News gennaio 2021

Responsabile scientifico: prof. Lorenzo Picotti - monitoraggio a cura di Chiara Crescioli, Beatrice Panattoni e Rosa Maria Vadalà

NOVITÀ SOVRANAZIONALI

1. Linee guida del Consiglio d'Europa sul riconoscimento facciale

La Commissione della Convenzione del Consiglio d'Europa n. 108 del 1981 in materia di protezione dei dati personali oggetto di trattamento elettronico, ha elaborato delle linee guida che forniscono un insieme di misure volte a garantire e proteggere i diritti umani fondamentali che potrebbero venire violati attraverso l'utilizzo di tecnologie di riconoscimento facciale (comprese anche quelle *live*). Il documento si rivolge quindi a legislatori, sviluppatori e produttori, nonché utilizzatori di tali tecnologie. Per quanto riguarda i legislatori, viene suggerita l'opportunità di prevedere una disciplina normativa che regolamenti il lecito trattamento di dati biometrici attraverso l'utilizzo delle tecnologie di riconoscimento facciale. Inoltre, determinati usi di queste tecnologici dovrebbero venire vietati, come l'utilizzo al solo scopo di determinare la condizione sanitaria o sociale, l'etnia, l'età, il genere o l'appartenenza religiosa di una persona, salva la previsione di apposite salvaguardie che evitino ogni rischio di discriminazione. Un particolare paragrafo è inoltre dedicato all'utilizzo delle tecnologie di riconoscimento facciale da parte dell'autorità pubblica. Per quanto riguarda invece gli sviluppatori e i produttori di tali tecnologie, le linee guida si concentrano sui requisiti che devono caratterizzare i *datasets* utilizzati dai sistemi di riconoscimento facciale e su alcune delle misure a cui tali attori privati potrebbero dover conformarsi per garantire il rispetto della protezione dei dati personali sensibili trattati. Per quanto concerne infine gli utilizzatori di tali tecnologie, essi devono essere in grado di dimostrare la stretta necessarietà e proporzionalità dell'utilizzo, garantendo che il trattamento dei dati biometrici sia trasparente, equo e sicuro.

Guidelines on Facial Recognition

2. I pareri congiunti EDPB-GEPD sulle clausole contrattuali standard per il trasferimento di dati personali a paesi terzi

In seguito alla sentenza Schrems II della CGUE (v. topic Privacy), il Comitato Europeo per la protezione dei dati personali (EDPB) e il Garante Europeo per la protezione dei dati personali (GEPD) hanno adottato pareri congiunti su due serie di clausole contrattuali standard (SCC) predisposte dalla Commissione UE. Il primo è relativo alle clausole contrattuali nei contratti tra titolari del trattamento e responsabili del trattamento ai sensi dell'art. 28 GDPR, il secondo, invece, riguarda le SCC per i trasferimenti di dati personali al di fuori della UE. Le nuove SCC per il trasferimento di dati personali verso paesi terzi ai sensi dell'art. 46 (2) (c) GDPR sostituiranno le SCC esistenti per i trasferimenti internazionali per renderle conformi ai requisiti introdotti dal GDPR, prevedendo salvaguardie più specifiche nel caso in cui le leggi del paese di destinazione influiscano sul rispetto delle clausole. Sia L'EDPB che il GEPD hanno accolto favorevolmente le nuove SCC, ma hanno sostenuto l'opportunità di adottare diverse modifiche rispetto alle bozze precedentemente pubblicate dalla Commissione europea. In particolar modo con riferimento alla c.d. "*clausola di docking*", che consente a qualsiasi entità di accedere alle SCC già stipulate diventando una nuova parte contrattuale in qualità di titolare o responsabile del trattamento, hanno sottolineato che è opportuno delimitare la ripartizione delle responsabilità nonché indicare chiaramente quale trattamento sia effettuato da un determinato responsabile, per conto di quale titolare e per quali scopi. Inoltre, l'EDPB e il GEPD suggeriscono che in generale gli allegati alle SCC chiariscano il più possibile i ruoli e le responsabilità di ciascuna delle parti in relazione a ciascuna attività di trattamento per facilitare ai titolari del trattamento o ai responsabili del trattamento l'adempimento dei propri obblighi. Inoltre, da migliorare o chiarire sono anche le disposizioni relative agli obblighi in materia di trasferimenti ulteriori, alla notifica all'Autorità Garante nonché agli aspetti sulla valutazione della legge del paese terzo in materia di accesso ai dati da parte della autorità pubbliche.

Parere congiunto n. 1/2021 EDPB-GEPD sulle clausole contrattuali standard

Parere congiunto n. 2/2021 EDPB-GEPD sulle clausole contrattuali standard

3. Linee guida per l'uso dell'Intelligenza artificiale in campo civile e militare

Nella Risoluzione approvata il 20 gennaio 2021, il Parlamento Europeo ha evidenziato la necessità di disporre di un quadro giuridico europeo comune, con definizioni armonizzate e principi etici comuni, anche per l'utilizzo dell'intelligenza artificiale a fini civili e militari. In Particolare, propone alla Commissione UE di adottare la seguente definizione di sistema d'Intelligenza artificiale: "*un sistema basato su software o integrato in dispositivi* hardware *che mostra un comportamento che simula l'intelligenza, tra l'altro raccogliendo e trattando dati, analizzando e interpretando il proprio ambiente e intraprendendo azioni, con un certo grado di autonomia, per raggiungere obiettivi specifici*". Inoltre, ritiene che l'IA utilizzata in un contesto militare e civile debba essere soggetta ad un significativo controllo umano, in modo tale che in qualsiasi momento la persona umana abbia i mezzi per correggerla, bloccarla o disattivarla in caso di comportamento imprevisto, intervento accidentale, attacchi informatici o interferenza di terzi con tecnologie basate sull'IA o qualora terzi acquisiscano tale tecnologia. Per quanto riguarda in particolare il settore giudiziario, il Parlamento ritiene che l'utilizzo dell'IA nel contrasto alla criminalità e alla cybercriminalità possa offrire un'ampia gamma di possibilità e opportunità, ma ribadisce la necessità che anche qualora le decisioni inerenti all'applicazione della legge siano in parte delegate all'IA, è sempre necessario mantenere un controllo umano sulla decisione finale.

Risoluzione del Parlamento europeo del 20 gennaio 2021 sull'intelligenza artificiale

4. Il diritto alla disconnessione

Il 21 gennaio 2021 il Parlamento europeo ha approvato una risoluzione contenente raccomandazioni alla Commissione sul "diritto alla disconnessione" (*right to disconnect*), dove per "disconnessione" si intende, secondo il testo della proposta legislativa allegato alla risoluzione, "*il mancato esercizio di attività o comunicazioni lavorative per mezzo di strumenti digitali, direttamente o indirettamente, al di fuori dell'orario di lavoro*".
Considerato infatti l'utilizzo sempre maggiore degli strumenti digitali a scopi lavorativi, esponenzialmente aumentato durante la pandemia e il ricorso allo *smart working* che flessibilizza l'orario, il luogo e il modo in cui il lavoro può essere svolto, è emersa una cultura del "sempre connesso" a scapito dei diritti fondamentali dei lavoratori. Dal momento che attualmente non esiste una specifica normativa europea sul diritto dei lavoratori alla disconnessione dagli strumenti digitali a scopi lavorativi, con questa risoluzione il Parlamento europeo invita la Commissione a presentare un quadro legislativo al fine di stabilire i requisiti minimi sul lavoro a distanza in tutta l'Unione Europea, precisando, integrando e rispettando i requisiti già previsti nelle direttive 2003/88/CE (sul diritto alle ferie annuali retribuite), 2019/1152/UE (sulle condizioni di lavoro trasparenti e prevedibili), 2019/1158/UE (sull'equilibrio tra attività professionale e vita familiare per i genitori e i prestatori di assistenza), nonché 89/391/CEE del Consiglio sulla sicurezza e la salute dei lavoratori.

Risoluzione del Parlamento europeo del 21 gennaio 2021 recante raccomandazioni alla Commissione sul diritto alla disconnessione (2019/2181(INL))

5. Competenza dell'autorità di controllo nazionale in caso di trattamento transfrontaliero dei dati

Nell'ambito della Causa C-645/19 (Facebook Ireland Limited, Facebook Inc., Facebook Belgium BVBA contro Gegevensbeschermingsautoriteit), la Corte d'appello di Bruxelles ha sottoposto alla Corte di Giustizia europea una questione pregiudiziale con cui chiede se il Regolamento europeo sulla protezione dei dati personali (GDPR) consenta all'autorità di controllo di uno Stato membro di agire in sede giudiziale dinanzi a un giudice di tale Stato per una presunta violazione del GDPR riguardo ad un trattamento transfrontaliero dei dati, anche se essa non è l'"autorità di controllo capofila", individuata secondo il meccanismo dello "sportello unico" (cfr. considerando 127, art. 56 § 1 e art. 4 punto 22 GDPR). Nelle sue conclusioni, l'avvocato generale Bobek ritiene che, fatta salva la competenza generale dell'autorità capofila sul trattamento transfrontaliero, l'autorità di controllo, che non è l'autorità capofila, può agire in sede giudiziale riguardo al trattamento transfrontaliero solamente in uno dei casi in cui il GDPR le conferisce specificatamente competenze a tal fine

(come i casi previsti dall'art. 55 § 2 GDPR o il caso in cui il titolare del trattamento non abbia alcuno stabilimento nell'Unione, o in casi di urgenza) e secondo le corrispondenti procedure.

Conclusioni dell'Avvocato Generale Michal Bobek nella causa C-645/19

NOVITÀ LEGISLATIVE E NORMATIVE NAZIONALI

1. I provvedimenti del Garante per la protezione dei dati personali verso i *social network*s

Con il provvedimento n. 20 del 22 gennaio 2021 il Garante per la protezione dei dati personali, viste le violazioni del GDPR contestate a Tik Tok nel procedimento già aperto dal Garante con nota del 15 dicembre 2020, ha disposto, ai sensi dell'art. 58, par. 2, lett. f) e 66, par. 1 del GDPR (che permette in casi d'urgenza di derogare al meccanismo di cooperazione con le autorità europee per l'applicazione coerente in tutta l'Unione ai sensi dell'art. 63 del GDPR), nei confronti del *social network,* la misura della limitazione provvisoria del trattamento, vietando l'ulteriore trattamento dei dati degli utenti che si trovano sul territorio italiano per i quali non vi sia assoluta certezza dell'età e, conseguentemente, del rispetto delle disposizioni collegate al requisito anagrafico. In un successivo comunicato stampa, il Garante ha dato atto della comunicazione ricevuta da Tik Tok, che ha affermato di voler adottare misure per bloccare l'accesso agli utenti minori di 13 anni (bloccando tutti gli utenti italiani a partire dal 9 febbraio e chiedendo di indicare nuovamente la data di nascita), la cui età potrebbe venire verificata anche attraverso l'utilizzo di sistemi di intelligenza artificiale. Rispetto all'effettiva efficacia delle singole misure, il Garante si riserva comunque successive verifiche.
Infine, il Garante ha aperto dei procedimenti anche nei confronti di Facebook, che controlla anche Instagram, chiedendo informazioni sulle modalità di iscrizione ai social e sulle verifiche dell'età dell'utente adottate per controllare il rispetto dell'età minima di iscrizione.

Provvedimento n. 20 del 22 gennaio 2021

Comunicato stampa del 27 gennaio 2021

2. Il Consiglio di Stato dà parere favorevole sulla disciplina del Comitato e della sperimentazione FinTech

Il Consiglio di Stato, con questo provvedimento, ha reso parere favorevole sullo schema di decreto del Ministro dell'economia e finanze, recante attuazione dell'art. 36, commi 2-bis e seguenti, d.l. 30 aprile 2019, n. 34, convertito, con modificazioni, dalla l. 28 giugno 2019, n. 58, il quale intende consentire ai soggetti che svolgono o intendono svolgere attività FinTech di usufruire, per un periodo transitorio, di un regime semplificato, consentendo, al contempo, al regolatore e alle autorità di vigilanza di osservare e monitorare il fenomeno.
Tra le osservazioni svolte dal Consiglio di Stato, è stata richiesta la riformulazione della definizione di FinTech quali "*attività volte al perseguimento, mediante nuove tecnologie quali l'intelligenza artificiale e i registri distribuiti, dell'innovazione di servizi e di prodotti nei settori bancario, finanziario, assicurativo e dei mercati regolamentati*".

Con riferimento, poi, all'ammissione alla sperimentazione anche di soggetto avente sede legale in un altro Stato membro dell'Unione europea e operante in Italia in regime di libera prestazione di servizi, richiamando la Comunicazione della Commissione europea 24.9.2020 COM(2020) 591 final (consultabile in questo Osservatorio al Topic FinTech) e il parere negativo sul punto espresso dalla Consob, il Consiglio di Stato ha invitato l'Amministrazione ad introdurre nel decreto apposite disposizioni volte a sviluppare le opportune ed efficaci forme di coordinamento e collaborazione tra le diverse Autorità nazionali dei Paesi dell'Unione Europea, a tutela dei consumatori e degli investitori. Sempre a tutela di questi ultimi, per garantirne il tempestivo risarcimento, laddove dovessero essere danneggiati dall'operato dei prestatori ammessi alla sperimentazione, ha altresì richiesto che tale ammissione sia subordinata al possesso di una adeguata garanzia finanziaria o assicurativa.

Consiglio di Stato, sez. atti norm., 29 gennaio 2021, n. 109, Pres. Troiano - Est. Prosperi

3. Abusivismo finanziario e provvedimenti Consob di oscuramento siti web

L'Autorità, avvalendosi dei poteri derivanti dal "decreto crescita" (art. 36, comma 2-terdecies d.l. 30 aprile 2019 n. 34 convertito con modificazioni dalla legge n. 58 del 28 giugno 2019), in base ai quali può ordinare ai fornitori di servizi di connettività *Internet* di inibire l'accesso dall'Italia ai siti web tramite cui vengono offerti servizi finanziari senza la dovuta autorizzazione, ha disposto nel solo mese di gennaio 2021 l'oscuramento di 14 siti *web*.
Dal 2019 ad oggi il numero dei siti oscurati degli intermediati finanziari abusivi è di 368.

I provvedimenti adottati dalla Consob sono consultabili sul sito dell'Autorità www.consob.it.

4. L'incremento del deposito telematico degli atti del procedimento penale

Con il D.M. 13 gennaio 2021, pubblicato il 21 gennaio 2021 in Gazzetta Ufficiale e in vigore dal 5 febbraio 2021, è stato ampliato il novero degli atti del procedimento penale per cui è prevista l'obbligatorietà del deposito in modalità telematica, rispetto a quelli già indicati nel d.l. n. 137/2020. In particolare, il nuovo obbligo riguarda le opposizioni all'archiviazione, le denunce e le querele dei privati con relative procure speciali, nonché le nomine, le rinunce e le revoche dei difensori di fiducia.

Decreto del Ministero della Giustizia del 13 gennaio 2021

NOVITÀ GIURISPRUDENZIALI NAZIONALI

1. L'invio massiccio di *e-mail* contenenti insulti e minacce integra il reato di atti persecutori

Con questa sentenza la Suprema Corte chiarisce che il reiterato invio di messaggi di posta elettronica, contenenti insulti e minacce costituisce una condotta invasiva, di per sé idonea a determinare uno degli eventi previsti dall'art. 612-*bis* c.p., nel caso in esame individuato nel timore della persona offesa per l'incolumità propria e dei propri familiari. Infatti, tale fattispecie non può essere assimilata al reato di molestie ex art. 660 c.p., poiché ha una diversa oggettività giuridica e presidia beni diversi; infatti per l'integrazione del delitto di atti persecutori non è necessario che le condotte invasive debbano rispettare i parametri nomativi di cui all'art. 660 c.p., che richiede l'uso del telefono, modalità di veicolazione delle molestie che invece è estranea al delitto di atti persecutori, che può riguardare qualsiasi condotta dotata di una portata invasiva e persecutoria.
I giudici di legittimità precisano poi che l'invio di messaggi di posta elettronica ha senz'altro natura invasiva, trattandosi di un sistema di comunicazione che è parte integrante della quotidianità delle persone, anche grazie al fatto che l'accesso alla propria casella di posta elettronica è oggi possibile anche da *smartphone* e *tablet* e non richiede di utilizzare necessariamente un *computer*. Pertanto, l'invio ripetuto, anche da indirizzi diversi di posta elettronica, di *mail* dal contenuto gravemente offensivo e minatorio nei confronti della persona offesa, costretta a subire tale mole di messaggi, costituisce non solo una condotta assimilabile a quella prevista dalla fattispecie penale di cui all'art. 612-*bis* c.p., ma anche un comportamento idoneo a determinare uno degli eventi previsti dalla stessa fattispecie. Non rileva che il destinatario possa cancellarle o evitare di leggerle, perché l'invasività di una condotta non è data dall'effettiva o potenziale possibilità che la persona offesa attui dei meccanismi di difesa per arginarne gli effetti. Infatti, quando ciò avviene la condotta ha già esaurito la propria portata violativa dell'altrui sfera individuale, pregiudicata dal fatto di dover predisporre dei meccanismi di difesa. Inoltre, al danno della ricezione di una pluralità di mail contenenti insulti e minacce, si aggiunge peraltro anche quello di dover effettuare una cernita preventiva prima di comprendere la destinazione, venendo così ulteriormente pregiudicata la libertà morale della persona offesa.

In senso conforme: Corte di Cassazione, sez. VI penale, sentenza 30 agosto 2010 (ud. 16 luglio 2010) n. 32404/2010 - Pres. De Roberto, Rel. Colla

Corte di Cassazione, sez. V penale, sentenza 13 gennaio 2021 (ud. 18 dicembre 2020), n. 1223/2021 - Pres. Miccoli, Rel. Riccardi

2. Truffe *online* e la circostanza aggravante della minorata difesa

Non è applicabile l'aggravante della minorata difesa, ai sensi dell'art. 61, n. 5 c.p., nell'ipotesi di truffa commessa attraverso la vendita di prodotti on-line quando la trattativa prenda avvio dall'ostensione di un bene su una piattaforma telematica, ma poi si sviluppi attraverso contatti telefonici e incontri in presenza.
In queste condizioni i contraenti risultano esposti a ordinarie azioni fraudolente, che non risultano agevolate dalla condizione di minorità in cui è posta la vittima di truffe contrattuali che si consumano attraverso trattative svolte interamente "a distanza", su piattaforme web.

Per approfondire: LEPERA M., *Un caso di reato semplice scambiato per reato circostanziato: sull'improbabile configurabilità dell'aggravante della "minorata difesa" in relazione alle truffe on-line*, in *Cass. Pen.*, 2017, n. 2, p. 687 ss.; CAJANI F., *Le truffe on line*, in PARODI C. (a cura di), *Diritto penale dell'impresa*, Milano, 2017, p. 573 ss.; PECORELLA C.-DOVA M:, *Profili penali delle truffe on line*, in *Arch. Pen.*, 2013, n. 3, p. 799 ss; CIPOLLA P., *E-commerce e truffa*, in *Giur. merito*, 2013, n. 3, p. 2624 ss..

Conformi: Corte di Cassazione, sez. VI penale, sentenza 22 aprile 2017 (ud. 22 marzo 2017), n. 17937/2017 - Pres. Rotundo, Rel. Criscuolo.

Corte di Cassazione, sez. II penale, sentenza 13 gennaio 2021, (ud. 14 ottobre 2020) n. 1086/2021 - Pres. Verga, Rel. Recchione

3. Il *locus commissi delicti* del reato di diffamazione a mezzo Internet

In caso di diffamazione commessa a mezzo Internet la Corte di Cassazione conferma che il giudice naturale va individuato in forza del criterio del luogo di domicilio dell'imputato, in applicazione della regola suppletiva stabilita dall'art. 9 c. 2 c.p.p., sostenendo che la competenza si sarebbe, peraltro, radicata presso lo stesso Tribunale anche applicando il criterio di cui al primo comma dell'art. 9 c.p.p., riprendendo quella giurisprudenza della Corte secondo cui nei reati di diffamazione tramite la rete Internet, ove sia impossibile stabilire il luogo di consumazione del reato e sia stato invece individuato quello in cui il contenuto diffamatorio è stato caricato come dato informatico, per poi essere immesso in rete, la competenza territoriale va determinata in relazione al luogo predetto, in cui è avvenuta una parte dell'azione.

In senso conforme: Corte di Cassazione, sez. V penale, sentenza 22 febbraio 2017 (ud. 23 gennaio 2017), n. 8482/2017 - Pres. Palla, Rel. Catena; Corte di Cassazione, sez. I penale, sentenza 26 aprile 2011 (ud. 15 marzo 2011), n. 16307/2011 - Pres. Siotto, Rel. Pieraccini.

Corte di Cassazione, sez. V penale, sentenza 12 gennaio 2021 (ud. 23 novembre 2020), n. 854/2021 - Pres. Catena, Rel. Romano

CONTRIBUTI DOTTRINALI DI RILIEVO

Sistema penale

CANZIO G., *Intelligenza artificiale, algoritmi e giustizia penale*

DELAITI F., *Cripto-valute e abusivismo finanziario: cripto-analogia o interpretazione estensiva?*

PITTIRUTI M., *Dalla Corte di cassazione un vademecum sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali omnibus*

☞ **Per accedere alle newsletter dei mesi precedenti clicca qui**