Le prime sanzioni delle Autorità di controllo a seguito dell'entrata in vigore del Regolamento UE 2016/679

di Filippo Lorè

Sommario

1. Cenni sul ruolo delle Autorità di controllo e sulle sanzioni previste dal Regolamento UE 2016/679 (RGPD).

Le disposizioni previste dal legislatore europeo richiedono, in ottica accountability, un cambio di prospettiva nell'applicazione dei principi della normativa in materia di protezione dei dati personali, chiamando gli attori principali ad una svolta di natura culturale, accantonando l'atteggiamento formale nei confronti della materia, a favore di un approccio di natura sostanziale, sostenuto dall'implementazione di misure tecniche ed organizzative allo scopo di tutelare le libertà fondamentali degli interessati. Prima di considerare l'impianto sanzionatorio previsto dal Regolamento UE 2016/679, è opportuno considerare il ruolo demandato alle Autorità di controllo.

Il Regolamento generale sulla protezione dei dati, oggi, all'art. 51 prevede, per ogni Stato membro, che ad una o più autorità pubbliche sia demandato il compito di sorvegliare l'applicazione del RGPD al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento delle informazioni e di agevolare la libera circolazione dei dati personali all'interno dell'Unione. Il diritto primario dell'Unione, muovendo i passi anche dalla riforma del Trattato di Lisbona[1], stabilisce e rafforza il ruolo delle Autorità indipendenti alle quali è demandato il compito di verificare la corretta applicazione della normativa rilevante a tutela della riservatezza degli individui. In considerazione della rilevanza che il diritto alla protezione dei dati personali assurge per i diritti fondamentali delle persone fisiche, le Autorità di controllo, così come richiamato dall'art. 8, paragrafo 3, della Carta dei diritti fondamentali dell'UE e dall'articolo 16, paragrafo 2, del TFUE, divengono custodi, organi deputati al rispetto delle disposizioni contenute nella disciplina rilevante in materia di privacy e, contestualmente, prezioso punto di contatto per gli interessati in caso di violazioni che impattano sulle libertà dei cittadini[2]. Le attuali

[1] B. Nascimbene, *Lo Stato di diritto e la violazione grave degli obblighi posti dal Trattato UE*, 2017, Eurojus.it rivista.

[2] CGUE, C-362/14, M. Schrems c. Data Protection Commissioner, 6 ottobre 2015.

disposizioni del diritto dell'Unione europea prescrivono che ogni Autorità, nell'assolvimento dei propri compiti istituzionali, debba operare secondo il principio di indipendenza, elemento cardine richiamato dallo stesso Regolamento europeo 2016/679, all'art. 69, rafforzato, successivamente dalla Convenzione n. 108 modernizzata che raccomanda il pieno esercizio delle funzioni delle Autorità, senza alcun condizionamento[3]. Le Autorità di controllo, quindi, adottano azioni tese alla cooperazione, assicurandosi assistenza reciproca, anche in fase di indagine e di ingiunzione di misure correttive, garantendo l'applicazione del Regolamento in maniera coerente, anche attraverso la funzione di garanzia esercitata dal Comitato europeo per la protezione dei dati personali, successore del Gruppo di lavoro articolo 29, considerato, ai sensi degli artt. 64, 65 e 70 del Regolamento, organismo cui sono affidate decisioni giuridicamente vincolanti, pareri sulle richieste di consulenza esercitate dalla Commissione per tematiche inerenti la protezione dei dati personali, e, non in ultimo, la pubblicazione di linee guida, raccomandazioni e buone prassi finalizzate alla promozione della corretta applicazione del Regolamento generale. Con riferimenti ai compiti delle Autorità di controllo chiamate a sorvegliare e assicurare l'applicazione del Regolamento[4], l'art. 57 prevede tra i poteri correttivi[5], nel caso della normativa nazionale italiana richiamati anche dagli artt. 154-*bis* e seguenti del D.Lgs n. 196/2003 e ss.mm.ii., specifiche azioni, quali l'avvertimento al titolare o al responsabile del trattamento, nel caso in cui i trattamenti posti in essere violino espressamente le disposizioni del RGPD; l'ammonimento, inteso quale strumento *soft*, nei confronti dei soggetti che si siano resi protagonisti di una violazione; l'ingiunzione di soddisfare le richieste dell'interessato di esercitare i diritti conoscitivi e di controllo richiamati dal RGPD e di conformare i trattamenti alle disposizioni del legislatore europeo entro un determinato termine; l'ingiunzione di comunicare all'interessato una violazione dei dati; l'imposizione di una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento; l'ordine di rettifica, cancellazione di dati personali o limitazione del trattamento a norma degli artt. 16, 17 e 18 RGPD[6]; l'inflizione di una sanzione amministrativa pecuniaria ai sensi dell'art. 83 RGPD, in aggiunta o in luogo delle altre misure, in funzione delle circostanze di ogni singolo caso. Proprio l'art. 83 RGPD configura l'impianto sanzionatorio stabilendo che le ingiunzioni debbano essere effettive, proporzionate e dissuasive[7]. I paragrafi 4, 5 e 6 dell'art. 83 specificano queste sanzioni. È soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 di Euro, o

[3] Convenzione n. 108 modernizzata, art. 15, paragrafo 5, "…*The supervisory authorities shall act with complete independence and impartiality in performing their duties and exercising their powers and in doing so shall neither seek nor accept instructions*"

[4] M. Barbarossa, C. Benvenuto, V. Ceriocchi, *Il processo di adeguamento al GDPR, Giuffrè Francis Lefebvre, pp.373-375, 2018*

[5] G. Busia, *Persona e mercato dei dati. Riflessioni sul GDPR*, Cedam Editore, pp. 298-300, 2019

[6] G. Finocchiaro, A. Ricci, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli Editore, Capitolo 4, pp.179-195, 2017

[7] Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa, *Manuale sul diritto europeo in material di protezione dei dati, pp. 273-276, 2018*

per le imprese, fino al 2 % del fatturato mondiale totale annuo, se superiore, la violazione delle disposizioni seguenti: a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43; b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43; c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4. È invece soggetta a sanzioni amministrative pecuniarie più elevate, fino ad euro 20 milioni, o per le imprese, fino al 4 % del fatturato mondiale annuo, se superiore, la violazione delle disposizioni riguardanti: a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9 RGPD; b) i diritti degli interessati a norma degli articoli da 12 a 22; c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49 RGPD; d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX; e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, RGPD o il negato accesso in violazione dell'articolo 58, paragrafo 1. Con la stessa sanzione è punita l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2[8]. Con riferimento al contesto nazionale, il legislatore europeo in materia di protezione dati personali, all'art. 84 del Regolamento generale 2016/679, lascia aperta la possibilità per gli Stati membri di prevedere ulteriori sanzioni, per le violazioni non soggette a sanzioni amministrative pecuniarie richiamata dall'art. 83, purché queste ultime conservino i requisiti di effettività, dissuasività e proporzionalità. Proprio in virtù di tale facoltà, il decreto di armonizzazione delle leggi nazionali al Regolamento europeo stabilisce, nella Parte III, Titolo III, del Codice in materia di protezione dei dati personali, ulteriori fattispecie che possono dar luogo ad una condotta illecita nei confronti dei protagonisti della normativa privacy. Nello specifico, l'art. 166, comma 1, del Codice privacy prevede una serie di specifiche casistiche per le quali le sanzioni possono essere inflitte nell'ammontare di euro 10 milioni o fino al 2% del fatturato dell'impresa, mentre al comma 2 dello stesso articolo, vengono elencate le sanzioni fino ad euro 20 milioni o fino 4 % del fatturato. Pur non essendo espressamente previste nel disposto normativo europeo in materia di protezione dei dati personali, lo stesso legislatore, nella stesura del Considerando 149 al RGPD[9], lascia salva la facoltà per gli Stati membri di introdurre sanzioni penali, possibilità raccolta dal legislatore italiano, con l'espressa disposizione degli artt. 167, 167-*bis*, 167-*ter*, 168 e 170 del Codice privacy[10] che

[8] G.M. Riccio, G. Scorza, E. Bellisario, *GDPR e normativa privacy commentato*, Ipsoa Editore, pp. 613-620, 2018

[9] Considerando 149 al Regolamento UE 2016/679, "*Gli Stati membri dovrebbero poter stabilire disposizioni relative a sanzioni penali per violazioni del presente regolamento, comprese violazioni di norme nazionali adottate in virtù ed entro i limiti del presente regolamento. Tali sanzioni penali possono altresì autorizzare la sottrazione dei profitti ottenuti attraverso violazioni del presente regolamento. Tuttavia, l'imposizione di sanzioni penali per violazioni di tali norme nazionali e di sanzioni amministrative non dovrebbe essere in contrasto con il principio del ne bis in idem quale interpretato dalla Corte di giustizia*"

[10] A.G. Paris, *Il Codice della Privacy*, Pacini Giuridica, pp. 867-917, 2019

puniscono i trasgressori con la previsione di sanzioni di natura penale[11]. È opportuno, quindi, allora analizzare sinteticamente le motivazioni che hanno indotto i Garanti nazionali a sanzionare i comportamenti (e in alcuni casi le omissioni) dei titolari e dei responsabili del trattamento.

2. Brevi casistiche di violazioni conseguenti all'errata individuazione della base giuridica del trattamento

Come noto, l'art. 5 paragrafo 1 del Regolamento generale sulla protezione dei dati personali rappresenta un punto cardine della stessa normativa europea e stabilisce, nella sua formulazione, che le informazioni di natura personale debbano essere trattate anche in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»). Con espresso riferimento alla "liceità del trattamento", l'art. 6 RGPD, al paragrafo 1, elenca tassativamente le possibili basi giuridiche che legittimano un trattamento di dati personali. Numerosi, a tal riguardo, risultano essere le sanzioni, conseguenti alla verifica della base giuridica del trattamento, irrogate dai Garanti nazionali. La Commissione per la protezione dei dati personali bulgara (KZLD[12]), grazie alla segnalazione di un utente che lamentava la modifica unilaterale del contratto di telefonia mobile, ha avviato una indagine nei confronti di un'azienda di telecomunicazioni che eseguiva operazioni di trattamento sui dati personali degli interessati, prescindendo dall'individuazione di una corretta base giuridica, in un contesto operativo, all'interno del quale i dipendenti dell'azienda eseguivano operazioni di trattamento sui dati personali degli abbonati per finalità ulteriori, rispetto a quelle per le quali gli stessi erano stati raccolti, senza alcuna ulteriore acquisizione del consenso informato[13]. Prendendo sempre quale riferimento le condizioni di liceità del trattamento, l'Autorità di controllo belga (DPA) ha irrogato la sua prima sanzione[14], nel quantum di 2.000 euro, considerato l'esiguo numero di interessati colpiti, la gravità e la durata dell'illecito, ad un sindaco per trattamento illecito di dati personali utilizzati per scopi elettorali. Il primo cittadino, secondo l'Autorità di controllo, pur avendo inizialmente raccolto gli indirizzi di posta elettronica dei cittadini nell'ambito di un progetto di pianificazione urbana, non si sarebbe attenuto, successivamente, alle disposizioni contenute nell'art. 5, paragrafo 1, lett. b), dalla cui lettura si evince il principio di limitazione delle finalità[15], riutilizzando, all'uopo, le informazioni personali nella propria disponibilità con lo scopo di contattare gli interessati durante la campagna elettorale. Stessa sorte, in occasione delle elezioni politiche regionali, toccava ad un medico, cui il Garante

[11] M. Iaselli, *Sanzioni e responsabilità in ambito GDPR*, Giuffrè Francis Lefebvre, pp. 84-85, 2019

[12] *Комисия за защита на личните данни*, Commissione per la protezione dei dati personali

[13] In https://www.cpdp.bg/

[14] In https://www.autoriteprotectiondonnees.be/news/lautorite-de-protection-des-donnees-prononce-une-sanction-dans-le-cadre-dune-campagne

[15] C. Cominotto, *I principi alla base del nuovo trattamento dati*, Diritto24, Il Sole 24 ore, http://www.diritto24.ilsole24ore.com/art/dirittoCivile/2016-07-21/i-principi-base-nuovo-trattamento-dati-164452.php

per la protezione dei dati personali italiano, tenendo fermi i principi contenuti nel Provvedimento generale in materia di propaganda elettorale del 6 marzo 2014[16], ha inflitto una sanzione di 16.000 euro per aver inviato delle missive a circa 3.500 ex-pazienti per manifestare il sostegno politico ad un candidato politico impegnato nella gara elettorale. L'Autorità di controllo italiana, conclusa la fase istruttoria, scaturita dall'evidenza di alcuni articoli di stampa che segnalavano la vicenda, ha giudicato illecito il trattamento di dati personali di pazienti per finalità differente rispetto a quella di cura, per la quale si sarebbe resa necessaria l'acquisizione di specifico ed autonomo consenso informato. L'Autorità di controllo francese[17], invece, ha sanzionato[18] per un importo pari a 20.000 euro, una Società che aveva posto i suoi dipendenti sotto costante videosorveglianza, senza fornire adeguata informativa e senza previsione di alcuna misura di sicurezza informatica. Nello specifico, nell'ambito dell'attività ispettiva organizzata dalla CNIL, si evinceva che, all'interno di un ufficio della predetta Società, l'impianto di videosorveglianza permetteva di riprendere i dipendenti nella rispettiva postazione di lavoro in assenza di una prima informativa minima che consentisse di segnalare la presenza di area videosorvegliata e di una distinta nota informativa completa, conforme a quanto espressamente disposto dalla normativa in materia di protezione dei dati personali. Con riferimento alla progettazione di misure tecniche ed organizzative, nella stessa Società si riscontrava, altresì, una mancata applicazione delle misure di sicurezza sulle postazioni di lavoro, lì dove l'accesso al *personal computer* era autorizzato senza alcuna procedura di autenticazione da parte dei dipendenti, i quali condividevano la password di accesso all'indirizzo di posta elettronica aziendale. Rilevante, allo stesso modo, è la prima sanzione inflitta dall'Autorità di controllo svedese (Datainspektionen, DPA)[19], nell'ammontare di 20.000 euro, disposta nei confronti di un istituto di scuola superiore di Skellefteå, a causa dell'utilizzo della tecnica di riconoscimento facciale degli alunni con il precipuo scopo di monitorare la partecipazione degli studenti all'attività didattica organizzata dall'Istituto. La valutazione circa la concreta attuazione del principio di accountability del titolare ha condotto il Consiglio del liceo ad individuare quale idonea base giuridica del trattamento, ai sensi dell'art. 6 del RGPD, il consenso degli studenti per le attività di rilevazione di dati biometrici, portando così l'Autorità svedese a sottolineare l'erronea acquisizione di manifesta volontà da parte degli interessati, considerata la condizione di subordinazione e soggezione degli studenti nei confronti dell'Istituto scolastico[20]. Risulta, quindi, di tutta evidenza che, nel caso appena riportato, il

[16] *Provvedimento del Garante in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale* - 6 marzo 2014 [Doc. web n. 3013267]

[17] Commission nationale de l'informatique et des libertés (CNIL)

[18] In https://www.cnil.fr/en/home

[19] In https://www.datainspektionen.se/nyheter/sanktionsavgift-for-ansiktsigenkanning-i-skola/

[20] Analogamente si segnala M. Gorga, *Il trattamento dei dati personali dei lavoratori del settore pubblico e privato non può fondarsi sul consenso*, Associazione Nazionale Professionale Segretari Comunali e Provinciali, 2019,https://www.segretaricomunalivighenzi.it/23-08-2019-il-trattamento-dei-dati-personali-dei-lavoratori-del-settore-pubblico-e-privato-non-puo-fondarsi-sul-consenso#null

consenso non possa essere considerato valido in virtù di uno squilibrio nei rapporti tra le parti richiamate, rappresentato da una prova di forza esercitata dal titolare del trattamento[21]. La Datainspektionen, in seguito all'attività istruttoria esperita, ha stabilito, inoltre, che il titolare del trattamento, in adesione ad una impostazione *risk based*, avrebbe dovuto individuare modalità operative meno invasive rispetto alla specifica finalità di rilevazione delle presenze[22] degli studenti, con il conseguente obiettivo di minimizzare le minacce che, potenziali fenomeni di *data breach*, avrebbero comportato sulla disponibilità, sulla riservatezza e sulla integrità dei dati personali degli interessati. Infine, e non certo per importanza, va ricordata la sanzione,[23] nell'ammontare di 1 milione di euro che il Garante per la protezione dei dati personali italiano ha comminato a *Facebook* per gli illeciti compiuti nell'ambito del caso "*Cambridge Analytica*"[24], la Società, che attraverso un'applicazione per test psicologici, otteneva l'accesso a dati personali di circa 87 milioni di utenti al fine di influenzare le elezioni presidenziali americane svoltesi nel 2016. L'Autorità di controllo italiana, precedentemente, aveva già negato a *Facebook* la possibilità di continuare a trattare dati degli utenti italiani, considerato che l'applicazione "*Thisisyourdigitallife*", inizialmente scaricata da circa 57 utenti italiani, attraverso il sistema di "*Facebook login*" e la conseguente funzione che consentiva di condividere dati degli "amici" della piattaforma social, acquisiva dati nell'ordine di più di 200 mila interessati, senza che questi ultimi fossero previamente informati della cessione dei loro dati e avessero rilasciato espresso consenso a questa cessione. Aspetto di assoluto rilievo, quindi, risiede nella contestazione operata dal Garante per la protezione dei dati personali nei confronti della piattaforma social, circa le violazioni derivanti, nell'ordine, dall'omessa informativa (fattispecie, ad oggi, non più espressamente prevista dal D.Lgs n. 196/2003 e ss.mm.ii.), dalla conseguente mancata manifestazione di espressa volontà degli interessati e, non in ultimo, il mancato riscontro ad una richiesta di informazioni ed esibizione di documenti, attività espressamente consentita, oggi, dall'art. 157 del D.Lgs n. 196/2003[25]. In conclusione, giova ritornare brevemente su una delle basi giuridiche previste dall'art. 6 del Regolamento generale UE 2016/679 e oggetto di analisi negli interventi delle Autorità di controllo riportati. Per l'appunto, il titolare del trattamento deve garantire che il trattamento dei dati personali avvenga sulla base delle indicazioni fornite dal

[21] Analogamente si segnala P. Tullini, *Controlli a distanza a tutela dei dati personali dei lavoratori*, Il nuovo diritto del lavoro, 2017, p. 22-23.

[22] L'atto di recepimento svedese del RGPD, tra l'altro, prevede un apposito divieto (con alcune eccezioni) al trattamento dei dati biometrici, essendo questi dati "particolari", capaci di rivelare caratteristiche personalissime dell'interessato

[23] Garante per la protezione dati personali, *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9121486*

[24] *Cambridge Analytica - Il Garante privacy incontra Facebook e chiede chiarimenti sulle possibili violazioni commesse in Italia*, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8533717

[25] Art. 157 del Codice in materia di protezione dei dati personali, *Richiesta di informazioni e di esibizioni di documenti, "1. Nell'ambito dei poteri di cui all'articolo 58 del Regolamento, e per l'espletamento dei propri compiti, il Garante può richiedere al titolare, al responsabile, al rappresentante del titolare o del responsabile, all'interessato o anche a terzi di fornire informazioni e di esibire documenti anche con riferimento al contenuto di banche di dati"*

legislatore europeo in materia di protezione dei dati personali. Il consenso, condizione di liceità riscontrata nel corso dell'attività ispettiva organizzata dal Garante svedese, oggi previsto dall'art. 5, paragrafo 2, della Convenzione 108 modernizzata e all'art. 6, paragrafo 1, lett. a) del RGPD, prevede che la manifestazione positiva di volontà, previa preventiva informazione, debba essere prestata dall'interessato, senza alcuna forma di condizionamento e revocabile in qualsiasi momento.

3. Brevi casistiche di violazioni per mancato rispetto del principio di minimizzazione

Come riferito in precedenza, l'art. 5 del Regolamento UE 2016/679 rappresenta un punto essenziale della normativa rilevante, dalla cui lettura si evince, tra gli altri, il principio di minimizzazione dei dati che viene individuato quale causa, tra l'altro, nella casistica di violazione, rilevata dall'Autorità garante portoghese,[26] nei confronti del presidio ospedaliero Centro Hospitalar Barreiro Montijo, colpevole aver reso disponibili dati personali e categorie di dati particolari dei pazienti a gran parte del personale in servizio, indiscriminatamente, senza alcuna politica di accesso al dato[27]. All'esito dell'attività istruttoria dell'Autorità di controllo, inoltre, sono state contestate le violazioni del principio di riservatezza e integrità delle informazioni di carattere personale e la mancata adozione di misure tecniche e organizzative necessarie a comprovare la corretta applicazione delle disposizioni richiamate dal legislatore europeo in materia di protezione dati personali[28]. La fattispecie scaturisce dalla segnalazione della rappresentanza sindacale del personale medico che, a buon diritto, segnalava la possibilità, anche per il personale non sanitario, di accedere ai sistemi informatici della struttura ospedaliera e alle cartelle cliniche degli assistiti. Dai rilievi ispettivi evinti dall'Autorità di controllo, si accertava l'attivazione di circa 900 utenze, con privilegi di autorizzazione riservato al personale medico, quando quest'ultimo, a pieno organico, constava di sole 300 unità, rendendo necessario sanzionare tale discrepanza attraverso l'irrogazione di due sanzioni, una

[26] Comissão Nacional de Protecção de Dados (CNPD)

[27] P. Perri, G. Ziccardi, *Data governance, protezione dei dati e GDPR*, Volume II, Giuffrè Francis Lefebvre, pp. 19-22, 2019

[28] Considerando 78 al Regolamento UE 2016/679 "*La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita. Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici*".

nell'ammontare di 150.000 euro per "*non aver garantito la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento*", ai sensi dell'art. 32 RGPD, e una successiva di 300.000 euro per mancata adozione di misure tecniche ed organizzative, utili ad implementare un sistema documentato di procedure di autenticazione e autorizzazione da assegnare al personale ospedaliero, modulato sulla base delle competenze funzionali per consentire, al contempo, la cancellazione di utenze appartenenti a soggetti il cui contratto con la struttura ospedaliera avesse spirato i relativi effetti. Altra casistica meritevole di attenzione, avente ad oggetto la violazione del principio di minimizzazione, si è verificata in Belgio, lì dove l'Autorità di controllo nazionale ha comminato una sanzione stabilita in 10.000 euro nei confronti di un commerciante, il quale per l'emissione di una carta fedeltà[29], in maniera inadeguata rispetto alla finalità stabilita, richiedeva la presa visione della carta d'identità elettronica degli interessati. Il trattamento, secondo la DPA, è risultato sproporzionato rispetto alle finalità del trattamento. Sempre con riferimento alle carte fedeltà, precedentemente all'entrata in vigore del Regolamento generale sulla protezione dei dati personali, il nucleo della Guardia di finanza italiana ha rilevato una condotta illecita da parte di un importante gruppo commerciale che, in violazione alle disposizioni rilevanti della normativa in materia di protezione dati, inoltrava ai suoi clienti, per ulteriori finalità di marketing, comunicazioni commerciali senza l'acquisizione di uno specifico ed espresso consenso[30]. La condotta illecita, segnalata all'Autorità di controllo italiana da clienti in possesso della carta fedeltà, risultava aggravata dall'inerzia della Società alle ripetute richieste degli utenti di cancellazione dalla mailing list pubblicitaria. Ancora, tornando al principio di minimizzazione del dato, il Garante rumeno[31] è intervenuto sul punto, nel giugno 2019, sanzionando[32] l'Istituto Unicredit per un totale di 130.000 euro, per aver violato due articoli del Regolamento generale sulla protezione dei dati personali, riguardanti, rispettivamente, il principio di minimizzazione, art. 5, paragrafo 1, lett. c) RGPD, e di protezione by design e by default, rinvenibili all'art. 25 RGPD, generando un pregiudizio per i diritti e le libertà fondamentali di circa 300.000 interessati. Secondo la situazione riscontrata dall'Autorità di controllo rumena, pertanto, i beneficiari dei pagamenti, all'atto di ricezione del pagamento, accedevano a dati identificativi (informazioni quali indirizzo e codice fiscale) rinvenibili dalla consultazione dell'estratto conto. Concludendo, il regolamento generale sulla protezione dei dati personali, con espresso riferimento al principio di minimizzazione[33], stabilisce, in maniera inequivocabile, che i dati raccolti debbano essere adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità

[29] In https://edpb.europa.eu/news/national-news/2019/belgian-data-protection-authority-imposes-fine-eu-10000_en

[30] *Provvedimento Garante per la protezione dei dati personali del 20 giugno 2019 [Doc. web n. 9124420]*

[31] Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal

[32] In https://www.dataprotection.ro/?page=Comunicat_Amenda_Unicredit&lang=ro

[33] A. Pisapia, *La tutela multilivello garantita ai dati personali nell'ordinamento europeo*, Rivista Federalismi, n. 3-2018, pp. 26-28

per cui sono trattati [34], richiamando il titolare del trattamento alla concreta applicazione del principio di *privacy be design* e di *privacy by default* nell'implementazione di un sistema di gestione che tenga in dovuta considerazione il ciclo di vita del dato personale.

4. Brevi cenni di casistiche di sanzioni per mancata adozione di misure di sicurezza e per violazioni dei dati personali (data breach)

Il data breach è una violazione di sicurezza, prevista in ambito pubblico dal Garante per la protezione dei dati personali già nel 2015[35], che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati[36]. La violazione consegue a condotte, colpose o dolose, in cui vi è una compromissione della sicurezza dei dati personali, pertanto, il Regolamento generale sulla protezione dati personali, in tali casi, prescrive specifici adempimenti. Come noto, in caso di violazione, al titolare del trattamento è demandato l'obbligo di notificare, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne sia venuto a conoscenza, l'evento all'Autorità di controllo[37] e procedendo alla relativa comunicazione agli interessati, qualora la violazione presenti rischi elevati in ordine ai diritti e le libertà delle persone fisiche. Strategica, a tal riguardo, è la corretta applicazione dell'art. 32 RGPD sulla sicurezza del trattamento dei dati, il quale stabilisce che le misure di sicurezza, non più minime (come previste dalla vecchia formulazione del Codice in materia di protezione dei dati personali) debbano essere approntate, dal titolare e dal responsabile del trattamento, secondo una valutazione preliminare che tenga dovutamente conto del contesto in cui si opera, dei costi di attuazione, dell'oggetto, delle finalità del trattamento e dei rischi derivanti dal trattamento di dati personali che possono impattare sui diritti e le libertà delle persone fisiche. Più dettagliatamente, il legislatore europeo in materia di protezione dei dati personali stabilisce l'adozione di misure tecniche e organizzative, progettate e revisionate alla luce della progresso tecnologico del momento[38], atte a garantire un livello di sicurezza commisurato al rischio (*risk based approach*)[39]. Con riferimento alle

---

[34] Si veda anche la Convenzione n. 108 modernizzata, articolo 5, paragrafo 4, lettera c)

[35] *Provvedimento sulle Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche del 2 luglio 2015* [Doc. web n. 4129029] e *Linee guida in materia di Dossier sanitario elettronico del 4 giugno 2015* [Doc. web n. 4084632]

[36] Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa, *Manuale sul diritto europeo in materia di protezione dati, pp. 191-193, 2018*

[37] Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679. Adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017- Versione emendata e adottata il 6 febbraio 2018.

[38] Si fa espresso riferimento ai Considerando 6 e 7 al Regolamento generale sulla protezione dei dati personali UE 2016/679 che rappresentano la necessità di tutela dei diritti e delle libertà delle persone fisiche nella Società moderna.

[39] Al paragrafo 3, l'art. 32 RGPD *stabilisce altresì che l'adesione a un codice di condotta o a un meccanismo di certificazione può essere utilizzata come elemento per dimostrare la conformità ai requisiti appena elencati. Chiunque agisca sotto l'autorità del titolare e del responsabile del trattamento e abbia accesso a dati personali deve essere opportunamente*

attività ispettive condotte dalle Autorità nazionali dall'entrata in vigore del Regolamento generale UE 2016/679, si può affermare che una considerevole parte delle rilevazioni di condotte illecite hanno ovviamente riguardato una inidonea progettazione delle misure di sicurezza e conseguenti eventi di data breach. Tale considerazione è emblematica del rischio a cui i dati personali degli interessati sono sottoposti, se si considera che, potenzialmente, i fenomeni di data breach resi pubblici o denunciati risultano essere soltanto una piccola parte del totale. L'attività delle Autorità di controllo, con riferimento allo specifico aspetto della sicurezza del trattamento, ad oggi, è intensa. Nel settembre 2018 l'Autorità di controllo dello stato di Baden Württenberg[40] ha sanzionato per un totale di 20.000 euro la società "*Knuddels*" [41] per aver violato, per l'appunto, l'art. 32 RGPD, mancando nella progettazione di un sistema misure di sicurezza adeguato per la gestione del sito web, con particolare riferimento al servizio di *chat online*, subendo un *leak* di quasi 2 milioni di coppie di username e password e circa 800 mila indirizzi di posta elettronica. La predetta Società, con conseguente atteggiamento proattivo e collaborativo, ha prontamente informato l'Autorità di controllo e i suoi utenti (nel frattempo gli *hackers* rendevano noti i dati personali violati), elemento del quale ha tenuto conto l'Autorità di controllo nel quantificare la sanzione. Il Garante polacco (UODO)[42] ha sanzionato nel mese scorso, per euro 645.000, il rivenditore online "*Morele.net*" per aver violato le disposizioni del legislatore europeo in materia di sicurezza del trattamento. In particolare, il rivenditore aveva subìto un rilevante attacco informatico, i cui effetti avevano condotto alla sottrazione e uso illecito di dati personali di circa 2 milioni di utenti[43]. La Società, dal proprio canto, ha rappresentato di aver tempestivamente informato i propri clienti sull'entità dell'incidente, tuttavia, all'esito dell'indagine dell'autorità polacca, è emerso che le misure organizzative e tecniche messe in atto dal titolare del trattamento risultavano inadeguate a mitigare il rischio esistente, in aperto contrasto con quanto richiesto dal legislatore europeo in materia di protezione dei dati personali[44]. Alla società sono state contestate la violazione delle disposizioni inerenti i principi applicabili al trattamento, richiamati all'articolo 5, paragrafo RGPD, e la mancanza di adeguate misure tecniche (di sicurezza insufficienti) e organizzative (sul monitoraggio dei potenziali rischi correlati al comportamento atipico online). Un evento simile, notificato al Garante per la protezione dei dati personali, ha interessato l'Istituto Unicredit Banca, con conseguente perdita di dati di circa 700 mila correntisti[45]. Di questi account, quasi

---

istruito sui suoi obblighi. In definitiva il principio di sicurezza prevede l'obbligo di riservatezza, integrità e disponibilità dei dati.

[40] Landesbeauftragte Für Den Datenschutz Und Die Informationsfreiheit – LFDI

[41] In https://www.bfdi.bund.de/DE/Home/home_node.html

[42] Urzad Ochrony Danych Osobowych, in https://uodo.gov.pl/en

[43] In https://uodo.gov.pl/decyzje/ZSPR.421.2.2019

[44] In https://edpb.europa.eu/news/national-news/2019/polish-dpa-imposes-eu645000-fine-insufficient-organisational-and-technical_it

[45] In https://www.federprivacy.org/associazione/item/709-data-breach-a-unicredit-731mila-i-correntisti-coinvolti

7.000 sono stati immediatamente bloccati dall'Istituto di credito, poiché gli hacker erano riusciti ad entrare nella disponibilità delle password (vale a dire il PIN), mentre per i restanti, all'esito di una valutazione di impatto, non era stata ravvisato un rischio elevato sulla sicurezza delle informazioni. Tenendo conto delle interlocuzioni avvenute, l'Autorità italiana ha ingiunto a "*Unicredit Banca*" di contattare tutti i correntisti coinvolti, visto che l'acquisizione dei "*citati dati personali è da ritenere già di per sé fonte di potenziale grave pregiudizio per gli interessati, in considerazione dell'abitudine diffusa tra gli utenti dei servizi online di utilizzare password e PIN facilmente memorizzabili e, dunque, della concreta possibilità che diversi interessati, ancorché Unicredit fornisca ai propri clienti 'indicazioni utili su come creare e aggiornare il PIN', non abbiano tenuto conto di tali consigli*"[46]. Analogamente, anche il Garante bulgaro è intervenuto nei confronti di Istituti di credito, comminando la sanzione di circa 500 mila euro al gruppo OTP, e più precisamente alla "DSK Bank" per la violazione dei dati personali di circa 33 mila clienti, riferibili a dati contatto, nomi e cognomi, indirizzi, copie di documenti di identità, ulteriori informazioni personali di clienti che avevano richiesto un prestito e di soggetti terzi (parenti) che avevano prestato garanzia nelle pratiche di finanziamento. Proseguendo, l'Autorità di controllo britannica, ICO, ha sanzionato[47] l'Hotel Marriott International per 99 milioni di sterline per il data breach dei dati di 339 milioni di ospiti provenienti da tutto il mondo, di cui circa 30 milioni appartenenti a residenti nello spazio economico europeo, e 7 milioni di residenti nel Regno Unito[48]. L'incidente informatico, notificato a novembre 2018, è scaturito dalla vulnerabilità di una società, la Starwood Hotel & Resort Worlwide, acquistata da Marriott International nel 2016. L'Autorità di controllo inglese ha rilevato una violazione dell'art. 32 del GDPR, in ordine alla misure di sicurezza applicabili al trattamento, in quanto Marriott avrebbe dovuto gestire l'acquisizione del gruppo Starwood in modo più diligente, verificando, in sede di rilevazione della predetta Società, eventuali criticità in ordine alla sicurezza informatica (e della relativa infrastruttura) e delle informazioni, adoperandosi, successivamente, nella progettazione di specifiche misure di sicurezza[49] sui sistemi informativi, utili, altresì, alla protezione dei dati personali (si tratta, nello specifico, di violazioni inerenti nomi e cognomi dei clienti, indirizzi email, numeri di telefono, numeri di passaporto, date di nascita, codici di prenotazione e dati relativi alle carte di credito) precedentemente raccolti dalla Società acquisita[50]. Analoga sanzione[51],

---

[46] Ibidem

[47] In https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/

[48] Il Commissario per le informazioni personali Elizabeth Denham riferisce che "*I dati personali hanno un valore reale, quindi le organizzazioni hanno il dovere legale di garantirne la sicurezza, proprio come farebbero con qualsiasi altra risorsa. Se ciò non dovesse accadere, non esiteremo a prendere misure energiche quando necessario per proteggere i diritti del pubblico*"

[49] P. Perri, G. Ziccardi, *Tecnologia e Diritto,* Giuffrè Francis Lefebvre, pp. 56-66, 2017

[50] In https://www.iusinitinere.it/le-sanzioni-gdpr-del-2019-le-piu-rilevanti-da-gennaio-a-luglio-22377#_ftn41

51 In https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/

nell'ammontare di 183 milioni di sterline, è stata inflitta dall'ICO alla compagnia aerea "British Airways" in forza di un evento di data breach scaturito da un cyberattacco, attuato attraverso una procedura tecnica che indirizzava gli utenti verso un sito web fraudolento che, a sua volta, permetteva di intercettare e catturare credenziali di accesso a siti, dati di contatto dei clienti, estremi delle carte di pagamento con relativi codici di sicurezza. La compagnia aerea, che aveva attivato la procedura di notifica della violazione all'Autorità di controllo, ai sensi dell'art. 33 del RGPD, nelle 72 ore dall'avvenuta conoscenza dell'evento e che si era resa, nella fase istruttoria, protagonista di un comportamento collaborativo con l'Autorità, si è vista eccepire dall'Ufficio del Commissario responsabile delle Informazioni, Autorità capofila per i restanti Garanti nazionali in forza del principio del One Stop Shop[52], la mancata adozione di adeguate misure di sicurezza a protezione delle informazioni personali degli interessati, dislocati anche al di fuori dello Spazio Economico Europeo. È opportuno, infine, segnalare la sanzione inflitta dal Garante italiano all'Associazione Rousseau, responsabile del trattamento, per la violazione degli artt. 32 e 83, paragrafo 4, lettera a) RGPD. La sanzione[53] inflitta ammonta a 50 mila euro, oltre agli adeguamenti necessari contenuti nel provvedimento[54]. Il Garante, dopo oltre un anno di attività istruttoria e due Provvedimenti ad *hoc*, è definitivamente intervenuto evidenziando come i sistemi di sicurezza, messi in atto dalla piattaforma di voto on line, mostrassero significative lacune tecniche, segnalando la condivisione delle credenziali di autenticazione da parte di più incaricati, dotati di elevati privilegi di gestione della piattaforma e la carenza di un completo tracciamento al database del sistema Rousseau. A riprova di quanto segnalato, la stessa piattaforma era stata oggetto di attacco informatico da parte di un hacker, resosi protagonista, altresì, della pubblicazione di dati personali di alcuni iscritti al Movimento Cinque Stelle.

52 Art. 56, par.1, Regolamento generale sulla protezione dati personali, Competenze dell'autorità di controllo capofila, "Fatto salvo l'articolo 55, l'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare e del trattamento o responsabile del trattamento è competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri effettuati dal suddetto titolare del trattamento o responsabile del trattamento, secondo la procedura di cui all'articolo 60".

53 Garante per la protezione dati personali sul sito web istituzionale, *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9101974*

54 *Provvedimento del Garante per la protezione dei dati personali*, n. 83 del 4 aprile 2019