Circolare del 28 giugno 2021

SOMMARIO

CONTROLLO INDISCRIMINATO DEI LAVORATORI: COMUNE SANZIONATO DAL GARANTE PER MONITORAGGIO OCCULTO DELLA NAVIGAZIONE WEB DEI DIPENDENTI

La protezione delle informazioni personali e il rispetto della vita privata vale anche nel pubblico impiego dove permane, comunque, una ragionevole aspettativa di riservatezza. Questo è uno dei principi ribaditi nel provvedimento del Garante Privacy n. 190 del 13 maggio 2021 con il quale ha irrogato una **sanzione da 84 mila euro al Comune di Bolzano** per aver tratto illecitamente i dati dei propri dipendenti in violazione del GDPR, nonché del Codice Privacy.

L'atto che ha dato origine all'avvio del procedimento da parte dell'Autorità Garante, è stato il reclamo presentato dall'interessato, dipendente della PA sanzionata, che eccepiva la liceità del trattamento dei dati personali utilizzati per avviare un procedimento disciplinare a suo carico, nonché la violazione dei principi di liceità, correttezza e minimizzazione del GDPR. Inoltre, veniva sollevata violazione dell'art. 4, L. 300/1970 poiché il controllo effettuato sulla navigazione apparentemente legittimato dalle necessarie misure tecniche da impiegarsi a salvaguardia dei dati trattati, come previsto dal Codice dell'Amministrazione Digitale (CAD), era invece da ritenersi massivo, costante ed indiscriminato. L'Ente, in via cautelativa, ha avviato diversi correttivi nella speranza che essi venissero presi in considerazione mitigando l'eventuale sanzione; ma il Garante, ha comunque sanzionato il Comune ribadendo interessanti principi con riguardo alla tutela della riservatezza dei prestatori di lavoro.

Tra gli altri, non sono stati ritenuti sufficienti né l'accordo siglato con le rappresentanze sindacali maggiormente rappresentative ex art. 4, L. 300/1970 né tanto meno il codice di comportamento relativo all'utilizzo della rete internet. Sul punto il Garante ha ribadito che il controllo/monitoraggio attraverso impianti audiovisivi e altri strumenti di lavoro può avvenire "esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale", precisando che i PC e gli altri dispositivi connessi alla rete non possono essere ricondotti nell'alveo degli strumenti di lavoro, diversamente dai sistemi di blocco automatico della navigazione per certe categorie di siti web (si v. anche provvedimento del 13 luglio 2016, n. 303, doc. web n. 5408460).

Inoltre, un controllo così come effettuato dal Comune di Bolzano (ex ante) esula dall'apparente finalità di monitoraggio dell'attività insolita o, comunque, a tutela della sicurezza dell'infrastruttura informatica ma è invece finalizzato al monitoraggio dell'attività lavorativa, tant'è che è sfociato in un procedimento sanzionatorio, anche se poi sospeso.

APP IO PER LE CERTIFICAZIONI VERDI, VIA LIBERA DEL GARANTE PRIVACY DOPO LE MODIFICHE APPORTATE DA PAGOPA

Il Garante per la protezione dei dati personali, anche alla luce delle modifiche tecniche apportate da Pago PA, ha espresso **parere favorevole all'utilizzo dell'App IO** per il recupero delle certificazioni Covid-19, in conformità al DPCM sul rilascio e la verifica delle certificazioni verdi, adottato dal Governo.

La società PagoPA, incaricata dello sviluppo e della gestione dell'App IO, dopo aver introdotto misure per risolvere le criticità rilevate dal Garante riguardo la privacy degli utenti, ha ulteriormente modificato l'app per mettere a disposizione anche il servizio "Certificazione Verde Covid-19" del Ministero della Salute. Gli utenti saranno informati su questa nuova funzionalità al primo accesso e avranno la possibilità di disattivarla.

Per assicurare maggiori tutele alle informazioni degli oltre 11 milioni di utenti che usano l'applicazione, alcune delle quali particolarmente delicate in quanto riguardanti lo stato di salute, il Garante ha comunque chiesto alla società che i dati relativi all'utilizzo del servizio ***Green Pass***, trasmessi a Mixpanel, siano conservati per un periodo limitato, non superiore a dieci giorni dalla raccolta, e successivamente cancellati senza ritardo.

PagoPA dovrà comunque, come già stabilito nel precedente provvedimento del 16 giugno, chiedere il consenso degli utenti al trasferimento dei dati a Mixpanel. E il blocco dei dati già raccolti dalla società statunitense, prima dell'intervento del Garante, permarrà fino alla fine dell'istruttoria avviata dall'Autorità.

SINDACO DIFFONDE SU FACEBOOK IMMAGINI E VIDEO DI MINORENNI DISABILI E PRESUNTI TRASGRESSORI: INTERVIENE IL GARANTE DELLA PRIVACY

Il profilo social del Sindaco non è di per sé di interesse pubblico. Il personaggio politico non può ritenere automaticamente legittimata dai compiti istituzionali la pubblicazione in rete di testi, immagini e video. È il principio desumibile dal provvedimento del Garante n. 197 del 13 maggio 2021, che ha irrogato una **sanzione di 50 mila euro a un primo cittadino**, per avere diffuso sulle proprie pagine social immagini e video in chiaro di minorenni disabili, persone disagiate, presunti autori di trasgressioni esponendoli ai commenti offensivi degli utenti del social network.

Non è bastato al Sindaco in questione sottolineare lo scopo di denunciare situazioni di degrado, né rimarcare di avere agito per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, di cui è investito quale primo cittadino. La pronuncia, al di là del caso specifico, mette in evidenza che l'ente pubblico e i suoi amministratori devono agire con cautela quando usano le reti sociali, caratterizzate da tanto apparente quanto ingannevole facilità di utilizzo.

Non a caso, nella pronuncia citata, il Garante ha disatteso la linea difensiva del Sindaco, rilevando l'inesistenza di una norma o di atti interni del comune diretti a contemplare l'utilizzo dei social network nell'ambito del perseguimento di finalità connesse all'esercizio di compiti di interesse pubblico. Peraltro gli strumenti della comunicazione elettronica, delle app di messaggistica e dei social non sono certo un tabù per le Pubbliche Amministrazioni, che devono agire, però, nel quadro di solide basi normative.

A tale proposito si ritiene che le PA possano agire nel solco della legge 150/2000, con adozione di un regolamento interno disciplinante l'apertura e l'utilizzo dei profili social istituzionali, o di profili di amministratori e dirigenti per scopi istituzionali, previa stesura di un piano di comunicazione e istituzione di un ufficio in grado di gestire e moderare l'attività sui social stessi, con la revisione del registro del trattamento e informative privacy. Aprire un profilo senza i necessari atti preparatori e regolatori porta dritto filato verso la sanzione del Garante della privacy.

TORINO, STOP DEL GARANTE DELLA PRIVACY ALLE TELECAMERE INTELLIGENTI

La giunta della Sindaca di Torino, Chiara Appendino, ha proposto il sistema di telecamere intelligenti ARGO, ma in queste ore è arrivato lo stop del Garante della Privacy. Il Comune capoluogo di regione aveva promosso un innovativo sistema di videosorveglianza, ma malgrado i proclami è arrivato lo stop. Il progetto ha trovato il diniego del centro Hermes per la tutela dei diritti umani, trovando il consenso del Garante.

La giunta Appendino lavora alla videosorveglianza ARGO da ben tre anni. Questo sistema di controllo è molto diverso da quello studiato per la periferia nord, dove le telecamere sono canoniche. Il progetto ha un costo di due milioni di euro, e prevede l'installazione di 273 telecamere intelligenti in aggiunta alle 107 già installate in città. Queste nuove telecamere hanno al loro interno un sistema che riconosce le targhe di auto ed indumenti per raccogliere metadati. Gli sviluppatori, la società 5T in collaborazione con la Polizia Municipale, rassicurano sulla mancata raccolta di dati biometrici (ossia il riconoscimento dei volti).

Il progetto ha trovato il supporto di prefettura e regione, e in questi giorni erano state installate le prime camere.

Malgrado le rassicurazioni, il Garante della Privacy ha deciso di aprire una istruttoria preliminare, che può portare a una sanzione o allo spegnimento delle telecamere.

Inoltre, malgrado i mancati dati biometrici, ARGO sa riconoscere indumenti e sesso dei passanti, creando potenzialmente uno strumento di pedinamento. L'ambiguità legata al vestiario, potrebbe creare falsi positivi e una ricerca errata di individui. Queste argomentazioni, unite all'ambiguità del termine "Metadati" ha portato il garante a emettere il provvedimento.

Il Comune di Torino, onde evitare sanzioni, ha chiesto al Garante la cooperazione per rilevare i migliori algoritmi per l'utilizzo di questa tecnologia.

FRANCIA: MULTA DA UN MILIONE DI EURO A IKEA PERCHÈ SPIAVA I DIPENDENTI

Il Tribunale di Versailles ha condannato Ikea a pagare oltre **un milione di euro** in multe per una campagna di spionaggio, non industriale, ma personale, su rappresentanti sindacali, dipendenti e, persino, su alcuni clienti insoddisfatti. Il processo, che ha preso il via lo scorso 22 marzo, ha avuto una sentenza piuttosto rapida, destinata a fare giurisprudenza in ambito lavorativo.

Secondo la sentenza, si tratta di "ricettazione di dati personali in modo fraudolento", condannando 13 dirigenti e l'ex Amministratore Delegato di Ikea France, Jean Lousi Baillot, a pene detentive con la condizionale (18 mesi), per aver fatto spiare diverse centinaia di dipendenti nel periodo fra il 2009 e il 2012. L'accusa aveva richiesto pene più severe, ma il tribunale ha deciso di escludere il capo di imputazione più grave, la "sorveglianza di massa". In quel caso, gli imputati avrebbero rischiato fino a dieci anni di reclusione; L'unico dei dirigenti ad aver ammesso lo spionaggio, Jean-Francois Paris, ha confessato ai giudici francesi che oltre 500.000 euro all'anno erano destinati da Ikea a queste indagini "parallele".

La filiale francese di Ikea impiega più di 10.000 persone in 34 negozi sparsi per tutto il paese. I sindacati hanno accusato Ikea France di aver raccolto dati personali con mezzi fraudolenti, in particolare attraverso file della polizia ottenuti illegalmente (pagando!) e di aver divulgato illecitamente informazioni personali.

Gli avvocati di Ikea Francia hanno negato che l'azienda avesse una strategia di ``spionaggio "generalizzato", comunque l'azienda, ha confermato di aver collaborato alle indagini, ha rischiato una multa fino a 3 milioni e 750.000 euro. L'avvocato Emmanuel Daoud (Ikea Francia), ha detto che la società non ha ancora deciso se fare appello.

Nell'emettere la tutto sommato mite sentenza, la Corte ha preso in considerazione il piano d'azione (e di pulizia) che Ikea ha messo in atto dopo la rivelazione dei fatti, a partire dal 2012. L'azienda, infatti, ha licenziato quattro dirigenti e cambiato la politica interna, subito dopo che la Procura francese ha aperto l'indagine penale.

AMAZON RISCHIA MAXI MULTA DA 425 MILIONI DI DOLLARI PER VIOLAZIONE DEL GDPR

L'autorità per la protezione dei dati del Lussemburgo ha proposto una **multa di oltre 425 milioni di dollari** (circa 350 milioni di euro) contro Amazon.com. Il caso è quello riguardante la protezione dei dati degli utenti nell'Unione Europea, che potrebbe terminare con la più alta sanzione inflitta per la violazione del GDPR, il Regolamento UE sulla privacy (GDPR).

La proposta è stata consegnata alle autorità degli altri Paesi del blocco, secondo le fonti del Wall Street Journal. L'opinione dell'autorità del Lussemburgo è importante, visto che Amazon ha il suo quartier generale proprio nel Granducato. Nel caso specifico, sotto accusa è la raccolta e l'uso dei dati personali degli individui e non è relativo ad Amazon Web Services, il suo business sul cloud computing.

La notizia arriva a pochi giorni da un'altra bacchettata giunta dalla Commissione Europea:

> «Occorre assicurare che la crescita di Internet avvenga in un modo competitivo. I primi risultati di alcune ricerche mostrano il ruolo centrale nell'assistenza voce e operativa di determinati Gatekeeper[1], come Google, Apple e Amazon, che indirizzano comportamenti che influenzano negativamente la concorrenza»

aveva detto la Commissaria UE alla concorrenza Margrethe Vestager, annunciando la pubblicazione di una relazione sul tema da parte della Commissione.

Nel dettaglio, la commissaria ha espresso la preoccupazione dell'UE per il fatto che certi Gatekeeper possano emergere e usare il loro potere per danneggiare la concorrenza. È necessaria una concorrenza leale per sfruttare al meglio l'"Internet delle cose' per i consumatori nella vita quotidiana. Se alcune di queste pratiche sono confermate, ha aggiunto, verranno aperte procedure di violazione della concorrenza.

[1] Il termine **Gatekeeping** è stato ampiamente usato per descrivere il meccanismo con cui avvengono le scelte nel lavoro mediale, specie le decisioni circa il lasciar filtrare o meno una particolare notizia tramite i 'cancelli' (in inglese Gates) di un mezzo di informazione.

TRAGEDIA MOTTARONE, INTERVIENE IL GARANTE: TRAGEDIA NON SIA SPETTACOLO

Il Garante interviene sui media per evitare derive sensazionalistiche con riferimento alla tragedia del Mottarone. In riferimento alla diffusione dei video che raccontano gli ultimi istanti della tragedia della funivia del Mottarone, il Garante per la protezione dei dati personali invita i media e gli utenti dei social network ad **astenersi dall'ulteriore diffusione delle immagini e da forme di spettacolarizzazione** dell'evento, che possono solo acuire il dolore dei familiari delle vittime e di quanti erano loro legati.

I video, il cui contenuto peraltro non era ancora stato portato a conoscenza degli stessi familiari, poco aggiungono, per quanto riguarda l'informazione dell'opinione pubblica, alla ricostruzione della dinamica del terribile incidente, già ampiamente trattata dai media.

Il Garante richiama pertanto gli stessi media al rispetto del principio di essenzialità dell'informazione, fissato dalle Regole deontologiche in materia di attività giornalistica, e alla salvaguardia della dignità delle persone.

L'Autorità lancia un particolare appello a quanti in queste ore stanno postando e condividendo i video sui social network affinché il dolore non diventi strumento per un like in più.

IL GARANTE PRIVACY BLOCCA 'MITIGÀ: L'APP IDEATA PER GESTIRE GLI ACCESSI 'COVID FREE' A EVENTI SPORTIVI E SPETTACOLI

Il Garante per la protezione dei dati personali ha disposto il blocco provvisorio dei trattamenti dei dati personali nei confronti della Società che gestisce l'app "**Mitiga Italia**". L'app era stata utilizzata per la prima volta il 19 maggio scorso per consentire l'ingresso alla finale di Coppa Italia degli spettatori in possesso di certificazione attestante l'avvenuta vaccinazione, la guarigione o lo stato di negatività dal Covid-19.

*La misura si è resa necessaria essendo emersa la possibilità che l'app, nei prossimi giorni, potesse essere utilizzata per governare l'accesso a altri eventi e spettacoli o altre iniziative sportive.

Nel suo provvedimento il Garante ha sottolineato come non esista al momento una valida base giuridica per il trattamento di dati, anche particolarmente delicati come quelli di natura sanitaria, effettuato mediante l'app e finalizzato ad accertare la situazione "Covid Free" di quanti partecipino ad avvenimenti sportivi nonché ad altre manifestazioni pubbliche o accedano a locali aperti al pubblico.

La società Mitiga, infine, avendo il 1° aprile sottoposto all'Autorità l'applicativo, avrebbe comunque dovuto astenersi da ogni trattamento di dati non essendo decorso il tempo previsto dal Regolamento per l'assunzione di una decisione da parte della stessa Autorità.

Il blocco ha effetto immediato e si protrarrà per il tempo necessario a consentire all'Autorità la definizione dell'istruttoria avviata.

SBANDIERARE ONLINE IL QR CODE DEL PROPRIO GREEN PASS È DA EVITARE

Con l'arrivo del Green Pass sui telefonini degli utenti cominciano a girare sui social network le prime immagini dei QR Code postate da chi ha ricevuto il **Pass Vaccinale**, ma si tratta di una prassi da evitare assolutamente, perché quel piccolo quadrato simile a un labirinto è in realtà una miniera di dati personali che racconta molti particolari sulla salute dell'interessato.

A lanciare l'allarme attraverso un videoclip diffuso online è Guido Scorza, componente dell'Autorità Garante per la protezione dei dati personali. Infatti, anche se tali informazioni non sono visibili ad occhio nudo, d'altra parte sono facilmente decifrabili da qualunque curioso che abbia tempo e voglia di mettere il naso nella nostra vita privata.

Benché possa apparentemente sembrare un insignificante geroglifico, così come i comuni codici a barre anche i QR Code (in inglese QR Code, abbreviazione di Quick Response Code) che sono contenuti nel Green Pass possono essere facilmente scansionati attraverso uno smartphone o un qualsiasi altro dispositivo inquadrando il codice con la fotocamera, dopodiché con un pizzico di ingegno e con l'aiuto di una delle varie app liberamente disponibili sugli store che servono per decifrare tali informazioni, sarà possibile leggere in chiaro tutta una serie di informazioni sanitarie che non tutti vorrebbero consapevolmente sbandierare ai quattro venti come chi siamo, se e quando ci siamo vaccinati, quante dosi abbiamo fatto, il tipo di vaccino, se abbiamo avuto il Covid-19 e quando, se abbiamo fatto un tampone e con quale esito.

Nell'utilizzo conforme alle norme che tutelano la privacy degli utenti, quando il codice QR Code del Green Pass viene scansionato dai soggetti autorizzati attraverso l'apposita app del Governo, essi verificano SOLAMENTE se si possiede un valido pass, ma oltre al "semaforo verde" per concederci l'accesso non vengono a conoscenza di alcuna altra informazione non necessaria.

Ogni altro uso del QR code è quindi pericoloso per lo stesso utente e anche per gli altri, perché potrebbe involontariamente facilitare la proliferazione e la circolazione di falsi pass vaccinali, ma anche individui senza troppi scrupoli potrebbero tentare di usare il nostro codice QR per farsi un viaggio all'estero o andare ad un evento sportivo usando i nostri dati personali.

CONDOMINIO: SULLE COMUNICAZIONI DA OSCURARE L'INDIRIZZO EMAIL PERSONALE DEL CONDÒMINO

Riguarda l'uso della mail nelle comunicazioni condominiali il recente provvedimento del Garante (rif. DREP/SK162838-1) facente seguito al reclamo proposto il 25 marzo 2021 da una condòmina, in base all'articolo 77 del GDPR.

LA VICENDA: Un condomino contestava che, nonostante continue richieste e asserite opposizioni in tal senso, l'amministratore trasmetteva comunicazioni via mail a molteplici destinatari lasciando visibile l'indirizzo della reclamante. Si specificava che era stata avanzata anche una richiesta di rettifica dei dati di contatto relativi alla reclamante da utilizzare ai fini dell'inoltro delle comunicazioni inerenti il condominio, rammentando che l'indirizzo email di una persona fisica, anche ove non riporti per esteso il nome dell'interessato, costituisce un dato personale in base all'articolo 4 del GDPR.

LA RISPOSTA: Secondo il Garante, anche laddove la mail possa avere un contenuto che «attiene a temi concernenti la gestione e l'amministrazione del condominio, che pertanto sono stati oggetto di condivisione in quanto di interesse per la compagine condominiale, deve riprendersi quanto già espresso con pronuncia 19 maggio 2000 (documento web 42268) in ordine alle utenze telefoniche ed espresso nel Vademecum «Il Condominio e la privacy» del 10 ottobre 2013 (documento web 2680240, pagina 6) ossia: «gli estremi identificativi delle utenze telefoniche intestate ai singoli condòmini o ai loro familiari, **non possono essere annoverati tra quelli oggetto di necessaria e obbligatoria comunicazione all'interno del condominio**, in quanto gli stessi non rappresentano elementi utili a determinare i diritti e gli oneri della cosa comune, né è rinvenibile alcun obbligo di legge in tal senso», ma resta comunque ferma la possibilità per l'amministratore di trattare e «di comunicare i numeri di telefono ai condòmini richiedenti con il consenso degli interessati (…) salve le eventuali disposizioni del regolamento di condominio».

I SUGGERIMENTI DEL GARANTE: In caso di invii a molteplici destinatari della medesima comunicazione si dovrebbe utilizzare la «funzione cosiddetta Copia Conoscenza Nascosta». E la PEC (posta elettronica certificata)? Il condominio non è obbligato ad averne una, ma se ne è in possesso può chiedere di ricevere lì ogni comunicazione. L'amministratore si ritiene esonerato dall'obbligo di PEC, tranne nei casi previsti dal Dl 185/2008 (ad esempio se è anche un professionista iscritto agli Ordini o Collegi, o quando esercita la propria attività sotto forma di impresa (società di persone o di capitali).

TRASFERIMENTI DI DATI VERSO PAESI EXTRA UE: LE NUOVE CLAUSOLE CONTRATTUALI STANDARD

Lo scorso 4 giugno la Commissione Europea ha adottato una nuova Decisione relativa alle c.d. ***Standard Contractual Clauses*** ("SCC"), in materia, tra l'altro, di trasferimento di dati personali verso paesi terzi. Si ricorda che le SCC costituiscono uno degli strumenti posti a garanzia del trasferimento di dati fuori dall'Unione Europea ai sensi di quanto previsto dall'art. 46 c. 2 lett. c) GDPR, e quindi una delle ipotesi che rendono legittimo tale trasferimento.

L'urgenza di nuove SCC (quelle precedenti risalivano al 2010) derivava, in particolare, da un lato, da un contesto economico ormai fortemente caratterizzato dalla globalizzazione dei mercati, ove il trasferimento internazionale dei dati costituisce un'attività fondamentale oltre che comune, e, dall'altro, dalla necessità di colmare il vuoto creatosi a causa della nota sentenza Schrems II del 16 luglio 2020 (https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091it.pdf), con la quale la Corte di Giustizia UE ha invalidato il c.d. Privacy Schield[2], lasciando "scoperti" i trasferimenti dei dati dall'UE agli USA.

L'iniziativa della Commissione Europa è di tutto rilievo nel mondo privacy, in quanto le nuove clausole contrattuali standard sono conformi alla disciplina di cui al GDPR (oltre che alla giurisprudenza e alla prassi formatesi alla luce del GDPR): in tal modo, gli enti e le aziende possono disporre di documenti standardizzati e approvati, mediante i quali è possibile garantire la compliance dei trattamenti dei dati personali ai principi e alla normativa privacy, in particolar modo per quanto concerne il trasferimento dei dati extra UE.

Il contenuto della Decisione in commento è piuttosto vario e ricco di spunti. L'intervento della Commissione Europea rappresenta uno strumento importante per tutti gli enti che, a prescindere dalle dimensioni, ricorrono al trasferimento dei dati personali fuori dall'ambito dell'UE e dello SEE, in quanto consente di effettuare tali trattamenti in piena conformità con il GDPR, senza "accontentarsi" di strumenti, quali ad esempio il consenso dell'interessato, troppo spesso sopravvalutato ma non idoneo, al contrario di quanto molti possano pensare.

[2] Lo scudo UE-USA per la privacy (in inglese EU-US **Privacy Shield**) è un accordo, dichiarato non valido dalla Corte di giustizia dell'UE il 16 luglio 2020, per gli scambi transatlantici di dati personali a scopo commerciale tra Unione europea e Stati Uniti d'America.

CAUSE DI SEPARAZIONE, LA CHAT È PROVA DEL TRADIMENTO SALVO UN DISCONOSCIMENTO «CHIARO, CIRCOSTANZIATO ED ESPLICITO»

Per far perdere in un processo la qualità di prova alle riproduzioni informatiche di una chat occorre un disconoscimento «**chiaro, circostanziato ed esplicito**», che si deve concretizzare «nell'allegazione di elementi attestanti la non corrispondenza tra realtà fattuale e realtà riprodotta». Sono quindi inefficaci i semplici richiami, fatti dal ricorrente, ai propri scritti difensivi nei quali dichiarava che quanto rappresentato dalle riproduzioni informatiche non corrispondesse alla realtà dei fatti in essa descritta.

Lo ha ribadito la Cassazione che, con l'ordinanza 12794 del 13 maggio 2021, ha confermato la centralità del deposito nel processo della famiglia delle riproduzioni informatiche di conversazioni via SMS, messaggi Email o Whatsapp: dai quali, nel caso esaminato dalla Cassazione, emergeva la relazione extraconiugale intrattenuta dal ricorrente, a cui i giudici del merito avevano addebitato la separazione.

Rientrano infatti tra le "riproduzioni" o "rappresentazioni" previste dall'articolo 2712 del Codice Civile, che riconosce queste come aventi valore di «piena prova dei fatti e delle cose rappresentate». A maggior ragione quando, come nel caso esaminato dalla Cassazione, i giudici del merito abbiano fondato il loro convincimento sugli ulteriori elementi costituiti dalla confessione stragiudiziale del ricorrente e sulle dichiarazioni dei testi, assunte durante l'istruttoria, che hanno confermato la realtà già rappresentata dalle "riproduzioni" della messaggistica depositate.

Nel caso esaminato, le contestazioni svolte con il ricorso alla Suprema Corte non hanno colto nel segno: il disconoscimento non ha raggiunto il requisito di legge. La contestazione svolta appare del tutto generica, si legge nell'ordinanza, e «carente di autosufficienza: infatti sono inammissibili, per violazione dell'articolo 366 Codice di procedura civile, n. 6, le censure fondate su atti e documenti del giudizio di merito qualora il ricorrente si limiti a richiamare tali atti e documenti, senza riprodurli nel ricorso ovvero, laddove riprodotti, senza fornire puntuali indicazioni necessarie alla loro individuazione (..) al fine di renderne possibile l'esame».

RANSOMWARE, +422% ATTACCHI IN AREA EMEA. ITALIA QUARTA TRA PAESI PIÙ COLPITI

L'Italia è quarta, poco sotto Regno Unito, Francia e Germania, per attacchi subiti da minacce ransomware nell'ultimo anno. Un ransomware è un tipo di malware che blocca l'accesso del dispositivo che infetta, richiedendo un riscatto da pagare per rimuovere la limitazione. I dati si evincono dalla classifica stilata da Mandiant, società parte dell'azienda di sicurezza informatica FireEye.

Nel nostro Paese, il trend di inviare e cadere nella trappola dei ransomware è in costante crescita. In tutta l'area Emea (che comprende Europa, Africa e Medio Oriente), proprio i ransomware rappresentano la tipologia di attacco cyber maggiormente in aumento, con un +422% tra febbraio 2020 e maggio 2021.

Per quanto concerne i settori presi di mira, il manifatturiero si conferma al primo posto, seguito dai servizi legali e professionali, retail e industria ingegneristica.

"I gruppi che operano attraverso attacchi ransomware continueranno a crescere fino a quando non inizieremo ad affrontare il problema a livello politico - ha spiegato Jens Monrad, Director, Head of Mandiant Intelligence, Emea - Rallentare queste attività criminali richiederà un livello di coinvolgimento che non abbiamo mai visto prima. Il cybercrime è una sfida globale e abbiamo necessità di segnalare e operare contro i paesi che offrono protezione ai cyber criminali o che accettano, con passività, le loro azioni, finché non colpiranno chi li ospita o li protegge".

DISABILI: DAL GOVERNO NUOVA BANCA DATI PER I PERMESSI ZTL, UN PASS VALIDO OVUNQUE. OK DAL GARANTE PRIVACY

ZTL DISABILI: NUOVA PIATTAFORMA INFORMATICA: Maggiore libertà di movimento per chi già soffre di enormi limitazioni legate alle diverse disabilità, ma anche semplificazione burocratica e tutti i vantaggi della transizione digitale in corso, a questo punta la nuova piattaforma (UNICA E NAZIONALE) annunciata dal Ministero delle Infrastrutture e della Mobilità Sostenibili (MIMS).

Grazie a questo servizio pubblico di rete, "unico e a carattere nazionale", sarà più agevole per le persone con disabilità titolari di contrassegni per l'auto spostarsi su tutto il territorio nazionale e accedere nelle zone a traffico limitato (ZTL) e nelle strade o corsie dove vigono divieti o limitazioni.

IL CUDE: alla piattaforma si aggiunge l'istituzione del CUDE (o Contrassegno Unico Disabili Europeo), che viene rilasciato dalla piattaforma stessa e con il quale è possibile muoversi liberamente in tutti i centri storici, accedere ad aree di sosta riservate ed attraversare luoghi a circolazione limitata in tutte le città d'Italia.

> "Questo decreto è fondamentale per rimuovere ostacoli e procedure che ad oggi ancora rappresentano un limite alla circolazione delle persone con disabilità. Gli strumenti digitali, ha affermato il Ministro delle Infrastrutture e della Mobilità Sostenibili Enrico Giovannini, possono migliorare la vita dei cittadini ed è importante che la Pubblica Amministrazione li utilizzi per semplificare e snellire pratiche e adempimenti. Con la piattaforma unica un cittadino diversamente abile non dovrà più preoccuparsi di chiedere l'autorizzazione a circolare nelle ZTL di Comuni diversi da quello di residenza, evitando così adempimenti ulteriori".

Invece che solo nel Comune di residenza, come accade oggi, il CUDE consentirà tranquillamente una nuova mobilità dedicata alle persone con disabilità ovunque nel Paese.

UN'APP PER COMUNICARE CON LA PIATTAFORMA: "Gli uffici comunali di ogni città italiana potranno verificare che la targa associata ad un contrassegno sia abilitata ad accedere nelle zone a traffico limitato", si legge nel comunicato del MIMS.

La persona titolare di contrassegno, inoltre, potrà comunicare direttamente alla piattaforma, in tempo reale attraverso un'app, eventuali nuove targhe di auto, diverse rispetto a quelle registrate.

PRIVACY AL SICURO: Un provvedimento atteso da diversi mesi, perché frutto di quanto stabilito nel decreto legge Semplificazioni, che necessitava appunto di un decreto attuativo, anticipato dall'accordo con le associazioni di settore delle persone con disabilità e previo il parere positivo del Garante privacy.

Cosa avvenuta nei giorni scorsi, con la Conferenza Unificata (Stato, Regioni e Enti locali) che ha approvato lo schema di decreto ministeriale predisposto dal MIMS, "di concerto con il Ministero dell'Economia e delle Finanze e con il Ministero dell'Interno e dopo aver consultato le associazioni delle persone con disabilità".

Fondamentale inoltre il parare favorevolmente del Garante per la protezione dei dati personali, perché si tratta di un data base in cui confluiscono i dati personali di decine di migliaia di cittadini italiani, che quindi andranno trattati in conformità con il GDPR.

Come detto, le disabilità sono diverse e il ministero ha stabilito un'altra novità importante: le persone con disturbi specifici dell'apprendimento (DSA) avranno più tempo per sostenere l'esame di teoria per la patente di guida e per il conseguimento della Carta di qualificazione del conducente (Cqc) per gli usi professionali con il supporto di strumenti compensativi.

Il Ministro Giovannini, venendo incontro alle richieste avanzate dalle associazioni di categoria, ha firmato il decreto che prevede un tempo più ampio per la prova di teoria ed estende al conseguimento della Cqc la possibilità per il candidato di chiedere l'ausilio di un file audio, possibilità già prevista per la patente di guida.

MOVIMENTO 5 STELLE: IL GARANTE PRIVACY ORDINA ALL'ASSOCIAZIONE ROUSSEAU DI CONSEGNARE I DATI DEGLI ISCRITTI

Il Garante per la protezione dei dati personali ha ordinato all'Associazione Rousseau di consegnare al Movimento 5 Stelle tutti i dati personali degli iscritti al Movimento. Il provvedimento è stato adottato d'urgenza all'esito dell'istruttoria avviata dal Garante dopo la segnalazione presentata dal Movimento 5 Stelle.

Dalla documentazione acquisita dall'Autorità, il Movimento e l'Associazione Rousseau risultano essere, rispettivamente, Titolare e Responsabile del trattamento dei dati degli iscritti al Movimento.

In base alla normativa sulla privacy, il Responsabile, "su scelta del Titolare del trattamento dei dati", è tenuto a cancellare o restituire tutti i dati personali, "dopo che è terminata la prestazione dei servizi richiesti relativi al trattamento". Questa disposizione, precisa il Garante, deve essere applicata in tutti i casi che regolano il rapporto Titolare-Responsabile.

In quanto Titolare del trattamento il Movimento ha quindi diritto, sottolinea il Garante, di disporre dei dati degli iscritti e di poterli utilizzare per i suoi fini istituzionali.

L'Associazione Rousseau dovrà quindi consegnare Movimento, entro 5 giorni, i dati degli iscritti di cui l'Associazione risulti Responsabile. Potrà invece continuare ad utilizzare i dati di quegli iscritti rispetto ai quali sia anche Titolare del trattamento.

GARANTE UE CHIEDE DI VIETARE IL RICONOSCIMENTO FACCIALE IN LUOGHI PUBBLICI

I due organismi che rappresentano i Garanti Europei, ovvero L'EDPS (European Data Protection Supervisor) e l'EDPB (European Data Protection Board), hanno unito le forze per chiedere il bando dell'utilizzo del riconoscimento facciale in luoghi pubblici. Il parere è in contrasto con la bozza del nuovo regolamento sull'Intelligenza Artificiale dell'Unione Europea, che propone invece l'uso in pubblico della tecnologia per motivi di sicurezza.

PROPOSTA GIÀ AD APRILE

Ad aprile la Commissione UE ha proposto un nuovo pacchetto di regole sull'intelligenza artificiale (già bocciata all'epoca dal Garante UE), che propone il bando di gran parte delle tecnologie di sorveglianza per mettere un freno e fissare un perimetro in un mercato, quello della sorveglianza e del controllo biometrico, dominato a livello globale da Cina e USA. Ma la proposta consente l'utilizzo di applicazioni di intelligenza artificiale ad alto rischio privacy. La proposta ora deve essere negoziata con gli Stati membri della UE e il regolatore europeo prima di diventare legge. Le due agenzie per la privacy, il Comitato europeo per la protezione dei dati (EDPB) e il Garante europeo per la protezione dei dati (EDPS), hanno messo in guardia sui rischi estremamente elevati posti dall'identificazione biometrica a distanza delle persone nelle aree pubbliche.

CHIESTO DIVIETO GENERALE

"L'EDPB e l'EDPS **chiedono un divieto generale** di qualsiasi uso dell'IA per il riconoscimento automatico di caratteristiche umane in spazi accessibili al pubblico, come il riconoscimento di volti, andatura, impronte digitali, DNA, voce, sequenze di tasti e altri segnali biometrici o comportamentali", hanno detto i due organismi in un parere congiunto. Nel loro parere le due agenzie hanno altresì affermato che anche i sistemi di intelligenza artificiale che utilizzano la biometria per classificare gli individui in gruppi in base a etnia, genere, orientamento politico o sessuale **dovrebbero essere vietati**. Anche l'uso della tecnologia per dedurre le emozioni di una persona dovrebbe essere vietato, tranne che in casi molto specifici, come per motivi di salute.

PARERE NON VINCOLANTE, MA IMPONENTE

Sebbene il parere non sia vincolante, ha un certo "peso" presso la Commissione, i paesi dell'UE e il Parlamento Europeo.

TELEMARKETING: NECESSARIO ACQUISIRE IL CONSENSO PER CIASCUN PASSAGGIO DEI DATI TRA PIÙ TITOLARI. IL GARANTE SANZIONA IREN

Il consenso, inizialmente rilasciato da un cliente ad una società anche per attività promozionali di terzi, non può estendere la sua efficacia anche a successive cessioni ad ulteriori Titolari.

Tali cessioni infatti non sarebbero supportate dal necessario consenso, specifico ed informato dell'interessato. Sulla base di questo principio, il Garante per la protezione dei dati personali ha comminato una **sanzione di circa 3 milioni di euro ad IREN Mercato S.p.A**., società operante nel settore energetico, per non aver verificato che tutti i passaggi dei dati dei destinatari delle promozioni fossero coperti da consenso.

A seguito di diversi reclami e segnalazioni il Garante ha accertato che la società aveva infatti trattato dati personali per attività di telemarketing, che non aveva raccolto direttamente, ma che aveva acquisito da altre fonti. IREN infatti aveva ottenuto liste di anagrafiche da una S.r.l., che a sua volta le aveva acquisite, in veste di autonomo Titolare del trattamento, da altre due aziende. Queste ultime società avevano ottenuto il consenso dei potenziali clienti per il telemarketing effettuato sia da loro che da parte di terzi, ma tale consenso non copriva anche il passaggio dei dati dei clienti dalla S.r.l. all'IREN.

L'ammontare della sanzione applicata dal Garante, è stato motivato anche dal fatto che le liste anagrafiche, prive di tutti i consensi necessari e di cui il Garante ha vietato ogni ulteriore utilizzo a fini promozionali, riguardavano diversi milioni di persone. L'Autorità ha infine rivolto un avvertimento alla società per aver fornito una rappresentazione ed una documentazione probatoria incompleta ed inidonea durante l'istruttoria.