Il data breach nei rapporti tra il Titolare e il Responsabile del trattamento.

Violazioni e incidenti di sicurezza connesse ad attività di dipendenti del responsabile.

L'esfiltrazione di dati personali da parte del dipendente del responsabile e la gestione del *data breach*.

*Andrea Broglia***

SOMMARIO: 1. Introduzione. - 2. Il *data breach* come fenomeno della società dell'informazione. - 3. I rapporti tra Titolare e Responsabile del Trattamento nel Regolamento Europeo n. 679/2016: obblighi e doveri connessi alla rilevazione di un incidente. 4. - Gli articoli 33 e 34 del GDPR: notifica all'Autorità di Controllo e comunicazione all'interessato. Il ruolo e gli adempimenti del responsabile. - 5. La valutazione del rischio determinato dall'incidente. Cenni. Conseguenze sull'obbligo del responsabile. – 6. Gli incidenti dovuti ad attività illecite commesse da dipendenti. - 7. L'esfiltrazione di dati personali operata da un soggetto in veste di autorizzato al trattamento presso il Responsabile. 8. La recente proposta di Direttiva NIS 2. - 9. Il *tool* del Garante. - 10. Le Linee Guida EDPB 1/2021: gli esempi in relazione alla notifica del *data breach*.

1. Introduzione

Recenti accadimenti di cronaca hanno portato e continuano a portare alla ribalta la questione relativa al c.d. *data breach*, non solo, per così dire, tradizionale o istituzionale, ovvero nel senso di accaduto nella sfera di controllo del titolare del trattamento ma, per diverse ragioni, anche di quella del responsabile[1].
Giornalmente gli operatori del settore si confrontano con le conseguenze che un tale evento comporta, con le difficoltà di gestione delle implicazioni correlate, con le necessità di una attenta valutazione di ogni aspetto dell'incidente ma anche, e in

***** Il presente lavoro costituisce l'elaborato finale redatto in occasione della fine del Corso di Perfezionamento Universitario in Criminalità Informatica e Investigazioni Digitali (a/a 2020-21), diretto dal PROF. G. ZICCARDI tenuto presso l'Università degli Studi di Milano.

[1] La bibliografia in tema di *data breach* è ampia. Per indicazioni cfr., ad esempio: R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè Francis Lefebvre, Milano, 2019, pagg. 381 e ss.; L. BOLOGNINI, E. PELINO, *Codice di disciplina della privacy*, Giuffrè Francis Lefebvre, Milano, 2019, pagg. 240 e ss.; N. BERNARDI (a cura di), Privacy, protezione e trattamento dei dati, Wolters Kluwer, Milano, 2019, pag. 305; E. BASSOLI, La nuova privacy, GDPR, Dike Giuridica S.r.L., Roma, 2018.

alcuni casi soprattutto, con la previsione dello stesso, il tutto ovviamente allo scopo di adempiere alle rilevanti prescrizioni dettate nel settore della protezione dei dati personali[2].
In questo breve scritto si affronteranno, senza pretesa di completezza, alcune delle problematiche connesse agli incidenti di "violazione di sicurezza" che riguardano dati personali e, in particolare, quelle derivanti da un comportamento illecito del dipendente di una società o di un ente che operi, nel "flusso" del trattamento, in qualità di autorizzato di un soggetto che abbia, a propria volta, il compito di trattare informazioni per conto di altri e, segnatamente, per il titolare[3].
Mentre infatti colui che, in base alla normativa rilevante, "determini finalità e mezzi del trattamento", ossia decida il "perché" e il "come" trattare dati personali è definito Titolare, colui che, invece, tale trattamento esegua in virtù di un espresso rapporto contrattuale, solo e nei limiti in cui esso gli venga affidato, è definito Responsabile[4].
Questo rapporto determina una notevole serie di obblighi e di doveri in capo alle parti coinvolte, addirittura prima ancora che il rapporto stesso venga ad esistenza.
Allorché poi, in particolare, un soggetto alle dipendenze del responsabile compia atti esulanti dalle istruzioni e indicazioni specificamente assegnategli, derivano da tali accadimenti diverse conseguenze: non solo in capo al titolare del trattamento, ma anche in capo allo stesso responsabile; questi infatti dovrà comunicare "senza ritardo" l'accaduto al titolare e coadiuvarlo nella gestione dell'incidente complessivamente considerato; ulteriormente il titolare dovrà mettere in atto procedure e valutazioni al fine di decidere se la circostanza determini la necessità di una formale notifica all'Autorità di Controllo e, ancora, valutare se si tratti di un caso che possa comportare, per l'interessato dei cui dati si tratti, un "rischio elevato" per i suoi diritti e libertà fondamentali.

---

[2] Nella sola prima parte del 2020 sono stati riportati oltre 108.000 *data breach*: https://enterprise.verizon.com/resources/reports/dbir/. Recentissimo il caso che ha visto coinvolto l'operatore low cost di un big della telefonia: https://www-infosec-news.cdn.ampproject.org/c/s/www.infosec.news/2021/01/04/news/sicurezza-digitale/ho-mobile-alza-bandiera-bianca-avevamo-ragione-noi/amp/, ma sono altrettanto noti gli episodi che hanno coinvolto, negli anni 2018 e 2019, Siae: https://www.edoardolimone.com/2018/11/03/anonymous-attacca-la-siae-pubblicato-un-archivio-dati-di-oltre-2-gb/; Saipem: https://in.reuters.com/article/us-italy-cyber-saipem-idINKBN1O92B1 e molti altri: https://www.cybersecurity360.it/news/i-10-peggiori-data-breach-del-2018-un-miliardo-di-account-violati-e-allarme/. Anche il settore bancario, come noto, è particolarmente soggetto ad attacchi di vario tipo: https://www.cybersecurity360.it/nuove-minacce/emotet-una-variante-del-banking-trojan-ci-infetta-con-e-mail-di-risposta-ai-nostri-stessi-messaggi-i-dettagli/. A livello internazionale, inoltre, come non ricordare il caso di Edward Snowden e le sue rivelazioni sui programmi di sorveglianza massiva, raccontati in prima persona nel libro *Errore di sistema*, Longanesi, 2019 (https://it.wikipedia.org/wiki/Edward_Snowden) o le violazioni connesse allo scandalo Cambridge Analytica: https://it.wikipedia.org/wiki/Cambridge_Analytica. L'elenco, purtroppo, potrebbe continuare a lungo, giacché anche nel corso del 2020 gli incidenti sono stati numerosi: https://www.cybersecurity360.it/news/sanzioni-gdpr-maglia-nera-allitalia-nel-2020-ecco-errori-e-sfide-da-affrontare/.

[3] Il tema della esfiltrazione di dati personali, intesa quale copia o trasferimento di dati non autorizzato o effettuato oltre i limiti o per finalità estranee a quelle demandate al soggetto, è estremamente vasto e si riconnette anche alla questione, di rilevanza penale, dell'accesso abusivo a sistema informatico di cui all'art. 615 *ter* c.p., sui v. *infra* nel testo.

[4] Per le definizioni più rilevanti in tema di trattamento dei dati personali si rimanda al Regolamento Europeo n. 679/2016 (GDPR), il cui articolo 4 contiene una ampia elencazione.

Come si vede il coinvolgimento, in una tale circostanza e a vario titolo, di una pluralità di soggetti e la presenza di notevoli obblighi comporta una serie di conseguenze che possono, di volta in volta, avere determinante rilievo e che comunque, in generale, devono essere attentamente considerate.

2. Il data breach *come fenomeno della società dell'informazione*[5]

Lo sviluppo delle tecnologie e il moltiplicarsi delle informazioni che circolano in ogni istante[6] in un mondo sempre più interconnesso[7] aumentano le possibilità che, accidentalmente o in modo illecito, avvengano violazioni di dati personali.
Il *data breach* è, in particolare, un avvenimento che "comporta … la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati"[8].
Allorché tali incidenti accadano non nella sfera di controllo del soggetto che i dati abbia raccolto per proprie finalità ma che tali dati, invece, tratti per conto di altri, ne derivano, in dipendenza degli obblighi e dei doveri nascenti dalle prescrizioni in tema di protezione dei dati personali da ultimo innovate a livello europeo dal GDPR[9], importanti conseguenze.
Il punto è che, nell'odierna società dell'informazione, gli attori sono mutualmente connessi e partecipano, molto spesso, a catene di trasferimenti di dati personali che rendono, talvolta, non solo il controllo da parte dei singoli interessati, cui i dati appartengono, particolarmente sfumato se non addirittura incomprensibile, ma, soprattutto, significativamente delicato anche per coloro che, d'altro canto, tali dati invece raccolgono e utilizzano per i più diversi scopi.
Quel che si vuol dire è che la quarta rivoluzione industriale e l'*infosfera*[10], basti pensare all'Internet delle cose o allo sviluppo delle piattaforme online per usufruire di una moltitudine di servizi e prestazioni, richiede il contemporaneo e/o successivo intervento di una pluralità di soggetti e di tecnologie abilitanti e, di conseguenza, una pervasiva e talvolta poco controllabile mobilità di dati e informazioni; si tratta, da un lato, di un fenomeno facilitante una moltitudine di servizi e opportunità per gli utenti della odierna società ma, dall'altro e al contempo, di una fonte di notevoli pericoli e minacce.

---

[5] Come noto il concetto di "servizi della società dell'informazione" deriva dalla direttiva 98/34/CE come modificata dalla direttiva 98/48/CE. Mentre nel testo il riferimento è, in senso ampio e generale, riferito ai servizi, alle tecnologie e alle piattaforme online, nella direttiva citata il riferimento è a qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi.
[6] Una nota infografica, periodicamente aggiornata, è rinvenibile qui: https://www.visualcapitalist.com/every-minute-internet-2020/.
[7] Interessanti, documentate osservazioni sono contenute in M. DELMASTRO e A. NICITA, Big Data, come stanno cambiando il nostro mondo, il Mulino, Bologna, 2019.
[8] Cfr. art. 4, 12), GDPR.
[9] V. nota 3: il Regolamento Europeo n. 679/2016, meglio noto come GDPR, entrato definitivamente in vigore il 18 maggio 2018, ha sostituito la precedente direttiva 95/46/CE (c.d. Direttiva "Madre"), così proponendosi come norma di rango superiore direttamente applicabile in tutti gli Stati dell'Unione senza necessità di atti di adeguamento e conversione, spesso forieri di disomogeneità anche notevoli.
[10] Il riferimento è, va da sé, a L. FLORIDI, *La quarta rivoluzione: come l'infosfera tra trasformando il mondo*, Raffaello Cortina, Milano, 2017.

In tale mobilità si annidano particolari *vulnera*, che l'intervento regolatore dell'Unione Europea ha voluto precipuamente controllare e possibilmente mitigare, ponendo in capo ai soggetti e alle entità economiche che da tali trattamenti ricavano lauti guadagni, importanti obblighi di *accountability* e trasparenza, il tutto al fine di mantenere e preservare un elevato livello di protezione dei diritti e delle libertà fondamentali degli individui.
Istituzioni europee come Enisa[11] ed Europol[12] sono da anni impegnate in una attenta analisi delle minacce che si annidano negli ambienti tecnologici e forniscono periodicamente rapporti, studi e valutazioni assai utili, anche se talvolta allarmanti; recentemente, inoltre, le vicende conseguenti alla purtroppo nota pandemia "da Covid-19" hanno aumentato i rischi per gli individui e le minacce conseguenti ad uno spesso forzato o necessitato degli strumenti tecnologici[13].
Se la normazione in materia di protezione dei dati personali e delle persone fisiche trae, nel tempo, le proprie radici nella Dichiarazione universale dei diritti umani[14], nella Convenzione europea dei diritti dell'uomo (CEDU)[15] e, successivamente, nella Carta dei diritti fondamentali di Nizza (CFREU)[16], oggi una rilevante tutela degli individui è rinvenibile non solo nel complesso dei "rinnovati" diritti dell'interessato analiticamente indicati negli articoli da 15 a 22 del GDPR[17], ma anche nelle previsioni dell'art. 34 laddove, in determinate circostanze, al titolare è imposto l'obbligo di comunicare anche all'interessato l'avvenuto accadimento di un "incidente di violazione dei dati personali": il *data breach*.

3. I rapporti tra Titolare e Responsabile del Trattamento nel Regolamento Europeo n. 679/2016: obblighi e doveri connessi alla rilevazione di un incidente

Il trattamento di dati personali comporta una interazione tra un soggetto che acquisisce dati e informazioni per utilizzarle ai propri fini e un soggetto cui tali dati si riferiscono.
Mentre il soggetto che conferisce i propri dati è l'interessato, il soggetto che decide "perché e come[18]" trattare tali dati è il titolare del trattamento[19].

---

11 https://www.enisa.europa.eu/.
12 https://www.europol.europa.eu/.
13 https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020; https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know.
14 Cfr. https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/itn.pdf.
15 Cfr. https://eur-lex.europa.eu/summary/glossary/eu_human_rights_convention.html?locale=it#:~:text=Firmata%20nel%201950%20dal%20Consiglio,le%20libert%C3%A0%20fondamentali%20in%20Europa.&text=La%20convenzione%20ha%20istituito%20la,dalle%20violazioni%20dei%20diritti%20umani.
16 Cfr. artt. 7 e 8 della Carta: https://www.europarl.europa.eu/italy/it/scoprire-l-europa/carta-dei-diritti-fondamentali_1.
17 Basti pensare a diritti "nuovi" come il diritto alla portabilità dei dati di cui all'art. 20 GDPR o a quello all'oblio, come sovente viene definito il diritto alla cancellazione di cui all'art. 17.
18 Il titolare "determina finalità e mezzi del trattamento", ossia *determines purposes and means of the processing*: art. 4, cit..
19 Cfr. art. 4, par. 7 del Regolamento: '*controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the*

Quest'ultimo normalmente si avvale, nella propria attività, non solo di persone interne alla propria organizzazione, ma anche e, come visto, sempre più spesso, di realtà "esterne" e altre rispetto alla propria, ossia, laddove si verifichino le condizioni stabilite dalla normativa che stiamo esaminando, di responsabili del trattamento: di soggetti, enti, società, organizzazioni che trattano e tratteranno dati per suo conto.
Il rapporto che lega titolare e responsabile deve essere attentamente e obbligatoriamente programmato e specificato[20].
Nel ribadire con forza la necessità che il trattamento di dati personali avvenga nel rispetto dei principi fondamentali stabiliti nell'art. 5 del Regolamento Europeo[21], questo stesso articolo sottolinea e rimarca la necessità che il titolare del trattamento, poiché "competente per il rispetto" di tali principi, debba anche essere "in grado di dimostrarlo"[22].
Uno dei modi, peraltro necessitati, di dimostrazione di tale rispetto è quello per cui ogni qualvolta il titolare si avvalga di entità esterne cui demandi una parte, o anche tutta, l'attività di trattamento, tale rapporto sia consacrato in un atto scritto: tipicamente un contratto relativo al trattamento dei dati personali o uno specifico allegato destinato ad accompagnare un più ampio rapporto, regolato altrove[23].
L'art. 28 del GDPR disciplina gli adempimenti che il titolare deve mettere in atto tutte le volte in cui si affidi, per una parte o anche per l'intera operazione di trattamento di dati personali, a soggetti esterni.
La corretta qualificazione di tale complessa vicenda appassiona da tempo gli studiosi della materia: molto spesso nella quotidianità delle relazioni commerciali non appare agevole stabilire con certezza quale sia il ruolo effettivamente svolto da ciascuno dei protagonisti che si avvicendano nei diversi affari e non è infrequente notare, anche nei più autorevoli interpreti, impostazioni differenti[24].

---

specific criteria for its nomination may be provided for by Union or Member State law; v. nota 3 per il rimando alle definizioni contenute nell'art. 4 del Regolamento.

[20] Cfr. sui ruoli in discorso: A. D'OTTAVIO, *Ruoli e funzioni privacy principali ai sensi del Regolamento*, in PANETTA (a cura di), cit. alla nota 1, pagg. 143 e ss.; E. PELINO, L. BOLOGNINI, in Codice della disciplina privacy, cit. alla nota 1, pagg. 42 e ss..

[21] I principi dettati dall'art. 5 del GDPR sono quelli, noti, di (a) liceità, correttezza e trasparenza, (b) limitazione della finalità, (c) minimizzazione, (d) esattezza, (e) limitazione della conservazione, (f) di integrità e riservatezza. Il paragrafo 2. dello stesso articolo esprime in pieno, insieme ovviamente a diverse altre disposizioni, come l'art. 24, l'art. 25, l'art. 32, il c.d. principio dell'*accountability*, ossia della necessità che il titolare sia il soggetto deputato al rispetto delle prescrizioni, con le conseguenti eventuali responsabilità derivanti dal mancato adeguamento, sia del contemporaneo obbligo di poterlo, doverlo e saperlo dimostrare.

[22] Tipicamente il rapporto, di cui nel testo, viene regolato con appositi *DPA*, *Data Processing Agreements*, ovvero con allegati, *Attachments* al rapporto principale.

[23] L'EDPB, *European Data Protection Board*, il comitato che raggruppa i Garanti Europei, ha recentemente rinnovato la propria (*rectius*: del WP29) storica *opinion 1/2010*, sui ruoli che stiamo esaminando, con le *Guidelines 7/2020* sul concetto di titolare e responsabile, con importanti specificazioni sulla contitolarità (*joint controllership*) e ulteriormente intervenendo in relazione ai ruoli da attribuirsi ad attori particolarmente attivi nel mondo online, quali i *Social Media Provider*, i *Targeter* (gli inserzionisti) e il mondo delle *AD Tech companies: Guidelines 8/2020 on targeting on social media users*. I provvedimenti in questione sono liberamente fruibili e scaricabili dal sito del *Board* (https://edpb.europa.eu/edpb_en).

[24] Basterebbe, al riguardo, ricordare le perduranti perplessità sottese alla qualificazione dell'OdV in seno alla L. 231 e le diverse posizioni che pur dopo l'intervento del Garante Italiano continuano a

Per riprendere la più recente lettura europea[25], ad ogni modo, vale la pena sottolineare che il concetto deve essere interpretato in modo funzionale e autonomo, con particolare riguardo all'effettivo ruolo in concreto svolto dal soggetto (ente o organizzazione) nel determinato contesto in cui esso opera e che la definizione prescinde da eventuali ulteriori o diverse qualificazioni date dalla legge concretamente applicabile.
Degni di nota paiono, anche al fine delle problematiche in esame nel presente scritto, gli ultimi approdi del *Board* dei Garanti in relazione alla attribuibilità della qualifica di titolare del trattamento anche ai soggetti che non abbiano accesso diretto ai dati personali perché li ricevano in forma aggregata o statistica: il rilievo, nell'eventualità di incidenti, non è di poco conto, se messo in relazione con le possibili conseguenze in caso di eventi che comportino un elevato rischio per gli interessati[26].
Mentre, dunque, il titolare del trattamento determina sia finalità sia modalità[27] del trattamento, in quanto ciò derivi da un'espressa norma di legge o da un'influenza di fatto derivante dal contesto di riferimento, il responsabile o i responsabili adempiono ad uno o più specifici incarichi loro demandati dal titolare: si tratta di entità separate che trattano, nello specifico contesto, i dati per conto del titolare.
Quando un trattamento dunque, per riprendere le parole dell'art. 28 del Regolamento europeo n. 679/2016, deve essere effettuato per conto del titolare, quest'ultimo deve rivolgersi unicamente a responsabili che presentino garanzie che consentano di ritenere che sia possibile soddisfare il complesso delle disposizioni in materia di protezione dei dati personali e ciò, anche e soprattutto, per garantire la tutela dei diritti degli interessati[28]: il principio dell'*accountability* viene rinforzato mediante

---

confrontarsi: il provvedimento, che riassume una buona parte di tali impostazioni, è rinvenibile qui: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9347842.

[25] Si veda nota n. 23.

[26] Nelle recenti, citate, *Opinion* sul concetto di titolare, contitolari e responsabili del trattamento nonché sul targeting degli utilizzatori dei social media (Opinion 7/2020 e 8/2020: v. nota 23) viene ribadito come "*It is not necessary that the controller actually has access to the data that is being processed*", mentre nella seconda, nella "distribuzione" delle competenze e responsabilità del trattamento derivante dalla contitolarità nascente dalla comune determinazione di alcune finalità derivanti dalla trasmissione reciproca di informazioni, di invio di comunicazioni mirate ai destinatari, di osservazione del comportamento e di elaborazione di inferenze, viene riproposto il principio già espresso nella sentenze Wirtschaftsakademie (C-210/16) e Fashion ID (C-40/17) della CJEU, ampiamente riprese nelle *opinion* qui ricordate. Per rilievi critici, antecedenti ai provvedimenti, cfr. S. ZIPPONI, in Codice della Disciplina Privacy, diretto da L. BOLOGNINI e E. PELINO, cit.., *sub* commento all'art. 26 del GDPR. Non aver accesso al dato o, ad esempio, contezza dell'identità dell'interessato, in ipotesi di insorgenza del dovere di effettuare la comunicazione di cui all'art. 34, non può che tramutarsi nell'imposizione, a livello di stesure e regolamentazione della *joint controllership*, dell'onere di provvedere, in caso, da parte del contitolare. In presenza di circostanze in cui (quanto meno in quelle considerate nelle citate decisioni) il potere contrattuale delle due parti appare più che *imbalanced*, ciò potrebbe causare problemi non da poco.

[27] I *means* del trattamento, i mezzi e le modalità, sono decisi dal titolare allorché si tratti di elementi essenziali: quali dati e informazioni, per quanto tempo, chi vi possa accedere, ecc.. In relazione a modalità e mezzi non essenziali, da tempo si conviene possano, in certa misura, essere determinati o decisi nello specifico dal responsabile; resta peraltro fermo l'onere del titolare di mantenere il controllo anche su tali aspetti.

[28] Tra le numerose e dettagliate previsioni dell'art. 28 possono ricordarsi, ad esempio: a) trattare i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale; b) garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o

l'imposizione dell'onere di servirsi, nello sviluppo e nel corso delle operazioni di trattamento, solo di soggetti che presentino adeguate garanzie e che, se del caso, coadiuvino il titolare nella dimostrazione dei propri obblighi.
Non solo, perché la responsabilizzazione avviene anche con l'imposizione di altri doveri: il personale dipendente che a vario titolo ponga in essere, per il titolare e nell'ambito dell'organizzazione di quest'ultimo, operazioni di trattamento deve, in qualche modo, essere "inquadrato" nell'ambito di ruoli e funzioni che consentano di dare conto delle scelte effettuate dal titolare.
L'art. 4, c. 1, lett. h) del Codice Privacy del 2003, abrogato a seguito delle disposizioni contenute nel D.Lgs. 101/2018, contemplava espressamente la presenza e insieme la necessità di individuare, autorizzare e istruire gli "incaricati", ossia le "persone fisiche autorizzate a compiere operazioni di trattamento".
La formulazione dell'art. 29 del Reg. Europeo nr. 679/2016, a mente del quale "il responsabile o chiunque agisca sotto la sua autorità o sotto quella del titolare … che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso …", aveva fatto sorgere alcuni dubbi sulla compatibilità della menzionata figura degli "incaricati" con il nuovo testo europeo[29].
Tuttavia, proprio la lettura del menzionato art. 29 porta a ritenere che chiunque possa accedere ai dati personali (trattati dal titolare o dal responsabile) debba essere specificamente autorizzato e, come vedremo, adeguatamente istruito.
L'art. 32, 4., in tema di sicurezza del trattamento, conferma infatti a chiare lettere che il titolare e il responsabile del trattamento devono far 'sì "che chiunque agisca sotto la loro autorità e abbia accesso ai dati personali non tratti tali dati se non è *istruito in tal senso*…".
Con l'entrata in vigore, nel settembre 2018, delle disposizioni di adeguamento del C.P. di cui al D.Lgs. 101/208 e, in particolare, con l'introduzione dell'art. 2 – *quaterdecies* nel D.Lgs. 196/2003, che prevede l'attribuzione "di funzioni e compiti a soggetti designati", gli eventuali dubbi in ordine alla possibilità (o meglio: necessità) di individuare specificamente i soggetti autorizzati al trattamento dei dati personali e di fornire loro specifiche istruzioni, sono svaniti.
Ne deriva che, si tratti di titolare o di responsabile, allorché nell'ambito dell'organizzazione di uno di questi (o meglio: sotto la diretta autorità di uno di essi) un soggetto acceda o comunque tratti dati personali, anche questi debba essere non solo espressamente autorizzato, ma anche debitamente istruito.
Tali istruzioni dovranno, come si vedrà a breve, anche prevedere obblighi e doveri in caso di eventi particolari, come avviene nel caso di incidenti.
Obblighi in tal senso sono previsti sia nell'art. 28 laddove è precisato che il responsabile deve garantire che le persone che abbia incaricato di lavorare per lui siano, a loro volta, in questa catena di sviluppo che può divenire molto estesa, non

---

abbiano un adeguato obbligo legale di riservatezza; c) adottare tutte le misure previste dall'art. 32; rispettare le condizioni per ricorrere ad altri responsabili; e) assistere il titolare nella predisposizione delle adeguate misure di sicurezza tecniche e organizzative al fine di dare seguito alle richieste di esercizio dei diritti da parte degli interessati, ecc..

[29] V. A. D'OTTAVIO, Ruoli e funzioni privacy principali ai sensi del regolamento: Cap. VI, in *Circolazione e Protezione dei Dati personali, tra Libertà e Regole del Mercato, Commentario al Reg. Eu n. 679/206*, cit., pagg. 178 e ss..

solo debitamente autorizzate, ma anche che si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale in tal senso[30].
Sul responsabile, di fatto, devono essere riversati gli obblighi e i doveri imposti in materia di protezione dei dati riguardanti gli interessati, senza che, da qualche parte, in qualche momento, possa trovarsi una falla: uno degli importanti obblighi che il rapporto tra titolare e quest'ultimo deve prevedere, infatti, è anche quello sancito dalla lettera f) dell'art. 28 già visto sopra: il responsabile deve assistere il titolare e assicurare una corretta gestione degli incidenti.

4. Gli articoli 33 e 34 del GDPR: notifica all'Autorità di Controllo e comunicazione all'interessato. Il ruolo e gli adempimenti del responsabile.

Il Regolamento generale sulla protezione dei dati personali introduce l'obbligo di notificare una violazione all'autorità di controllo nazionale competente (oppure, in caso di violazione transfrontaliera, all'autorità capofila) e, in alcuni casi, di comunicare la violazione alle singole persone i cui dati personali sono stati interessati dall'evento[31].
Come accennato nel paragrafo n. 2, un *data breach*[32] può essere classificato, sulla base dei principi di sicurezza delle informazioni (accidentale o illecito che sia), come:

a) una violazione della *riservatezza*, quando i dati siano divulgati o a essi accedano soggetti non autorizzati;

b) una violazione della *disponibilità*, laddove i dati siano persi, distrutti, o vi siano accessi accidentali o abusivi;

c) una violazione della *integrità*, allorché le informazioni siano modificate in carenza di autorizzazione o, comunque, accidentalmente[33].

In caso di violazione di dati personali il titolare del trattamento, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, è tenuto a:

i) notificare la violazione al Garante, a meno che sia improbabile che essa comporti un rischio per i diritti e le libertà fondamentali dell'interessato (art. 33);

ii) allorché la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà dell'interessato, il titolare deve anche comunicare a tale soggetto, sempre senza ingiustificato ritardo, la violazione (art. 34).

---

30 Art. 28, par. 3, lett. g).

31 Insieme ovviamente agli articoli 33 e 34 del Regolamento, il documento più rilevante in tema di incidenti è costituito dalle Linee Guida del Gruppo di Lavoro Art. 29 (WP29), oggi sostituito dal più volte menzionato EDPB. Nella versione emendata e adottata il 6 febbraio 2018, il Gruppo rileva come "mentre tutte le violazioni di dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono necessariamente violazioni di dati personali". Il documento è scaricabile al seguente link: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

32 Il Considerando 85 del GDPR recita: "Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che l(e) riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata."

33 Cfr. C. GALLOTTI, Sicurezza delle informazioni, valutazione del rischio, i sistemi di gestione, la norma Iso/Iec 27001, Lulu, versione gennaio 2019, pagg. 9 e ss..

In ogni caso il titolare è tenuto anche a:

iii) documentare qualsiasi violazione dei dati personali, tenendo traccia delle stesse e annotando quanto previsto dall'ultimo paragrafo dell'art. 33[34].

E' importante rilevare, anche per le implicazioni di cui si discute in questo scritto, che, a propria volta, "il responsabile del trattamento informa il titolare senza ingiustificato ritardo (*without undue delay*) dopo essere venuto a conoscenza dell'avvenuta violazione" (art. 33, 2.).

Mentre dunque il titolare deve, nei casi sopra visti (possibile rischio per i diritti e le libertà delle persone fisiche), notificare l'accaduto all'Autorità e, ulteriormente, in talune ipotesi (allorché il rischio sia elevato), anche comunicare il fatto al diretto interessato, il tutto "senza ingiustificato ritardo e in ogni caso entro 72 ore dal momento in cui ne è venuto a conoscenza", d'altro canto il responsabile, invece, è tenuto ("solamente" si potrebbe dire parafrasando i commentatori di lingua inglese che si riferiscono a tale incombente come a *the sole notification duty of the processor*[35]) a rivolgersi al solo titolare[36].

Appare immediatamente evidente che la tempestività della comunicazione del responsabile al titolare sia essenziale, non solo per consentire a quest'ultimo di valutare gli adempimenti impostigli e, di conseguenza, agire conformemente alle norme ma, in generale, per consentire un intervento con le modalità più opportune, in relazione ai propri processi di valutazione, prevenzione, gestione e risposta all'incidente.

Un primo aspetto che pare opportuno valutare è, innanzi tutto, l'individuazione del momento in cui si verifichi il "venire a conoscenza" dell'incidente.

---

[34] L'art. 33, 5. prevede che il siano documentate, oltre alla violazione in sé, quanto meno "le circostanze della stessa, le sue conseguenze e i provvedimenti adottati per porvi rimedio." Ciò anche al fine di consentire "all'autorità di controllo di verificare il rispetto del presente articolo."

[35] Cfr. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-decoding-the-date-controller-and-processor-relationship-in-a-data-breach.pdf.

[36] L'art. 34 si occupa di precisare i contenuti e la portata della comunicazione all'interessato: "(1) Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo. (2) La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d). (3) Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni: a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura; b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1; c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia. (4) Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta."

Le Linee Guida dell'ex Gruppo di Lavoro 29 hanno chiarito che tale momento è quello nel quale il soggetto che ha subito la violazione raggiunge una "ragionevole contezza dell'accaduto"[37].
Ne consegue l'onere per i titolari (ma anche per i responsabili) di una adeguata predisposizione di misure tecniche e organizzative che consenta di poter avere una tale contezza con tempistiche che rendano possibile attivarsi come richiesto[38].
Abbiamo già rilevato come anche il responsabile cui siano affidate operazioni di trattamento dei dati personali sia tenuto a organizzarsi in modo tale da potersi rendere conto del fatto che abbia, o possa aver subito, una violazione: si tratta, in realtà, di un vero e proprio obbligo, derivante dal principio dell'*accountability* e, più in particolare, dalla ricordata previsione inserita nell'art. 28 al par. 3, laddove è imposto che, nella regolamentazione dei rapporti tra titolare e responsabile, quest'ultimo debba necessariamente essere vincolato ad assistere il titolare negli adempimenti necessari al rispetto delle prescrizioni di cui agli articoli da 32 a 36 e, pertanto, per tutto ciò che concerne non solo la sicurezza del trattamento (art. 32), ma anche le conseguenze derivanti dagli incidenti di cui discutiamo (artt. 33 e 34); non per ultime, anche per le procedure relative all'effettuazione della valutazione di impatto (artt. 35 e 36).
Sebbene, come visto, il responsabile debba "solo" avvertire il titolare, ciò deve fare, però, "senza ingiustificato ritardo".
Pur non essendo dunque fissato un preciso termine temporale entro il quale comunicare l'accadimento (a differenza di quanto previsto per gli obblighi del titolare), il Gruppo di lavoro Articolo 29 raccomanda che i responsabili notifichino *prontamente*[39] l'accaduto, corredando la comunicazione con ulteriori informazioni che coadiuvino il titolare nella gestione, eventualmente anche per fasi, mano a mano che anch'essi raccolgano evidenze o che effettuino le relative investigazioni.
Ciò corrisponde all'onere imposto al titolare di effettuare l'eventuale comunicazione in ogni caso senza ritardo e al più tardi nelle 72 ore da quando abbia raggiunto una ragionevole certezza, con la precisazione che gli è consentito, se del caso, effettuare una prima notifica e, successivamente, man mano che il dettaglio di quanto avvenuto si chiarisca, specificare ulteriormente il contenuto del proprio rapporto[40].
Come evidente, quanto sopra è essenziale anche al fine di coadiuvare il titolare nell'osservanza del termine per la notifica alla Autorità di controllo nelle previste 72 ore.
E' noto come, non da oggi e certamente in ancora di più in futuro, le organizzazioni coinvolgano ampiamente e regolarmente terze parti per una vasta platea di servizi, prestazioni e soluzioni di elaborazione, archiviazione e, in generale, per il trattamento di dati: siano esse soluzioni basate su cloud, su piattaforme, su applicazioni web o

---

37 "*A controller should be regarded as having become aware when that controller has a reasonable degree of certainty that a security incident has occured that has led to personal data being compromised*": Linee Guida sul data breach, versione febbraio 2018, citt. alla nota n. 31.
38 V. gli esempi contenuti nelle Linee guida citate, pagg. 11 e 12.
39 "*Promptly*": cfr. Linee Guida citt..
40 "*In most cases these preliminary actions should be completed soon after the initial alert (i.e. when the controller or processor suspects there has been a security incident which may involve personal data.) – it should take longer than this only in exceptional cases*", ibidem.

mediante software, il mercato è oggigiorno inestricabilmente collegato da una pluralità di servizi interconnessi.
Un incidente lungo la filiera di questi trattamenti, laddove coinvolga dati personali, deve essere gestito secondo quanto stabilito dalle norme che stiamo esaminando[41].
Il titolare del trattamento rimane certamente il soggetto sul quale incombono e permangono gli obblighi generali della protezione dei dati personali ma, come rilevato anche nelle Linee Guida europee, il responsabile del trattamento ha un ruolo importante per consentire al titolare di adempiere ai propri obblighi.
L'articolo 33, par. 2 chiarisce che se il responsabile viene a conoscenza di una violazione dei dati personali trattati per conto di altri, deve notificare l'accaduto al titolare "senza indebito ritardo": a differenza del titolare egli non ha l'obbligo, cui abbiamo accennato e di cui tra poco, di valutare la probabilità di un rischio derivante agli interessati (e, tanto meno, di un eventuale elevata gravità dello stesso): egli deve solo stabilire se si è verificata una violazione e quindi informare il titolare.
Il WP 29[42] precisa che "il titolare del trattamento dovrebbe essere considerato 'consapevole' una volta che il responsabile del trattamento lo abbia informato della violazione."
Come accennato e come evidente, un tale obbligo del responsabile, adempiuto senza ritardo, consente al titolare del trattamento di porre rimedio alla violazione e di determinare se sia tenuto o meno a effettuare la notifica all'autorità di controllo nonché eventualmente la comunicazione alle persone interessate.

5. La valutazione del rischio determinato dall'incidente. Cenni. Conseguenze sull'obbligo del responsabile

Si accennato, ed è intuibile, che un *data breach* configura una tipologia di incidente di sicurezza avente ad oggetto dati personali.
Ne deriva, come conseguenza, che si tratta di una ipotesi in cui, di fatto, il titolare del trattamento non è in grado o non è stato in grado di proteggere i dati personali come richiesto, invece, dalle norme: l'art. 32 del Regolamento europeo impone, in questo caso sia al titolare sia al responsabile, di mettere in atto misure tecniche e

---

[41] Per la verità e per completezza non possono non ricordarsi le prescrizioni introdotte dalla normativa NIS – Cyber: il 26 luglio 2016 è entrata in vigore la direttiva UE n. 1148/2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi. La direttiva è stata recepita in Italia con il decreto legislativo 18 maggio 2018, n. 65. La cyber security è stata ulteriormente regolata col recente decreto legge 21 settembre 2019, n. 105, che ha specificato le norme citate e stabilito Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica. Tali norme, destinate agli OSE, Operatori di Servizi Essenziali e ai FSD, Fornitori di Servizi Digitali (artt. 4 e 5 direttiva), contengono previsioni per l'adozione di misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi; all'adozione di misure adeguate per la prevenzione e minimizzazione dell'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali, per assicurarne la continuità; l'adozione di una procedura di notifica *senza indebito ritardo* all'autorità competente o al CSIRT in relazione agli incidenti aventi un impatto rilevante sulla continuità dei servizi prestati. Recentemente, come vedremo oltre, la Commissione ha pubblicato una proposta di aggiornamento della direttiva (NIS 2): https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union.
[42] WP 29, ossia *Working Party article 29*, deriva dall'art. 29 della direttiva 95/46/CE, che istituì il Gruppo di Lavoro, oggi divenuto *European Data Protection Board*.

organizzative "adeguate", tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'ambito, del contesto e delle specifiche finalità perseguite, ma anche dei rischi che il trattamento può comportare rispetto ai diritti e alle libertà degli interessati.
Il tema della sicurezza è centrale nella normativa di protezione dei dati personali ed è configurato, diversamente rispetto al passato, mediante lo "strumento" dell'*accountability*, non con una analitica elencazione di misure di sicurezza[43], bensì e in un certo qual modo all'opposto, lasciando (meglio sarebbe dire: imponendo) al titolare e al responsabile del trattamento, la scelta di quali siano, nello specifico contesto di riferimento, le misure, appunto, adeguate e idonee[44] ad affrontare e mitigare il rischio derivante dal trattamento. In pari tempo e proprio a motivo di tale libertà di scelta delle misure, laddove richiesti, i soggetti prima indicati (titolare e responsabile), dovranno essere in grado di comprovarne l'adeguatezza, come previsto dall'art. 5 par. 2[45].
Per quanto concerne, in particolare, la scelta, da parte del titolare, dei propri fornitori, *vendors*, *outsourcers* e, quindi, della "catena" di ausiliari, deve ribadirsi, come già notato, che l'art. 28 è molto chiaro nello stabilire una lunga serie di requisiti che essi devono avere o di garanzie che devono fornire; tra queste anche l'ausilio al titolare nella gestione di un incidente[46].
Ricordato che il responsabile è tenuto a comunicare al titolare l'accadimento senza ritardo e non appena a conoscenza della violazione, può accadere, nella pratica, che vi sia la necessità di indagare con uno o più livelli di maggiore dettaglio: ciò anche perché potrebbe non essere immediatamente possibile, nello specifico, conoscere con un sufficiente grado di specificazione i fatti e le circostanze non solo rilevanti, ma anche necessarie e utili per provvedere a quanto richiesto; è ben vero che il responsabile deve comunicare senza ritardo l'evento non appena ne abbia una ragionevole conoscenza ma, nel contempo, egli dovrà certamente coadiuvare il titolare nel complesso delle attività comunque richieste: non solo comunicando l'evento ma anche fornendo ausilio per la messa in atto delle necessarie procedure di riposta[47].

---

[43] Il riferimento è alle "vecchie", oggi abrogate, Misure minime di sicurezza di cui al D.Lgs. 196/2003.
[44] Si parla, al riguardo, di approccio *risk based*.
[45] Non è questa la sede per affrontare, ulteriormente, i profili riguardanti il c.d. P.I.A., *Privacy Impact Assessment* o il D.P.I.A., *Data Protection Impact Assessment*, la Valutazione di impatto sulla protezione dei dati, che riguarda i trattamenti, come previsto dall'art. 35 del GDPR e dai provvedimenti sia europei sia dell'Autorità italiana, che presentino un "rischio elevato" per i diritti e le libertà delle persone fisiche: si veda F. SARTORE, *La valutazione di impatto nel GDPR*, in *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, cit, pagg. 333 e ss..
[46] Vale la pena sottolineare la recente pubblicazione, da parte della Commissione Europea, delle clausole contrattuali standard, quale modello per regolare, alla luce dell'articolo 28 del GDPR, il rapporto contrattuale tra titolare e responsabile del trattamento dei dati. La loro adozione non è un obbligo, ma è certamente un utile strumento, anche perché evidentemente rappresentano uno standard cui le istituzioni europee mirano in relazione agli accordi tra titolari e responsabili: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12740-Data-protection-standard-contractual-clauses-between-controllers-processors-located-in-the-EU-implementing-act-
[47] Le metodologie e i processi di risposta agli incidenti sono molteplici e dipendono da diversi fattori che fanno sostanzialmente capo alla scelte aziendali. E' peraltro generalmente comune la previsione di un *Response Team*, composto non solo dal Titolare e, nei casi in cui gli incidenti siano relativi ad attività commissionate a fornitori, anche di questi ultimi, ma anche, laddove presente, del *DPO* – RPD, del

Ciò nondimeno è essenziale che la comunicazione (*notify*) al titolare avvenga senza ritardo ma, se del caso, successivamente precisata e approfondita.
Nelle clausole contrattuali (o nei contratti di tipo DPA) è dunque necessario che sia stabilito un termine assai breve, imposto al responsabile, al fine della comunicazione: nella pratica, in effetti, si possono notare differenze che vanno da poche ore a un giorno o due, in dipendenza del settore di riferimento (si pensi ai settori finanziari o sanitari), della tipologia di dati trattati (dati comuni o di carattere particolare, oppure relativi a minori) nonché della stessa tipologia di accadimento (accidentale o "malevolo") ma anche ovviamente del potere contrattuale a disposizione delle parti: è evidente che un termine di poche ore potrebbe essere preteso da un titolare forte nei confronti di un proprio fornitore, mentre al contrario, un responsabile in posizione avvantaggiata (si pensi ad un cloud provider, o a un fornitore di un servizio web based nei confronti di una piccola o media impresa), potrebbe avvantaggiarsi nell'ottenere termini maggiormente dilatati.
Il concreto assetto di tale specifico aspetto della contrattazione tra le parti coinvolte dipende spesso anche dal livello di consapevolezza e di adeguamento delle stesse: imprese strutturate e particolarmente attente ai temi della protezione delle informazioni si sono da tempo dotate di policy e procedure anche per la gestione delle terze parti, in cui vengono attentamente definiti gli obblighi e i doveri, anche di dettaglio, come del resto risulta essere sempre più richiesto a livello europeo[48].
In ogni caso una corretta distribuzione degli oneri e, soprattutto, delle tempistiche di comunicazione in caso di incidente consente una più agevole gestione della valutazione del rischio conseguente allo stesso, necessaria al fine di valutare se sussistano gli obblighi più volte visti: notifica all'autorità e comunicazione all'interessato.
Nell'ottica della tutela e protezione delle persone fisiche, infatti, la valutazione del rischio che un incidente di violazione può comportare è infatti essenziale.
Una violazione può infatti potenzialmente avere un insieme di effetti negativi che possono concretizzarsi in danni materiali ma anche immateriali[49].
Il GDPR specifica che tali conseguenze includono, tra le altre: la perdita del controllo sui propri dati personali; la limitazione dei diritti degli interessati; la discriminazione; il furto di identità; la frode; la perdita finanziaria; la possibile identificazione di un soggetto pseudonimizzato; il danno alla reputazione; la perdita della riservatezza sui

---

Responsabile della Protezione dei Dati, che si occupa della fase di "valutazione" del *privacy incident* e dell'eventuale fase di notifica; altrettanto presenti sono generalmente i fornitori IT esterni, che si occupano della gestione dei sistemi loro affidati, nonché del *CISO*, o *Chief Information Security Officer*, che si occupa della sicurezza IT e degli eventuali incidenti di sicurezza sui sistemi. Laddove implementati standard BCMS, *Business Continuity Management System*, come previsto dallo standard ISO 22301:2019, vengono osservati i requisiti necessari alla protezione e riduzione della probabilità di accadimento degli incidenti e ottimizzati i tempi di risposta e ripristino delle attività a seguito di eventi destabilizzanti. Come detto, sostanzialmente (e molto succintamente), le metodologie e i processi tendono a realizzare processi di gestione che rispondano alle necessità di *detect*, *respond*, *recover*.

[48] Cfr. nota precedente: le clausole in questione contengono numerose specificazioni al riguardo.

[49] Può essere utile ricordare che, differentemente da quanto avviene nella procedura di cui all'rt. 35 relativa alla valutazione di impatto del trattamento sulla protezione dei dati, laddove sono considerati sia i rischi determinati dal trattamento per come è stato programmato dal titolare sia i rischi che deriverebbero da un eventuale incidente e che deve essere effettuata prima che il trattamento abbia inizio, per quanto riguarda il *data breach* la valutazione del rischio che questo possa comportare è successiva, nel senso che l'evento si è già verificato.

dati personali protetti da segreto professionale; ogni altra perdita economica o svantaggio sociale significativo per l'interessato.
Il titolare, ogni qualvolta abbia conoscenza di un incidente di violazione, deve valutare se esso comporti o meno un rischio e, in caso positivo, ulteriormente valutare se tale rischio sia elevato.
Il livello di rischio è definito sulla base dei parametri della *i) probabilità*, intesa come il grado di possibilità che la violazione segnalata presenti un rischio e della *ii) gravità*, intesa come la rilevanza degli effetti pregiudizievoli che la violazione segnalata è in grado di produrre.
Ai fini della identificazione dei valori da attribuire ai predetti due parametri per la valutazione del rischio[50], si prendono generalmente in considerazione fattori come il tipo di violazione in merito alla riservatezza, integrità e disponibilità dei dati personali; la natura, sensibilità e volume dei dati personali oggetto di violazione; il numero degli interessati coinvolti dalla violazione; la facilità nella identificazione degli interessati; le gravità delle conseguenze per gli interessati; la particolarità degli interessati (come ad esempio i minori o soggetti particolarmente vulnerabili).
La probabilità e la gravità sono stimate qualitativamente[51]: la probabilità è intesa come il grado di possibilità che la violazione comporti un rischio per i diritti e le libertà delle persone (grado suddiviso in basso, ossia l'evento temuto non dovrebbe manifestarsi; medio, l'evento temuto potrebbe manifestarsi, alto: l'evento temuto ha una alta probabilità di manifestarsi). Per quanto riguarda la gravità, essa viene rapportata all'impatto della violazione sui diritti e le libertà delle persone fisiche coinvolte, anche in questo caso come un impatto basso, un impatto medio, impatto poco significativo, reversibile, ovvero alto, significativo, irreversibile.
Il livello di rischio deriva dalla risultante del rapporto tra probabilità e impatto[52].
Recenti ricerche hanno evidenziato come la compromissione di credenziali, l'errata configurazione di sistemi di archiviazione in cloud abbiano rappresentato, insieme alla sfruttamento di vulnerabilità presenti in software di terze parti, le cause più comuni e frequenti di *data breach*[53].

6. Gli incidenti dovuti ad attività illecite commesse da dipendenti

Come abbiamo rilevato in precedenza, sia il titolare sia il responsabile devono fare in modo che chiunque agisca sotto la loro responsabilità non tratti dati personali "se non è istruito in tal senso"[54]. In pari tempo essi devono prevedere, "sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e

[50] Tra le metodologie più note e accreditate seguite per la valutazione del rischio che un incidente comporta non può non segnalarsi quella di ENISA, pubblicata nel 2013: https://www.enisa.europa.eu/publications/dbn-severity.
[51] Cfr. C. GALLOTTI, cit., pag. 63.
[52] Le più volte citate Linee Guida WP 29 contengono un utile appendice di casi esemplificativi di eventi che possono comportare, o al contrario non richiedono, rispettivamente, notifica e comunicazione.
[53] Cfr.: https://www.ibm.com/security/data-breach;
https://www.csoonline.com/article/3434601/what-is-the-cost-of-a-data-breach.html.
[54] Cfr. art. 29 GDPR.

funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità"[55].
Ciò significa, innanzi tutto, che per la legittimità di ogni trattamento eseguito nell'ambito della sfera di influenza del titolare o del responsabile da parte di specifici soggetti, questi ultimi debbano, primariamente, essere debitamente e specificamente autorizzati[56].
Ma non basta, giacché tali soggetti non devono solamente essere autorizzati, ma anche debitamente istruiti e formati: una rilevante parte della formazione del personale è relativa alla corretta gestione degli accadimenti che possano costituire incidenti[57]: la formazione e la sensibilizzazione del personale sono essenziali ai fini del rispetto dei principi di protezione dei dati personali e costituiscono un obbligo di *accountability* per titolari e responsabili[58].
Tuttavia, nonostante il titolare o il responsabile abbiano provveduto e provvedano alla formazione del proprio personale autorizzato al trattamento dei dati personali, gli incidenti accadono: siano essi accidentali o meno, è necessario prevedere sistemi di gestione e reazione, come accennato in precedenza.
Limitando l'analisi ad eventi di tipo "malevolo" e, pertanto, di natura illecita, vengono in rilievo possibili comportamenti illegittimi di dipendenti i quali, violando le istruzioni loro impartite, si impossessino di informazioni cui abbiano accesso o, ancor peggio, accedano a informazioni cui non avrebbero dovuto aver accesso.
In relazione a ipotesi come quelle appena indicate, laddove esse accadano non nella diretta sfera di controllo del titolare ma del responsabile cui sono affidate determinate operazioni, ben si comprende come ne derivino problematiche di diverso genere.
Senza pretesa di completezza è possibile indicare, quali comportamenti costituenti reato: la frode informatica (art. 640 *ter* del codice penale), consistente nell'alterazione di un sistema informatico allo scopo di procurarsi un ingiusto profitto; l'accesso abusivo ad un sistema informatico o telematico (art. 615 *ter* c.p.); la detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici (art. 615 *quater* c.p.); la diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 *quinquies* del c.p.).

7. L'esfiltrazione di dati personali operata da un soggetto in veste di autorizzato al trattamento presso il Responsabile

Limitando la presente analisi all'ipotesi del comportamento di un soggetto che acceda a, e si appropri di, sottraendoli, dati personali allorché alle dipendenze di una persona

---

55 Cfr. art. 2 *quaterdecies* D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018.
56 Si veda G. ZICCARDI, *GDPR e set di istruzioni per i soggetti che trattano dati: l'uso degli strumenti informatici, la gestione dei possibili data breach e la protezione dal phishing*, in Diritto di Internet, n. 1/2019, pagg. 223 e ss., Pacini Giuridica, Pacini Ed., Pisa: l'Autore ricorda come la prima funzione delle autorizzazioni di cui nel testo sia, in effetti, quella di "realmente formare, istruire e preparare i soggetti a un trattamento di dati sicuro", mentre la "seconda funzione, esterna", sia "quella di mostrare in ogni momento l'attenzione del titolare a tali temi, in un'ottica di accountability che sia dimostrabile".
57 Cfr. G. SIRONI, *Il DPO e la formazione*, in *Gli adempimenti del DPO* (a cura di S. RICCI e G. VACIAGO), pagg. 97 e ss..
58 Cfr. G. ZICCARDI e P. PERRI (a cura di), *Tecnologia e diritto*, Vol. III, G. F. Lefebvre, Milano, 2019, pagg. 263 e ss..

fisica o giuridica, di un'autorità pubblica, di un servizio o di un altro organismo che tratti dati per conto di un titolare[59], risulta evidente come un adeguato *assessment*, anche di tipo preventivo ma ovviamente e soprattutto reattivo, possa aiutare nella gestione di un incidente di tale tipo, consentendo, in prima battuta al responsabile, di onorare gli adempimenti sullo stesso pendenti sia, in un secondo tempo, al titolare di effettuare per tempo la complessa e complessiva valutazione dell'evento al fine non solo di mitigarlo ma anche di adempiere, se del caso, agli obblighi di notificazione e comunicazione.
Una esfiltrazione di dati personali può essere sostanzialmente definita come una esportazione non autorizzata di informazioni da un sistema: si tratta di un insieme di possibili eventi e di circostanze che possono avere gravi conseguenze, sia in relazione all'integrità e disponibilità dei dati sia, soprattutto, in relazione alla loro riservatezza[60]. Mentre infatti gli incidenti che comportano la modifica delle proprietà di accuratezza e completezza e, quindi, dell'integrità delle informazioni e quelli che causano una temporanea o permanente mancanza di disponibilità sono, in generale, probabilmente più semplici da rilevare, talvolta, invece, le violazioni che causano la perdita della riservatezza delle informazioni possono risultare più ardue da accertare[61]; in ogni caso, laddove il soggetto tratti dati per conto di altri, ne risulta una complicazione per entrambi i soggetti coinvolti: per il titolare ma anche appunto per il responsabile[62].
In caso di infedeltà di un dipendente che si appropri, esportandoli o copiandoli, di dati personali, è evidente come i rischi che ne possono derivare siano notevoli e diversi, pur dipendendo da molteplici fattori.
Si pensi a dati personali anche (solo) di tipo "comune", come possono essere dati anagrafici (nome e cognome, numero di telefono, codice fiscale e account email, luogo di residenza, data di nascita, ecc.): mediante correlazione e interrelazione di tali dati potrebbero essere possibili furti o sostituzioni di identità, anche legati ad accessi ad account configurati tramite i dati, oppure mediante *phishing*. Aggregare coerentemente dati di questo tipo non risulta affatto, oggigiorno, problematico per un soggetto che abbia, oltre che intenzioni malevole, un minimo di conoscenze specialistiche[63].

---

[59] Così la definizione di responsabile all'art. 4, 8), del GDPR.
[60] Esistono e sono generalmente utilizzate diverse metodologie per la *detection* di un incidente: sommariamente può rilevarsi come alcune di esse vengano effettuate da persone fisiche (utenti, clienti, persone esterne), mentre altre siano affidate al controllo di sistemi tecnologici (firewall, IDS/IPS, sistemi di DLP, *Data Loss Prevention*, antivirus, ecc.).
[61] Si veda C. GALLOTTI, cit., sulle tecniche di minaccia, pagg. 111 e ss..
[62] Cfr. C. CRISCUOLI e V. GIUFFRÈ, *Come prepararsi e reagire a un data breach di un sistema di intelligenza artificiale?*, in *Come preparare la propria azienda alla digital revolution*, Dip. I.P.T. Studio Legale DLA Piper (a cura di), Wolters Kluwer Italia, 2020, pagg. 53 e ss. i quali ricordano non solo l'importanza della gestione dei flussi di comunicazione aziendale al fine di sensibilizzare le funzioni aziendali in caso di incidenti, ma suggeriscono anche l'istituzione di "canali di comunicazione fra i diversi dipartimenti competenti affinché vengano prontamente segnalate le problematiche emergenti", nello specifico relative alla sicurezza dei sistemi di I.A. e ribadiscono la necessità, in presenza di fornitori, di adeguate cautele in sede di redazione degli accordi di cui all'art. 28 GDPR.
[63] Cfr. P. DAL CHECCO e A. LONGO, *Ho Mobile, tutti i rischi per gli utenti dopo il furto dati*: https://www.agendadigitale.eu/sicurezza/ho-mobile-tutti-i-rischi-per-gli-utenti-dopo-il-furto-dati/ (ultima consultazione in data 7/01/2021).

Per completezza deve ulteriormente aggiungersi, anche se non oggetto del presente scritto, che nel concetto di esfiltrazione di informazioni ben potranno farsi rientrare anche ipotesi più diversificate, come avviene ad esempio nei casi di *spoofing,* dove un soggetto mette in atto un complesso di comportamenti caratterizzati dal camuffamento allo scopo di alterare o avere accesso a informazioni cui non avrebbe diritto[64].

Episodi quali quelli qui solo sommariamente indicati, sempre più frequenti, come abbiamo visto, confermano la necessità di ripensare, ad ogni livello, la sicurezza informatica e la gestione delle problematiche che essa comporta[65]: appare evidente che le imprese dovranno sempre più essere in grado di conoscere nel dettaglio non solo le modalità mediante le quali una violazione si è verificata, ma anche predeterminare nel modo più attento possibile le forme di intervento e reazione: le analisi, anche forensi[66], post incidente, dei sistemi, possono e devono portare alla luce le evidenze che consentano di definire l'accaduto con il miglior grado di dettaglio possibile (si pensi ai file di log, alle tracce di accesso ai file, a database, Api, ecc.), senza dire che una corretta e completa contezza degli eventi, pur necessitando, probabilmente, diverse fasi di approfondimento, consentirà di gestire le nascenti obbligazioni di notifica alle autorità e di comunicazione ai singoli diretti interessati nel modo più opportuno[67].

Da un parzialmente analogo punto di vista vale la pena segnalare come una recente sentenza della Corte di Cassazione abbia stabilito la configurabilità del reato di appropriazione indebita la sottrazione definitiva di file o di dati informatici, attuata mediante duplicazione e successiva cancellazione da un personal computer aziendale, affidato a un soggetto per motivi di lavoro e, successivamente, restituito formattato[68]. La Corte chiarisce che i dati informatici, per struttura fisica, misurabilità delle dimensioni e trasferibilità, devono essere considerati come cose mobili ai sensi della legge penale: tiene conto del mutato panorama storico e informatico, consentendo di classificare come cosa mobile, possibile oggetto del reato in questione, anche elementi come i file e i dati, che non hanno le tradizionali caratteristiche di materialità e tangibilità dei beni mobili ordinariamente intesi. Per la verità la sentenza si ferma, in un certo senso, all'affermazione della configurabilità del reato solamente all'ipotesi di sottrazione definitiva, laddove, come forse utile, parrebbe giunto il momento di

---

64 Cfr. voce *Spoofing*, in *Dizionario Legal Tech*, G. ZICCARDI, P. PERRI (a cura di), G. F. Lefebvre, Milano, 2020.

65 Cfr. A. LONGO, *Leonardo, perché è gravissimo il furto di dati al nostro 'campione nazionale'*: https://www.cybersecurity360.it/cybersecurity-nazionale/perche-e-gravissimo-il-furto-di-dati-a-leonardo/ (ultima visita 8/01/2021).

66 In relazione alla complessa attività di analisi forense, non può che rimandarsi, per ogni rigerimento, al sito del dott. Paolo Dal Checco: https://www.dalchecco.it/.

67 Vale forse la pena ricordare che le comunicazioni di cui all'art. 34 del GDPR non devono essere inviate, nel caso, indistintamente a tutta la clientela dell'azienda interessata ma, se necessario, ai soli utenti o interessati coinvolti: cfr. anche Linee Guida WP 29 sul data breach più volte ricordate.

68 L'imputato, nello specifico, dopo essersi dimesso, veniva assunto da una nuova compagine societaria, operante nello stesso settore; prima di presentare le dimissioni aveva restituito il notebook aziendale con l'hard disk formattato, senza traccia dei dati informatici originariamente presenti, così provocando il malfunzionamento del sistema informatico aziendale e impossessandosi dei dati originariamente esistenti, che in parte venivano ritrovati nella disponibilità dell'imputato su computer da lui utilizzati: https://www.giurisprudenzapenale.com/wp-content/uploads/2020/04/cass-pen-2020-11959.pdf.

andare oltre: anche una copia non autorizzata potrebbe configurare l'ipotesi in discorso[69].
Ne deriva pertanto come un dipendente di un responsabile del trattamento ben potrebbe illecitamente appropriarsi di dati e informazioni trattate dal proprio datore di lavoro, con conseguente violazione di quanto previsto dall'art. 28, par. 3, lettere b) e c) del GDPR.
Ulteriore ipotesi degna di nota è quella, già anticipata, dell'accesso abusivo a sistema informatico, prevista dall'art. 615 *ter* del codice penale: il delitto si perfeziona allorché un soggetto acceda, senza autorizzazione, a un sistema informatico, anche a distanza, o vi si mantenga.
Come chiarito dalle Sezioni Unite della Cassazione (SS.UU. 27 ottobre 2011, n. 4694[70]) la questione dovrà essere riguardata sotto il profilo delle finalità perseguite da chi acceda o si mantenga nel sistema; le Sezioni compongono il precedente contrasto interpretativo ritenendo meritevole di sanzione anche il soggetto che (semplicemente) si introduca, o anche si mantenga nel sistema per finalità diverse rispetto a quelle consentite[71]: la rilevanza penale del comportamento discenderà da un accesso alle informazioni che vada oltre quelle che sono le istruzioni e le limitazioni impartite al soggetto[72].
Per quanto estremamente limitata, la superiore disamina vorrebbe però segnalare, come anticipato, la delicatezza del tema nascente da un incidente, malevolo od occasionale che sia, che accada nella sfera di controllo del responsabile: è ben vero che, ai sensi del Regolamento, una volta che questi ne abbia avuto un ragionevole grado di certezza, deve esclusivamente provvedere alla notifica dello stesso al titolare, ma non pare potersi dubitare che, nella gran parte dei casi, a causa della complessità dei rapporti e dei trattamenti spesso demandati a terzi fornitori, senza una fattiva e concreta collaborazione del responsabile, il titolare non sarà in grado di adempiere a tutte le prescrizioni originate dalla ricezione della notifica inviatagli: a partire dalla identificazione e classificazione dell'incidente, passando attraverso la mitigazione e il contenimento, il recupero e il ripristino, la registrazione dello stesso e di cui all'art. 33, 5) del GDPR, per finire alle notifiche e comunicazioni, non pare si possa negare l'importanza, a livello di *accountability*, anche per il responsabile, di prevedere apposite procedure di *response* nel caso di accadimenti relativi a dati trattati per conto d'altri, a maggior ragione laddove i titolari siano molteplici[73].

---

[69] Cfr. https://www.cybersecurity360.it/soluzioni-aziendali/file-e-dati-informatici-quali-tutele-contro-il-reato-di-appropriazione-indebita/, anche nelle conclusioni.
[70] https://www.penalecontemporaneo.it/upload/1361977389Cass%20201204694.pdf.
[71] E' del tutto normale che un dipendente sia fornito di nome utente e password per accedere al sistema aziendale: si tratta del c.d. sistema di autenticazione.
[72] Si tratta del noto caso di un dipendente di un tribunale che aveva fatto accesso al registro informatico delle notizie di reato e aveva preso visione di dati relativi a un procedimento penale di un conoscente, affidato a un P.M. diverso da quello presso il quale prestava servizio: cfr. B. INDOVINA, *Accesso abusivo a sistema informatico: l'interpretazione delle sezioni unite*, online su: http://www.medialaws.eu/accesso-abusivo-a-sistema-informatico-linterpretazione-delle-sezioni-unite/ (ultima consultazione in data 7/01/2021).
[73] Ciò che, del resto, è prescritto dal WP 29 nelle già citate Linee Guida: "*Where the processor provides services to multiple controllers that are all affected by the same incident, the processor will have to report details of the incident to each controller*".

Mette conto infine ricordare come il Gruppo ex art. 29 abbia da tempo rilevato come, in seno agli accordi tra titolare e responsabile, possa essere previsto che il responsabile abbia facoltà di provvedere alla notifica per conto del titolare, sebbene ovviamente nel rispetto delle tempistiche già viste: ciò può costituire, in molti casi, in dipendenza dei differenti contesti e delle particolari tipologie di trattamenti, un ausilio di cui tenere conto.

8. La recente proposta di Direttiva NIS 2

Merita qui brevemente segnalare come le istituzioni europee, consapevoli delle attuali esigenze e problematiche discendenti da sempre maggiori, più ampie, diversificate e sottili minacce, amplificate dalla pandemia da Covid-19[74], la quale ha ulteriormente ed esponenzialmente aumentato i rischi e le minacce in ambito informatico, abbia recentemente pubblicato, tramite la Commissione, a soli due anni dalla scadenza del termine per il recepimento della Direttiva NIS (2016/1148), una proposta tesa a rivedere e rinnovare quest'ultima, con importanti nuovi obblighi per gli operatori di quelli che dovrebbero divenire i servizi "essenziali e importanti"[75].
Tra altre rilevanti previsioni essa mira a rinforzare gli obblighi di sicurezza per i soggetti cui sarà applicabile, stabilendo un approccio alla gestione del rischio che dovrebbe prevedere un elenco di misure di sicurezza da applicare obbligatoriamente[76]. Restano fermi, al momento, gli adempimenti relativi agli obblighi di adozione di misure tecniche e organizzative adeguate e proporzionate alle minacce alla sicurezza delle reti e dei sistemi informativi e per minimizzare l'impatto di eventuali incidenti informatici.
Le misure nella proposta, peraltro, riconoscendo il mutato quadro di riferimento e di cui si è fatto cenno in precedenza, ampliano l'elenco delle misure da adottare nel processo di gestione dei rischi, comprendendo anche controlli sulla sicurezza informatica dei fornitori: tra le misure di *Cybersecurity risk management* è previsto, ad esempio, che esse includano "la sicurezza della catena di approvvigionamento, compresi gli aspetti relativi alla sicurezza riguardanti il rapporti tra ciascuna entità e i suoi fornitori o fornitori di servizi, come i fornitori di servizi di archiviazione ed elaborazione dati o i servizi di gestione della sicurezza" (art. 18, p. 2).
La questione della *security*, soprattutto laddove, come spesso obbligatoriamente accade, demandata a terzi, è dunque un argomento estremamente sensibile e delicato: soprattutto in settori di grande importanza[77].
In ogni caso appare evidente come le catene di fornitori e sub fornitori dovranno essere sempre più sensibilizzate, passando molto probabilmente da un atteggiamento di adeguamento al GDPR formale e "cartolare" ad uno più concreto e sostanziale, effettivo e fattivo, come del resto il Regolamento e altre normative richiedono[78].

---

[74] Cfr. https://www.enisa.europa.eu/topics/wfh-covid19.
[75] Cfr. nota n.41.
[76] A differenza del regime attuale di operatività, destinato ai Operatori di Servizi Essenziali (OSE) e ai Fornitori di Servizi Digitali (FSD). Cfr. anche https://dirittoaldigitale.com/2021/01/07/direttiva-nis-revisione/.
[77] Cfr. le al solito pungenti considerazioni di A. MONTI, sul suo blog: *Cosa insegna il "caso Leonardo"*, https://www.ictlex.net/?p=3313 (ultima visita: 7/01/2021).
[78] I provvedimenti sanzionatori del G.P. nel corso del 2020 hanno del resto evidenziato anche la necessità di un più attento controllo della filiera dei fornitori da parte del titolare.

9. Il tool *del Garante.*

Per finire questa analisi, certamente incompleta, vale la pena ricordare come recentemente il Garante Italiano abbia messo a disposizione, sul proprio sito, un *tool* di ausilio agli operatori: "gli utenti potranno accedere al modello di notifica al Garante e alla procedura di auto-valutazione (*self assessment*) che aiuta il titolare (ma anche il responsabile, *ndr*) nell'assolvimento degli obblighi in materia di notifica di una violazione dei dati personali all'autorità di controllo e di Comunicazione di una violazione dei dati personali all'interessato", il che conferma l'intenzione di modernizzazione e attualizzazione delle proprie attività e servizi, anche attraverso il *restyling* del logo istituzionale[79].

10. Le Linee Guida EDPB 1/2021: gli esempi in relazione alla notifica del data breach

Proprio mentre la Corte di Cassazione si esprime nuovamente, reprimendolo, in merito al comportamento del professionista che, lasciando uno studio professionale, effettui copia del database dei clienti per utilizzarlo nella propria nuova attività, qualificandolo come accesso abusivo a sistema informatico[80], il Board dei Garanti europei emana, in pubblica consultazione per sei settimane, interessanti e utili Linee

[79] Cfr. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9510133. Il tool, disponibile al link https://servizi.gpdp.it/databreach/s/, appare, *absit iniuria verbis*, un poco semplificato: probabilmente sarebbero utili indicazioni di maggior dettaglio. Ad ogni modo, utilizzandolo e cliccando, via via, nelle diverse fasi, allorché si giunge alla conferma di rivestire la qualifica di responsabile, il sistema restituisce quanto qui si riporta integralmente: *Autovalutazione per individuare le azioni da intraprendere a seguito di una violazione dei dati personali - Devi informare, senza ingiustificato ritardo, il titolare del trattamento circa la violazione dei dati personali occorsa. - Se l'incidente riguarda dati personali che tratti per conto di più titolari, devi informare ciascun titolare. - Se il titolare del trattamento ricorre a un responsabile del trattamento e quest'ultimo viene a conoscenza di una violazione dei dati personali allora «il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza di una violazione»; (cfr. art. 33Apertura sito esterno in una nuova scheda per l'articolo 33 del Regolamento (UE) 2016/679, par. 2, del Regolamento (UE) 2016/679 e art. 26 del D.Lgs 51/2018). - Le "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 3 ottobre 2017, come modificate e adottate in ultimo il 6 febbraio 2018 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018 (di seguito "Linee guida Apertura sito esterno in una nuova scheda per le Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679"), sottolineano che il responsabile del trattamento non è chiamato a valutare la probabilità che la violazione presenti un rischio per gli interessati. Il responsabile deve accertare se si è verificata una violazione e in caso positivo notificarla al titolare del trattamento senza ritardo. Nel caso in cui informazioni di dettaglio circa le cause e circostanze della violazione non siano tempestivamente disponibili, il responsabile informa tempestivamente il titolare circa l'avvenuta violazione, comunicando le informazioni di dettaglio in un momento successivo, non appena disponibili. - L'obbligo di comunicazione consente al titolare del trattamento di venire a conoscenza della violazione, di fronteggiarla in maniera tempestiva ed efficace e di stabilire, anche sulla base delle informazioni fornite dal responsabile, se la violazione deve essere notificata all'Autorità di controllo e comunicata agli interessati coinvolti.*

[80] Cfr. https://www.cybersecurity360.it/legal/cassazione-il-backup-dei-dati-effettuato-dallex-socio-e-accesso-abusivo-a-sistema-informatico/. Cfr. anche l'interessante raccolta di decisioni in tema al seguente link: https://sites.les.univr.it/cybercrime/index.php/accesso-abusivo-a-sistemi-informatici-illegal-access-to-computer-system/.

Guida contenenti diversi esempi pratici in relazione alle misure preventive, reattive e agli obblighi di notifica in caso di violazione dei dati[81].
Il provvedimento è destinato a completare e integrare le precedenti indicazioni del WP 29 sulla notifica di violazione dei dati[82] mediante raccomandazioni orientate alla gestione pratica degli incidenti, sia in relazione a misure preventive di *risk assessment*, sia in relazione ai comportamenti e alle valutazioni da eseguirsi *ex post*[83].
L'EDPB si rivolge ovviamente in prima battuta ai titolari del trattamento ma è del tutto evidente come la pubblicazione sia di grande aiuto anche nella complessiva valutazione e assessment dei trattamenti complessivamente considerati e, di conseguenza, anche nell'ottica di coloro che svolgano trattamenti "demandati", ossia dei responsabili: per quanto di loro competenza, infatti, nelle decisioni da adottare per gestire il *data breach*, anch'essi potranno trarre spunti e riferimenti utili, sia nella preventiva valutazione delle circostanze di rischio, sia nell'adozione di misure adeguate a, possibilmente, contenerlo.
Le Linee guida contengono, in particolare, un elenco dei casi di notifica di violazione dei dati ritenuti più comuni dalle autorità di controllo nazionali, come gli attacchi *ransomware*, gli incidenti derivanti dal furto o dallo smarrimento di dispositivi e, non per ultimi, i casi, considerati anche in questo scritto, di esfiltrazione di dati; ciò sia in relazione a servizi genericamente *web based*, sia anche in relazione a comportamenti di dipendenti infedeli.
Vengono presentate le *best practice* e forniti consigli su come identificare e valutare i rischi, evidenziando i fattori che dovrebbero essere presi in particolare considerazione; non mancano, ovviamente, indicazioni in merito alle concrete necessità di notifica alla Autorità Garante come anche di eventuale necessaria comunicazione ai singoli interessati.
Si tratta, a modesto avviso di chi scrive, a prima veloce lettura, di un documento che risulterà assai utile per tutti gli operatori del settore.
Viene, in particolare, nel capitolo relativo ai rischi derivanti dai fattori umani interni alle organizzazioni, preso in considerazione anche il caso, esemplificato, di un dipendente che durante il periodo di preavviso effettui copia di dati dal database del proprio datore di lavoro, cui abbia usualmente accesso nell'adempimento delle proprie mansioni e che, successivamente, impiegato altrove, utilizzi i dati copiati (prevalentemente costituiti da dati comuni, anagrafici e di contatto) proprio per contattare i clienti del proprio ex datore al fine di "invogliarli" a fare affari con lui.
Come anticipato il documento suddivide le indicazioni in temi diversi, in relazione a misure preventive e valutazione dei possibili rischi e, successivamente, di reazione e valutazione degli obblighi nascenti dal caso specifico.
In relazione alle misure preventive, in casi come quello appena indicato, l'EDPB riconosce innanzi tutto la difficoltà di adottare misure preventive, in primo luogo a motivo del fatto che il lavoratore ha, normalmente, legittimo accesso alle informazioni, proprio per la posizione che ricopre.
Ciò, all'evidenza, rende arduo impedire preventivamente fatti come quello considerato: limitare l'ambito di operatività del dipendente e non consentirgli la

[81] https://edpb.europa.eu/news/news/2021/edpb-adopts-guidelines-examples-regarding-data-breach-notification_it.
[82] Cfr. nota 31.
[83] V. anche quanto già brevemente anticipato alla nota 47.

disponibilità del database aziendale potrebbe significare impedire il normale svolgimento non solo dell'attività del lavoratore, ma anche il proseguimento del business latamente inteso.
Il Board, tuttavia, sottolinea come adeguate policy interne e rigorose procedure[84] autorizzative e formative siano, di fatto, un primo imprescindibile baluardo protettivo che il titolare deve porre in essere e implementare (ciò, ovviamente, vale anche per il responsabile che, a propria volta, è il titolare nei confronti del proprio personale).
Un adeguato risk assessment, pertanto, appare doveroso, come sempre tenuto conto non solo della tipologia di possibile incidente che potrebbe accadere, ma anche della natura, caratteristiche e volume dei dati nello specifico contesto trattati.
Come si è già rilevato[85] incidenti quali quello in considerazione costituiscono nella stragrande maggioranza casi violazioni della riservatezza[86].
Nonostante nell'ipotesi considerata nelle Linee Guida la quantità di dati esfiltrata non sia rilevante, non si tratti di dati di carattere particolare e si possa, inoltre, presumere che le finalità dell'ex dipendente possano limitarsi a eventuali contatti dei clienti dell'ex datore di lavoro, il Board ritiene tuttavia che quest'ultimo non sia, in effetti, nella posizione di sapere con esattezza quali siano le reali intenzioni dell'agente e le conseguenze che ne potrebbero derivare; esse, ad esempio, potrebbero andare oltre il mero contatto a fini promozionali e causare ulteriori e più gravi abusi[87].
Porre rimedio a casi simili non è facile, riconosce il Board[88].
Ciò presupporrebbe innanzi tutto una immediata contromisura di tipo legale volta a prevenire e impedire all'ex dipendente di commettere abusi e comunicare o diffondere ulteriormente i dati sottratti. Una tale azione potrebbe anche rivelarsi utile in casi futuri.
Di fatto, ad ogni modo, l'EDPB sottolinea come non esista una soluzione che possa dirsi valida in tutti i casi possibili e come, di conseguenza, sia di volta in volta, laddove possibile, necessario un approccio sistematico di tipo preventivo.
I Garanti europei suggeriscono, ad esempio, di prevedere particolari misure da applicare nelle ipotesi di dipendenti che abbiano annunciato le proprie dimissioni o che, comunque, stiano per lasciare l'azienda; in tali casi si potrebbe pensare, prosegue il Board, a particolari modalità di inibizione degli accessi a determinati settori del patrimonio informativo aziendale, oppure all'utilizzo di metodologie e software che consentano di monitorare e registrare determinati accessi, così come particolari clausole contrattuali appositamente redatte per vietare o limitare la disponibilità delle informazioni. Si tratta, ad avviso di chi scrive, di suggerimenti volti all'implementazione di sistemi e procedure, spesso di tipo automatico, di protezione cui abbiamo già fatto cenno[89].
Per finire questa breve analisi, il Board rileva come in casi come quelli considerati sia improbabile che la violazione possa comportare un rischio elevato per i diritti e le

---

[84] Si vedano il par. 6 e, in particolare, la nota 56.
[85] Cfr. par. 7.
[86] Cfr. Linee Guida cit., pag. 19 (73): "*these kinds of breaches are typically breaches of confidentiality, since the database is usually left intact, its content 'merely' copied for further use*".
[87] "*... further and more grave abuse of the stolen data is not ruled out*", *ibidem.*
[88] Cfr. pag. 20 (75).
[89] Cfr. nota 60.

libertà delle persone fisiche, per cui nella maggior parte dei casi la notifica all'Autorità Garante dovrebbe probabilmente essere sufficiente.
Tuttavia fornire informazioni e comunicare l'accaduto agli interessati potrebbe rivelarsi per il titolare una scelta opportuna: venire a conoscenza dell'accaduto da fonti diverse potrebbe costituire, ad esempio, un episodio in grado di ledere la reputazione aziendale, come avverrebbe nel caso di diretto contatto del cliente da parte dell'ex dipendente.
Infine i Garanti ribadiscono la necessità di una adeguata documentazione dell'accaduto sul c.d. "registro delle violazioni", come previsto dall'articolo 33, par. 5. del GDPR.

8 Febbraio 2021 – A.B.