrate hanno reso evidente che alcuni diritti (es. oscuramento, delega, consenso specifico) e misure (es. misure di sicurezza, livelli di accesso differenziati, qualità dei dati) introdotte dal decreto, proprio a tutela dei pazienti, non sono garantite in modo uniforme in tutto il Paese. Oppure sono esercitabili ed esigibili solo dagli assistiti di talune Regioni e Province autonome, con un potenziale e significativo effetto discriminatorio sugli assistiti.

Tale disomogeneità contraddice inoltre lo spirito della riforma del FSE 2.0 volta a introdurre misure, garanzie e responsabilità omogenee sul tutto il territorio nazionale, rischiando così di compromettere anche la funzionalità, l'interoperabilità e l'efficienza del sistema FSE 2.0.

Le violazioni nelle quali sono incorse Regioni e Province autonome, con diversi livelli di gravità e responsabilità, possono comportare l'applicazione delle sanzioni previste dal Regolamento europeo.

---

20 Giugno 2024 – Corte di Giustizia UE: la condanna al risarcimento del danno da trattamento ai sensi dell'articolo 82 del GDPR non deve necessariamente essere aggravata per contestuale violazione di altre normative (come quelle sull'ordinamento professionale), pur restando libero il giudice di decidere discrezionalmente caso per caso.

La vicenda ha riguardato alcuni contribuenti tedeschi che si erano rivolti a un commercialista per la dichiarazione dei redditi. Questi aveva trasmesso il plico cartaceo via posta, ma a un indirizzo sbagliato, determinandosi una situazione per cui terzi non legittimati avevano avuto accesso ai dati fiscali dei contribuenti che avevano poi fatto causa per danni al commercialista.

Ai vari quesiti posti dal giudice del rinvio, la Corte di Giustizia UE ha risposto quanto segue.

In primo luogo, una violazione del GDPR non è sufficiente, di per sé, a fondare un diritto al risarcimento ai sensi dell'articolo 82. L'interessato deve altresì dimostrare l'esistenza di un danno causato da tale violazione, senza tuttavia che detto danno debba raggiungere un certo grado di gravità.

In secondo luogo, La Corte chiarisce che il il timore nutrito da una persona che i suoi dati personali, a causa di una violazione del GDPR, siano stati divulgati a terzi, senza che si possa dimostrare che ciò sia effettivamente avvenuto, è sufficiente a dare fondamento a un diritto al risarcimento purché tale timore, con le sue conseguenze negative, sia debitamente provato.

Infine, per determinare l'importo dovuto a titolo di risarcimento di un danno fondato sull'articolo 82 del GDPR:

- non si devono applicare *mutatis mutandis* i criteri di fissazione dell'importo delle sanzioni amministrative pecuniarie previsti all'articolo 83 del GDPR;
- non si deve conferire a tale diritto al risarcimento una funzione dissuasiva;
- non occorre tenere conto di violazioni simultanee di disposizioni nazionali relative alla protezione dei dati personali, ma che non hanno come oggetto quello di precisare le norme del GDPR.

INTELLIGENZA ARTIFICIALE.

25 Giugno 2024 - L'ESMA fornisce orientamenti alle imprese che utilizzano l'intelligenza artificiale nei servizi di investimento.

L'Autorità europea degli strumenti finanziari e dei mercati (ESMA), l'autorità di regolamentazione e vigilanza dei mercati finanziari dell'UE, ha pubblicato una dichiarazione che fornisce una guida iniziale alle imprese che utilizzano tecnologie di intelligenza artificiale (IA) quando forniscono servizi di investimento ai clienti al dettaglio.

Quando si utilizza l'IA, l'ESMA si aspetta che le imprese rispettino i requisiti pertinenti della Direttiva MiFID II, in particolare per quanto riguarda gli aspetti organizzativi, la condotta degli affari e il loro obbligo normativo di agire nel migliore interesse del cliente.

Sebbene le tecnologie di IA offrano potenziali vantaggi alle aziende e ai clienti, comportano anche rischi intrinseci, come ad esempio:

- discriminazioni algoritmiche (*bias*) e problemi di qualità dei dati;
- processo decisionale opaco;
- eccessivo affidamento all'IA da parte di aziende e clienti per il processo decisionale; e
- problemi di privacy e sicurezza legati alla raccolta, all'archiviazione e all'elaborazione della grande quantità di dati necessari ai sistemi di IA.

I potenziali usi dell'IA da parte delle imprese di investimento che sarebbero coperti dai requisiti previsti dalla MiFID II includono l'assistenza clienti, l'individuazione delle frodi, la gestione del rischio, la conformità e il supporto alle imprese nella fornitura di consulenza in materia di investimenti e gestione del portafoglio.

L'ESMA e le autorità nazionali competenti continueranno a monitorare l'uso dell'IA nei servizi di investimento e il pertinente quadro giuridico dell'UE per determinare se siano necessarie ulteriori azioni in questo settore.

---

21 giugno 2024 - La Commissione europea ospita la prima riunione di alto livello per il prossimo Consiglio dell'UE sull'IA, per impostare l'attuazione dell'AI Act.

Sebbene si sia ancora in attesa dell'entrata in vigore formale del Regolamento Generale UE sull'IA (la pubblicazione in Gazzetta Ufficiale è prevista per il prossimo 12 Luglio 2024, l'entrata in vigore 20 giorni dopo, all'inizio di agosto), la Commissione UE ha ospitato la prima riunione di alto livello per gettare le basi per l'imminente attuazione dell'AI Act.

L'ordine del giorno prevedeva discussioni tra cui:

- visione strategica sull'attuazione della legge sull'AI e sul ruolo del Consiglio sull'IA;
- approcci nazionali alla *governance* e alla supervisione dell'AI Act;
- primi risultati e priorità relativi all'attuazione della legge sull'IA da parte della Commissione europea;
- organizzazione del Consiglio sull'IA, come il mandato, il processo di selezione del presidente, il processo decisionale e la creazione di sottogruppi.

Oltre ai delegati della Commissione europea erano presenti delegati di alto livello di tutti gli Stati membri dell'UE. Il Garante europeo della protezione dei dati (GEPD) ha partecipato in qualità di osservatore al Consiglio dell'AI. Inoltre, erano presenti in qualità di osservatori anche i rappresentanti dei membri del SEE/EFTA, Norvegia, Liechtenstein e Islanda.

La prossima riunione si terrà dopo l'entrata in vigore della legge sull'IA, all'inizio dell'autunno.

Le disposizioni chiave relative all'istituzione e ai compiti del Consiglio dell'AI sono gli articoli 65 e 66 del Regolamento sull'IA.

---

20 Giugno 2024 – Commissione UE: Avviata una consultazione pubblica mirata sull'Intelligenza Artificiale nel settore finanziario.

La Direzione generale della Stabilità finanziaria, dei servizi finanziari e dell'Unione dei mercati dei capitali della Commissione europea ha avviato una consultazione pubblica sull'intelligenza artificiale (IA) nel settore finanziario.

Il Regolamento dell'UE sull'IA integra le normative già esistenti in materia di servizi finanziari e la consultazione mira a raccogliere le informazioni utili alla Commissione per evitare la duplicazione di requisiti.

La consultazione prende in considerazione le applicazioni dell'IA nei servizi finanziari, compresi casi d'uso particolari come il rilevamento delle frodi, la gestione del rischio, l'automazione delle attività di routine, la consulenza finanziaria personalizzata, il miglioramento del processo decisionale e il miglioramento dei servizi ai clienti. La consultazione mira, inoltre, a chiarire le sfide e i rischi dell'uso delle applicazioni di IA, come la conformità normativa alle normative finanziarie, i pregiudizi e la discriminazione, la trasparenza, la spiegabilità e l'affidabilità.

Particolare rilevanza ha l'applicazione della IA per uso generale (GPAI) nei servizi finanziari, conformemente alla definizione di cui all'articolo 3, paragrafo 63, della legge sull'IA.

Inoltre, la consultazione prende in considerazione casi d'uso specifici dell'IA nei servizi bancari e finanziari, come l'impiego dell'IA nel settore dei pagamenti e l'uso dell'IA per la valutazione del rischio di credito e il *credit scoring*, la conformità, l'antiriciclaggio e il servizio clienti. Analogamente, la consultazione mira a ottenere informazioni sull'uso dell'IA nei mercati mobiliari per le valutazioni del rischio e sui possibili usi dell'IA nelle assicurazioni e nelle pensioni.

Infine, la consultazione richiede un riscontro circa orientamenti adeguati per attuare le disposizioni sui due casi specifici di impiego dell'IA ad alto rischio nel settore finanziario di cui all'Allegato III dell'AI Act: **(1)** quando i sistemi di IA sono utilizzati per valutare il merito creditizio delle persone fisiche o stabilire il loro punteggio di credito e **(2)** quando i sistemi di IA sono utilizzati per la valutazione del rischio e la fissazione dei prezzi per le persone fisiche nel caso dell'assicurazione sulla vita e sull'assicurazione sanitaria.

La partecipazione alla consultazione pubblica è aperta fino al 15 settembre 2024.

MERCATI DIGITALI.

3 Luglio 2024 – Per la Commissione UE il modello "Pay or consent" adottato da Meta vìola il Digital Markets Act.

La Commissione UE ha informato Meta delle sue conclusioni preliminari secondo cui il suo modello pubblicitario "pay or consent" non è conforme al Digital Markets Act (DMA). Secondo la Commissione, tale scelta binaria costringe gli utenti ad acconsentire alla combinazione dei loro dati personali e non fornisce loro una versione meno personalizzata ma equivalente dei social network di Meta.

Le piattaforme online spesso raccolgono dati personali attraverso servizi propri e di terze parti per fornire servizi pubblicitari online. Grazie alla loro posizione significativa nei mercati digitali, i gatekeeper sono stati in grado di imporre termini di servizio alla loro vasta base di utenti, raccogliendo così grandi quantità di dati personali. Ciò ha dato loro potenziali vantaggi rispetto ai concorrenti che non hanno accesso a una quantità così grande di dati, sollevando così forti barriere alla fornitura di servizi di pubblicità online e servizi di social network.

Ai sensi dell'articolo 5, paragrafo 2, della legge sui mercati digitali (Regolamento UE 2022/1925), i gatekeeper devono chiedere il consenso degli utenti per combinare i loro dati personali tra i servizi di piattaforma di base designati e altri servizi e, se un utente rifiuta tale consenso, dovrebbe avere accesso a un'alternativa meno personalizzata ma equivalente.

---

24 Giugno 2024 – Commissione UE contro Apple, App Store viola il Digital Markets Act (Regolamento UE 2022/1925).

In data 24 giugno 2024, la Commissione UE ha informato Apple che le regole dell'App Store violano il Digital Markets Act (DMA), poiché impediscono agli sviluppatori di app di indirizzare liberamente i consumatori verso canali alternativi per offerte e contenuti.

Inoltre, l'esecutivo europeo ha avviato una nuova procedura di non conformità contro Apple a causa del timore che i suoi nuovi requisiti contrattuali per gli sviluppatori di app di terze parti e gli app store, inclusa

la nuova "*Core Technology Fee"* di Apple, non siano in grado di garantire l'effettiva conformità agli obblighi di Apple ai sensi il DMA.

Secondo la DMA, gli sviluppatori che distribuiscono le loro app tramite l'App Store di Apple dovrebbero essere in grado, gratuitamente, di informare i propri clienti su possibilità di acquisto alternative più economiche, indirizzarli verso tali offerte e consentire loro di effettuare acquisti.

Attualmente Apple ha tre categorie di termini commerciali che regolano il suo rapporto con gli sviluppatori di app, comprese le regole di indirizzo dell'App Store. La Commissione UE constata preliminarmente che:

- nessuno di questi termini commerciali consente agli sviluppatori di guidare liberamente i propri clienti. In particolare, gli sviluppatori non possono informare i clienti dei prezzi all'interno dell'app o comunicare in altro modo con i propri clienti per promuovere offerte disponibili su canali di distribuzione alternativi;
- nella maggior parte delle condizioni commerciali a disposizione degli sviluppatori di app, Apple consente la guida solo tramite "link-out", ovvero gli sviluppatori di app possono includere nella loro app un collegamento che reindirizza il cliente a una pagina web dove il cliente può concludere un contratto. Il processo di collegamento è soggetto a numerose restrizioni imposte da Apple che impediscono agli sviluppatori di app di comunicare, promuovere offerte e concludere contratti attraverso il canale di distribuzione di loro scelta.

Sebbene Apple possa ricevere un compenso per facilitare l'acquisizione iniziale di un nuovo cliente da parte degli sviluppatori tramite l'App Store, i compensi addebitati da Apple vanno oltre quanto strettamente necessario per tale compenso.

Ora Apple ha la possibilità di esercitare i propri diritti di difesa esaminando i documenti contenuti nel fascicolo dell'indagine della Commissione europea e rispondendo per iscritto alle risultanze preliminari dell'esecutivo.

Se le opinioni preliminari della Commissione saranno confermate, la Commissione adotterà una decisione di non conformità entro 12 mesi dall'apertura del procedimento (25 marzo 2024).

---

18 Giugno 2024 – Commissione UE: pubblicato il rapporto sullo stato di attuazione negli Stati Membri della Direttiva 2019/2161 sulla modernizzazione e il rafforzamento della protezione dei consumatori on line.

La Commissione europea ha pubblicato un rapporto sull'attuazione della direttiva 2019/2161 relativa a una migliore applicazione e modernizzazione delle norme dell'Unione in materia di protezione dei consumatori, che ha introdotto rilevanti aggiornamenti alla normativa esistente, soprattutto per quanto riguarda:

- divieti di pratiche online sleali come la pubblicità e i posizionamenti a pagamento nei risultati di ricerca;
- nuovi obblighi di trasparenza per quanto riguarda il posizionamento dei risultati di ricerca online e la conclusione di un contratto in un mercato online; e
- l'estensione della direttiva sui diritti dei consumatori ai servizi digitali gratuiti per i quali i consumatori forniscono dati personali anziché un compenso monetario.

In particolare, il rapporto ha evidenziato lacune nella implementazione nazionale delle norme sulla trasparenza sui risultati di ricerca. Inoltre, è stato rilevato come debbano essere meglio applicate le norme che impongono ai fornitori di servizi di ricerca online che includono annunci pubblicitari nei risultati di ricerca di garantire che siano chiaramente visibili e facilmente distinguibili dagli altri risultati di ricerca. Il rapporto ha ricordato che nel caso delle piattaforme online di grandi dimensioni (VLOP) e dei motori di ricerca online di grandi dimensioni (VLOSE), il Digital Services Act (DSA) richiede la disponibilità di almeno un'opzione di sistema di raccomandazione non personalizzata.

Inoltre, il rapporto ha evidenziato che i mercati online hanno implementato l'obbligo di fornire ulteriori informazioni sullo status dei fornitori terzi, ma che i consumatori non sono ancora sicuri dell'identità dei venditori e delle modalità della transazione.

Infine, sebbene diversi Stati membri dell'UE abbiano attuato nuove opzioni per consentire ai consumatori di revocare il consenso nelle transazioni basate sulla fornitura di dati personali, non esiste ancora alcuna misurazione dell'impatto di tali pratiche.

INFORMATION TECHNOLOGY

2 Luglio 2024 – Corte Suprema di Cassazione: i messaggi WhatsApp costituiscono corrispondenza anche se già letti e conservati dal destinatario e ad essi si applica la disciplina del sequestro di corrispondenza.

Con la sentenza n. 25549 del 28 giugno 2024 la Suprema Corte di Cassazione ha per la prima volta applicato il nuovo orientamento espresso dalla Corte Costituzionale nella sentenza n. 170 del 2023 ed ha chiarito se i messaggi di WhatsApp, dopo essere stati letti e conservati dal destinatario, devono essere acquisiti nel rispetto della disciplina delle intercettazioni di comunicazioni informatiche o telematiche oppure di quella del sequestro di corrispondenza oppure di quella dei semplici documenti.

Fino alla pronuncia della Corte costituzionale (che ha stabilito che far perdere ai messaggi WhatsApp la natura di corrispondenza soltanto perché letti restringerebbe l'ambito della tutela costituzionale di cui all'art. 15 Cost.) la Suprema Corte seguiva un indirizzo che riconduceva i messaggi del social letti e conservati a meri documenti, rendendo applicabile l'articolo 234 c.p.p., stabilendo che: "*in tema di mezzi di prova, i messaggi di posta elettronica i messaggi WhatsApp e gli SMS conservati nella memoria di un dispositivo elettronico conservano la natura di corrispondenza anche dopo la ricezione da parte del destinatario, almeno fino a quando per il decorso del tempo per altra causa essi non abbiano perso ogni carattere di attualità, in rapporto all'interesse e alla sua riservatezza, trasformandosi in un mero documento storico sicché - fino a quel momento - la loro acquisizione deve avvenire secondo le forme previste dall'art. 254 cod. proc. pen. per il sequestro della corrispondenza*".

---

25 Giugno 2024 – Sezioni Unite della Cassazione: principi chiarificatori in materia di acquisizione come prova attraverso un ordine europeo di indagine presso un'autorità giudiziaria straniera di dati tratti da criptofonini.

Le Sezioni Unite penali della Corte di cassazione con la sentenza 14 giugno 2024, n. 23755 hanno dato risposta ai seguenti quesiti: «*Se l'acquisizione di messaggi su chat di gruppo, scambiati con sistema cifrato, attraverso un ordine europeo di indagine presso un'autorità giudiziaria straniera che ne abbia eseguito la decrittazione costituisca acquisizione di documenti e di dati informatici ai sensi dell'art. 234-bis c.p.p. o di documenti ex art. 234 c.p.p. ovvero sia riconducibile ad altra disciplina relativa all'acquisizione di prove; se l'acquisizione di cui sopra debba essere oggetto, ai fini della utilizzabilità dei relativi dati, di preventiva o successiva verifica giurisdizionale della sua legittimità da parte della autorità giurisdizionale nazionale*».

Questi i principi di diritto acclarati dalla Suprema Corte:

- la trasmissione, richiesta con ordine europeo di indagine, del contenuto di comunicazioni scambiate mediante criptofonini, già acquisite e decrittate dall'autorità giudiziaria estera in un procedimento penale pendente davanti ad essa, non rientra nell'ambito di applicazione dell'art. 234-bis c.p.p., che opera al di fuori delle ipotesi di collaborazione tra autorità giudiziarie, bensì nella disciplina relativa alla circolazione delle prove tra procedimenti penali, quale desumibile dagli artt. 238 e 270 c.p.p. e 78 disp. att. c.p.p.;

- in materia di ordine europeo di indagine, le prove già in possesso delle autorità competenti dello Stato di esecuzione possono essere legittimamente richieste ed acquisite dal pubblico ministero italiano senza

la necessità di preventiva autorizzazione da parte del giudice del procedimento nel quale si intende utilizzarle;

- l'emissione, da parte del pubblico ministero, di ordine europeo di indagine diretto ad ottenere il contenuto di comunicazioni scambiate mediante criptofonini, già acquisite e decrittate dall'autorità giudiziaria estera in un procedimento penale pendente davanti ad essa, non deve essere preceduta da autorizzazione del giudice italiano, quale condizione necessaria a norma dell'art. 6 Direttiva 2014/41/UE, perché tale autorizzazione, nella disciplina nazionale relativa alla circolazione delle prove, non è richiesta per conseguire la disponibilità del contenuto di comunicazioni già acquisite in altro procedimento;

- la disciplina di cui all'art. 132 del Codice della privacy relativa all'acquisizione dei dati concernenti il traffico di comunicazioni elettroniche e l'ubicazione dei dispositivi utilizzati, si applica alle richieste rivolte ai fornitori del servizio, ma non anche a quelle dirette ad altra autorità giudiziaria che già detenga tali dati, sicché, in questo caso, il pubblico ministero può legittimamente accedere agli stessi senza chiedere preventiva autorizzazione al giudice davanti al quale intende utilizzarli;

- l'utilizzabilità del contenuto di comunicazioni scambiate mediante criptofonini, già acquisite e decrittate dall'autorità giudiziaria estera in un procedimento penale pendente davanti ad essa, e trasmesse sulla base di ordine europeo di indagine, deve essere esclusa se il giudice italiano rileva che il loro impiego determinerebbe una violazione dei diritti fondamentali, fermo restando che l'onere di allegare e provare i fatti da cui inferire tale violazione grava sulla parte interessata;

- l'impossibilità per la difesa di accedere all'algoritmo utilizzato nell'ambito di un sistema di comunicazioni per criptare il testo delle stesse non determina una violazione dei diritti fondamentali, dovendo escludersi, salvo specifiche allegazioni di segno contrario, il pericolo di alterazione dei dati in quanto il contenuto di ciascun messaggio è inscindibilmente abbinato alla sua chiave di cifratura, ed una chiave errata non ha alcuna possibilità di decriptarlo anche solo parzialmente.

CYBERSECURITY

3 Luglio 2024 - Pubblicata sulla Gazzetta Ufficiale la Legge sula Cybersicurezza nazionale.

E' stata pubblicata sulla Gazzetta Ufficiale n. 153 del 2 luglio 2024 la Legge 28 giugno 2024, n. 90 recante "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*".

Il testo è composto da 24 articoli che introducono, tra le altre modifiche:

- pene più severe per reati quali l'accesso abusivo a sistema informatico o il danneggiamento di informazioni, dati e programmi informatici;
- un allargamento del perimetro dei soggetti tenuti a rafforzare le proprie difese;
- nuovi delitti come l'estorsione informatica;
- allungamento dei tempi d'indagine e si favorisce il ricorso alle intercettazioni;
- la centralità, per i reati più gravi, della Procura antimafia;
- una procedura di allarme e di collaborazione con Acn, l'Agenzia per la cyber sicurezza, per gli interventi riparatori;
- una modalità di intervento quando ci sono competenze concorrenti, per esempio, di Acn e della polizia giudiziaria;
- rafforzamento dell'azione contro i crimini informatici, con l'individuazione di nuove fattispecie di reato e l'uso di più efficaci strumenti di indagine.

Tra le diverse novità è prevista anche l'introduzione di un 3 comma nell'art. 629 c.p. (estorsione), a sua volta richiamato nell'art. 24-bis D. Lgs. n. 231/2001 in tema di responsabilità degli enti, secondo cui «chiunque, mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000. La pena è della reclusione da otto a ventidue anni e

della multa da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nel terzo comma dell'articolo 628 nonché nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o per infermità».

---

3 Luglio 2024 – Adottato dall'Agenzia Nazionale per la Cybersicurezza il Regolamento Unico per il Cloud delle PA e la qualificazione dei software e dei servizi: il nuovo regime è in vigore dal 1° agosto 2024.

I servizi digitali sono la modalità primaria di fornitura delle prestazioni al cittadino da parte delle Pubbliche Amministrazioni. Il percorso di transizione al cloud della PA garantisce affidabilità, sicurezza e sostenibilità nel tempo dei servizi pubblici.

Il processo di **qualificazione** consente all'Agenzia di svolgere le verifiche preventive sul livello di conformità dei servizi cloud offerti da operatori privati, dei quali si possono avvalere le PA in alternativa all'erogazione in proprio dei servizi.

La scelta dei servizi cloud qualificati da ACN avviene in base alla classificazione dei dati e dei servizi. Grazie alla classificazione viene stabilito l'impatto dei servizi e dei dati trattati da una PA in relazione al loro livello di criticità.

Le PA possono consultare il catalogo ACN per individuare i servizi e il livello di qualificazione concesso, per verificare in via preventiva se sono conformi al livello di classificazione necessario per gestire i propri dati o servizi.

Il Regolamento unico per le infrastrutture e i servizi cloud per la PA di ACN chiarisce:

- le modalità per la **classificazione**, per la **migrazione** e per la **qualificazione** dei servizi cloud, di cui la PA può approvvigionarsi ricorrendo al libero mercato;
- le misure e i requisiti per il raggiungimento dei **livelli minimi** di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA;
- le **caratteristiche** di qualità, sicurezza, performance, scalabilità e portabilità dei servizi cloud per la PA.

Il Regolamento, adottato da ACN con Decreto Direttoriale n. 21007/24 del 27 giugno 2024 e applicabile dal 1 agosto 2024, aggiorna i livelli minimi e le caratteristiche al mutato scenario di rischio e i termini legati al procedimento di rilascio delle qualifiche. Il Regolamento norma anche l'utilizzo delle **infrastrutture di housing** e i **servizi di prossimità** (cosiddetti edge), sempre più diffusi in ragione dell'esigenza di ridurre i tempi di latenza per gli utenti finali.

Una delle principali novità riguarda inoltre la differenziazione tra:

- la **qualifica** dei servizi cloud erogati da fornitori privati, che prevede una verifica di conformità ex-ante a cui fa seguito la pubblicazione della relativa scheda sul catalogo ACN,
- l'**adeguamento** delle infrastrutture (a prescindere dalla natura del soggetto responsabile) e dei servizi erogati da operatori pubblici, basata sulla dichiarazione di conformità inviata ad ACN rispetto ai requisiti previsti.

In entrambi i casi, è prevista una fase di **monitoraggio ex-post** nel periodo di validità della qualifica e dell'adeguamento (36 mesi), grazie alla quale ACN può verificare il mantenimento dei requisiti necessari al trattamento dei dati e dei servizi in linea con il livello di classificazione.

Dal 1° agosto 2024, le infrastrutture dei servizi cloud che avevano ottenuto una qualifica di livello QI1-4, in corso di validità, saranno convertite – per quanto riguarda la nomenclatura – in livello AI1-4.

---

27 Giugno 2024 – Pubblicati nella Gazzetta Ufficiale della UE i Regolamenti delegati della Commissione UE attuativi di alcuni obblighi del Regolamento DORA.
Sono stati pubblicati sulla Gazzetta Ufficiale dell'Unione Europea i seguenti atti delegati in attuazione del Regolamento UE 2022/2554 sulla resilienza operativa digitale (Regolamento DORA):

- **Regolamento Delegato (UE) 2024/1772** relativo ai criteri per la classificazione degli incidenti informatici
- **Regolamento Delegato (UE) 2024//1773** relativo alla politica per la fornitura di servizi ICT da parte di terzi a supporto di funzioni essenziali o importanti
- **Regolamento Delegato (UE) 2024/1774** relativo agli strumenti, ai metodi, ai processi e alle politiche per la gestione dei rischi informatici

I regolamenti delegati entreranno in vigore il 15 luglio 2024, saranno obbligatori in tutti i loro elementi e direttamente applicabili.

Molte entità finanziarie, bancarie e assicurative tenute – dal prossimo 17 Gennaio 2025 - all'applicazione del Regolamento UE 2022/2554 sulla resilienza operativa digitale (Regolamento DORA) sono tenute a rivedere molte politiche gestionali interne. Ad esempio, il Capo V con soli tre articoli (28-30) ridisegna e impatta profondamente sulle procedure di selezione e qualifica dei fornitori ICT e sulla stessa struttura dei contratti con fornitori terzi ICT e sul loro ciclo di vita. Inoltre, il Regolamento DORA obbliga ad aggiornare ruoli, organigrammi e direttive al personale, impatta sui piani di formazione – da diversificare a seconda del ruolo dirigenziale o meno - riscrive le responsabilità dei revisori legali e soprattutto pone al centro del sistema di responsabilità l'organismo di gestione. Anche pubblicazione in GU – lo scorso 25 giugno – dei sopra citati atti delegati della Commissione UE (tra l'altro il quadro complessivo, tra DORA, Regulatory Technical Standard – RTS tra Gennaio e Luglio 2024 e atti delegati e di straordinaria complessità e articolazione) conferma la necessità di coordinare gli adempimenti DORA con le altre politiche in essere. Il profondo intreccio tra il Regolamento DORA e il GDPR, ad esempio: non solo il Regolamento DORA insiste sugli obblighi di garantire "*autenticità, integrità, riservatezza e disponibilità*" di dati sia personali che non personali, ma gli stessi atti delegati ora publicati disciplinano l'impatto degli adempimenti DORA sulle politiche di adeguamento al GDPR già in essere. Ad esempio il Regolamento Delegato (UE) 2024/1772 relativo ai criteri per la classificazione degli incidenti informatici fissa il rapporto con la notifica della *data breach* GDPR in caso di incidente; oppure il Regolamento Delegato (UE) 2024//1773 relativo alla politica per la fornitura di servizi ICT da parte di terzi a supporto di "*funzioni essenziali o importanti*" ricorda che nel caso il fornitore sia anche un Responsabile esterno ai sensi del GDPR, gli adempimenti *data protection* vanno fatti confluire nella politica, la quale (si veda ad esempio l'articolo 5, comma 3, lettera (e) del Regolamento Delegato (UE) 2024//1773) deve includere anche una valutazione preliminare del rischio specifica sul fornitore per quanto riguarda "i rischi legati alla protezione dei dati riservati o personali" (valutazione che anche le Linee Guida del Comitato europeo per la protezione dei dati personali n. 7/2020 sul concetto di titolare e responsabile del trattamento richiedono di svolgere sul fornitore esterno-responsabile del trattamento).

REATI INFORMATICI

21 Giugno 2024 – *Revenge porn*: la diffusione del materiale deve essere realizzata solo da chi ha fatto le riprese o se ne è indebitamente impossessato.

La controversia in esame ha ad oggetto il reato di diffusione illecita di immagini o video sessualmente espliciti ex art. 612-*ter* c.p., comunemente indicato utilizzando l'espressione "*revenge porn*".

Tizio ricorre per cassazione censurando la sentenza impugnata sostenendo che la diffusione «*deve intervenire senza il consenso delle persone rappresentate e deve riguardare materiali sessualmente espliciti destinati a rimanere privati, ma, come più volte osservato, realizzati consensualmente, tant'è che la condotta può essere realizzata solo da chi ha operato la ripresa o da chi se ne è indebitamente impossessato, sottraendola a chi l'aveva realizzata*».

Nel caso in esame, invece, la ripresa era stata frutto di intercettazione ambientale eseguita dall'A.G. a totale insaputa dei soggetti ripresi, per cui, salva la violazione del principio di legalità e tassatività, essa non può essere considerata alla stregua del materiale indicato dai commi primo e terzo dell'art. 612-*ter* c.p..

In sede di legittimità, la Suprema Corte di Cassazione, sez. V Penale, con la sentenza del 20 giugno 2024, n. 24379 ripercorre anzitutto il fenomeno del “revenge porn”, a cui il nostro Legislatore ha risposto con l'introduzione nel Codice penale dell'art. 612-ter, approvato con un emendamento alla Legge n. 69/2019, il cd. “Codice Rosso”.

Come emerge dal testo normativo, «la norma non solo richiede l'assenza di consenso, ma anche che le immagini o i video siano "destinati a rimanere privati", come se, si è osservato in dottrina, ancor prima dell'assenza di consenso alla divulgazione, vi sia la rottura di un *pactum fiduciae* tra due individui, presumibilmente legati da una relazione, tale da aver impresso una precisa destinazione ai contenuti, poi disattesa da uno dei due».

Quanto al motivo di ricorso sopra specificato, la Suprema Corte lo ritiene fondato.

In virtù dell'evoluzione ermeneutica delle condotte e della latitudine del sintagma revenge porn, la Corte ritiene che la condotta incriminata sia più ampia di quella realizzata unicamente nell'ambito di un pregresso rapporto sentimentale, nel cui contesto si sia verificato un utilizzo diverso del materiale originariamente destinato a rimanere circoscritto e riservato. Depone a favore di tale orientamento la rubrica della norma, la quale delinea la rilevanza penale della diffusione illecita di immagini e video sessualmente espliciti, senza alcun riferimento ad uno specifico contesto di pregressa relazione sentimentale.

Ciò detto, la Cassazione ribadisce i due requisiti che devono sussistere entrambi contemporaneamente: la mancanza di consenso e la destinazione privata, intesa come formazione del materiale ad opera degli stessi soggetti che vi sono rappresentati. Pertanto, è necessario che l'autore della condotta di diffusione del di tale materiale sia colui che aveva in precedenza realizzato il detto materiale, o se ne era impossessato sottraendolo.

Tali requisiti non risultano ricorrere nel caso in esame, in quanto l'autore del fatto è un soggetto del tutto diverso da colui che aveva realizzato il materiale, né risulta che egli se ne sia appropriato sottraendolo.
Per questi motivi, la Cassazione accoglie il ricorso.