RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 2-2020
DOI: 10.32091/RIID0020

La violazione dei requisiti di sicurezza informatica di cui all'articolo 32 del GDPR

Juan Sebastien Vanegas*

Allineare le misure di sicurezza informatica ai requisiti previsti dall'articolo 32 del GDPR costituisce una delle difficoltà principali che le organizzazioni devono affrontare nei loro processi di conformità complessiva al GDPR. Tale difficoltà è certamente giustificata da alcune criticità proprie del tema specifico delle misure di sicurezza, come ad esempio il vastissimo ambito in cui esse sono implementate, la grande diversità di misure implementabili e il necessario coinvolgimento di diverse figure professionali. L'articolo 32, inoltre, non precisa quali misure debbano essere implementate, né tantomeno quali misure possano considerarsi adeguate, ma si limita a fornire un elenco non esaustivo di possibili misure. Pertanto, un'analisi della giurisprudenza delle autorità di controllo europee può rappresentare un utile contributo sia per individuare con precisione le misure informatiche ritenute inadeguate (anche al fine di verificare l'applicazione uniforme dei criteri di sicurezza) che per accompagnare gli operatori di settore nei loro processi di conformità. Per raggiungere tale obiettivo, sono state analizzate diverse decisioni emesse da autorità di cinque paesi (Italia, Regno Unito, Spagna, Francia e Danimarca), e le vulnerabilità rilevate sono state raggruppate in macrocategorie: *accountability*, gestione degli accessi, utilizzo di applicazioni obsolete e protezione dei dati. Il quadro che emerge dall'analisi è un approccio sostanzialmente uniforme da parte delle autorità di controllo, le quali sembrano concordare sia sul carattere inadeguato di alcune misure rilevate sia sul carattere adeguato di misure alternative discusse nei provvedimenti. L'interesse sul tema potrebbe d'altronde essere esteso in un futuro lavoro all'analisi delle politiche sanzionatorie e correttive adottate dalle autorità.

GDPR – Misure di sicurezza – *Compliance* – Europa

1. Introduzione

Secondo un sondaggio condotto da una prestigiosa società, la difficoltà principale incontrata dalle imprese nel processo di adattamento al Regolamento (UE) 2016/679 (il "GDPR") è stata quella di allineare le proprie misure di sicurezza, predisposte a tutela dei dati personali trattati, ai parametri stabiliti dall'articolo 32 del GDPR[1]. Tale articolo, come noto, richiede ai titolari e ai responsabili del trattamento di implementare misure tecniche e organizzative adeguate per garantire un livello di sicurezza del trattamento adeguato al rischio[2]. Se questo è vero, il recente anniversario dei due anni di entrata in vigore del GDPR rappresenta dunque una buona occasione sia per ripercorrere rapidamente le principali vulnerabilità informatiche rilevate fino ad oggi dalle autorità di controllo europee, sia per analizzare nel merito i corrispondenti provvedimenti correttivi e sanzionatori adottati da quest'ultime. Per

*J.S. Vanegas è collaboratore presso lo studio Eversheds-Sutherland, LL.M. Queen Mary College, Master Protezione dei Dati Personali Università di Roma Tre. L'Autore ringrazia per i preziosi commenti il prof. Andrea Rossetti, professore associato di filosofia del diritto all'università Bicocca di Milano, e gli avvocati Massimo Maioletti e Andrea Zincone. Le valutazioni espresse nel presente articolo sono esclusivamente dell'Autore.

contestualizzare storicamente la normativa oggetto della presente analisi, si ricorda che il GDPR ha sostituito il precedente regime fondato sulla direttiva 95/46/CE, il cui articolo 17 disciplinava gli obblighi di sicurezza del trattamento dei dati personali[3]. Benché la Commissione Europea abbia affermato nel memorandum esplicativo sul GDPR la sostanziale continuità normativa fra l'articolo 32 del GDPR e l'articolo 17 della direttiva 95/46/CE[4], quest'ultima è stata a suo tempo recepita dagli Stati membri con formulazioni e tecniche diverse. Ad esempio, mentre le leggi di recepimento francesi[5] e britanniche[6] avevano replicato nei rispettivi ordinamenti il requisito dell'adeguatezza delle misure di sicurezza, la legge italiana[7] aveva ulteriormente precisato tale requisito, tipizzando[8] per legge specifiche misure tecniche minime di sicurezza[9].

Da tale diversità di regime nazionale[10] è conseguita ovviamente una diversità di giurisprudenza amministrativa sulla sicurezza del trattamento: mentre alcune decisioni rese dalle autorità francesi e britanniche sulla base del regime anteriore possono ancora essere utilmente analizzate per precisare il contenuto dei requisiti di sicurezza previsti dal GDPR, tanto non può dirsi delle decisioni rese dall'autorità italiana, in quanto fondate su criteri specifici e tipizzati non più previsti dal GDPR[11]. Pertanto, nel presente articolo, oltre alle decisioni rese in vigenza del GDPR, verranno analizzate anche alcune decisioni rese nella vigenza del regime precedente, ma solo nella misura in cui sono idonee a precisare il concetto di adeguatezza previsto dall'articolo 32 del GDPR.

Fatta questa breve premessa storica, per delineare invece il contesto attuale nel quale si colloca la questione dell'adeguatezza delle misure di sicurezza, è utile ricordare una serie di difficoltà, sia pratiche che di natura legale, proprie di questa particolare tematica.

Innanzitutto, dal punto di vista legale, sin dalla pubblicazione del GDPR[12], l'interpretazione dei requisiti di sicurezza è apparsa particolarmente difficoltosa in ragione delle variabili cui il criterio di adeguatezza è sottoposto, che qui brevemente si richiamano: (i) lo stato dell'arte; (ii) i costi di attuazione (delle misure di sicurezza); (iii) la natura, l'oggetto, il contesto e le finalità del trattamento e (iv) il rischio di varia probabilità e gravità di compressione o violazione dei diritti e delle libertà delle persone fisiche. Naturalmente, l'eccessiva apertura e indeterminatezza di detti criteri mal si concilia con la necessità di certezza e precisione di cui gli esperti di sicurezza hanno bisogno nella fase di *design*, d'implementazione e di *auditing* delle misure di sicurezza. Inoltre, non tutte le autorità di controllo europee hanno intrapreso iniziative finalizzate ad accompagnare pienamente gli operatori nei loro processi di *compliance*[13] come, ad esempio, la pubblicazione di linee guida a carattere tecnico. Né, sino ad oggi, i provvedimenti emessi dalle varie autorità europee sono stati particolarmente illuminanti, stante l'assenza di uniformità nelle modalità di redazione, di dettagli tecnici relativi alle vulnerabilità di volta in volta rilevate, di indicazioni uniformi sui criteri utilizzati per valutare la gravità delle infrazioni, e di dettagli circa le misure correttive imposte alle organizzazioni. Tali fattori, sommati alla scarsa reperibilità dei testi delle decisioni in inglese, rendono l'analisi complessiva del merito delle decisioni particolarmente difficoltosa, anche nella prospettiva di un'interpretazione e applicazione uniforme dei criteri di sicurezza del trattamento dei dati personali da parte delle stesse autorità di controllo europee.

Per quanto riguarda, invece, le difficoltà pratiche, è necessario ricordare il vastissimo ambito applicativo delle misure di sicurezza richieste dal GDPR, che coinvolgono l'ambito informatico, quello organizzativo e quello fisico. La presente analisi si concentra particolarmente sulle misure informatiche, ma è opportuno precisare che le autorità di controllo attribuiscono pari importanza alle misure organizzative[14] e fisiche[15]. Inoltre, è necessario tenere presente che nel campo della sicurezza informatica la componente umana è di importanza fondamentale: come noto, una larga parte[16] di violazioni informatiche ha origine dallo sfruttamento di una vulnerabilità umana[17]. Pertanto, l'efficacia delle misure informatiche dipende in buona parte anche dall'implementazione di solide misure organizzative[18].

Un ulteriore elemento potenzialmente foriero di problematiche è poi dato dal fatto che l'individuazione e l'implementazione di misure di sicurezza informatiche coinvolge necessariamente figure professionali con competenze e approcci diversi e sovente impreparate a comprendere il linguaggio, il metodo e le esigenze altrui, rendendo dunque non agevole la collaborazione e il lavoro di sintesi. Tale contesto è aggravato dalla grande diversità di misure di sicurezza informatiche astrattamente implementabili, come, ad esempio, le misure relative alla rete, le misure di protezione delle applicazioni e le misure relative alla protezione dei dati archiviati o in trasmissione.

Infine, vale la pena aggiungere che il concetto di "sicurezza assoluta" di un sistema informatico è quantomeno utopistico. Il continuo sviluppo delle tecnologie, l'aggiornamento dei software, e i test costanti cui sono sottoposte le misure di sicurezza comportano, inevitabilmente, la scoperta di vulnerabilità e, quindi, la violazione di sistemi ritenuti fino a quel

momento "sicuri". Da un punto di vista giuridico, tale problematica sembra richiamare l'utilità della distinzione fra obbligazioni di mezzo e obbligazioni di risultato ai fini dell'accertamento e dell'imputazione di responsabilità civili e amministrative connesse a violazioni di sicurezza, questione certamente importante in ragione del costante aumento di dati compromessi[19].

Nonostante queste difficoltà, è anche opportuno sottolineare che l'implementazione di misure di sicurezza appropriate non consente solamente il rispetto dei requisiti di sicurezza previsti dalla normativa in tema di dati personali, ma anche di proteggere dati aziendali non personali. Pertanto, i costi di implementazione dovrebbero essere considerati anche come un investimento a tutela del business dell'organizzazione, e non solo come un semplice costo di *compliance*.

Tanto premesso, a due anni dall'entrata in vigore del GDPR è finalmente possibile tracciare un primo quadro delle azioni poste in essere dalle autorità di controllo dei vari paesi europei riguardo le misure di sicurezza informatiche. Come messo in luce da una recente decisione emessa nei confronti di una primaria compagnia aerea dall'ICO[20], autorità di controllo britannica, il percorso verso una protezione informatica adeguata sembra essere ancora lungo: tale decisione, infatti, ha sanzionato una serie di vulnerabilità di sicurezza particolarmente gravi ed in ambiti molto diversi, come ad esempio il controllo degli accessi, la protezione della rete, la cifratura dei dati e l'obsolescenza dei software e delle applicazioni, tanto da rappresentare un caso paradigmatico di mancanza di *compliance* rispetto ai requisiti di sicurezza previsti dalla normativa in tema di protezione dei dati personali.

L'obiettivo del presente articolo è quindi di analizzare analiticamente ma senza pretesa di esaustività le più comuni tipologie di vulnerabilità riscontrate dalle autorità europee, raggruppandole in quattro macrocategorie ed evidenziandone la gravità.

2. *Accountability* e sicurezza informatica

Per quanto si possa ritenere che l'*accountability*, espressamente prevista dall'articolo 5(2) e dall'articolo 24 del GDPR, e principio cardine della normativa sulla protezione dei dati personali[21], non costituisca una misura di sicurezza in sé, essa costituisce nondimeno un principio base attorno al quale qualsiasi misura di sicurezza, sia essa di natura tecnica o organizzativa, dovrebbe essere implementata. In ragione della sua importanza, è dunque opportuno richiamarne le principali caratteristiche.

Come noto, l'*accountability* è composta da due distinti adempimenti cumulativi: il primo è costituito dal rispetto di una disposizione, il secondo dalla capacità del titolare del trattamento di dimostrarne il rispetto[22]. Pertanto, per conformarsi a questo principio, il titolare del trattamento è di regola chiamato a predisporre e conservare una grande quantità di documenti e, dunque, a tenere un comportamento attivo[23]. Estendendo l'*accountability* all'ambito della sicurezza informatica, il primo adempimento sarà costituito dalla predisposizione e dall'implementazione di misure di sicurezza "adeguate", ai sensi dell'articolo 32 GDPR, mentre il secondo riguarderà la capacità di dimostrare l'adeguatezza di tali misure.

Prima di analizzare dettagliatamente i due adempimenti, occorre premettere che, come rilevato dall'ICO, la predisposizione di misure di sicurezza richiede la conoscenza da parte del titolare dell'architettura informatica implementata e, in particolare, il luogo e il supporto su cui sono custoditi i dati personali, informazione senza la quale è probabile che le misure implementate risultino inadeguate[24]. Tale conoscenza, che può apparire ovvia, non è purtroppo scontata, in particolar modo in organizzazioni complesse, dove può accadere che dispositivi informatici accesi o servizi attivi vengano "dimenticati" per lunghi periodi di tempo.

Quindi, considerando il criterio dell'adeguatezza di ciascuna misura di sicurezza, un sistema informatico non è più forte del suo componente più vulnerabile come una catena non è più forte del suo anello più debole. Infatti, una singola vulnerabilità è sufficiente a causare una violazione di dati personali[25]. Pertanto, l'articolo 32(1)(d) del GDPR richiede al titolare del trattamento di mettere in atto «una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento». Tra le tante misure possibili, in ambito informatico le autorità di controllo richiedono in particolare l'implementazione di misure di *auditing*[26] o, più nel dettaglio, *vulnerability scan* e *penetration test*[27].

Invece, per quanto attiene al requisito della dimostrazione dell'adeguatezza delle misure, il vantaggio dei sistemi e dei programmi informatici è che, *by default*, producono (o possono produrre) una grande quantità di informazioni riguardo il loro funzionamento (detti *log*). Allora, il comportamento richiesto al titolare è quello di impostare e conservare correttamente i messaggi di *log*. Come si vedrà più nel dettaglio, è importante che ciascuna misura di sicurezza produca *log* e che, in presenza di una infrastruttura informatica di grandi dimensioni, il titolare si doti di aggregatori di messaggi di *log*[28] al fine di avere co-

stantemente una panoramica d'insieme sul corretto funzionamento dei propri sistemi e programmi.

a) La conduzione di *vulnerability scan*

La conduzione di *vulnerability scan* permette ad un'organizzazione di identificare vulnerabilità di dominio pubblico[29] presenti sui propri sistemi, e costituisce uno strumento di sicurezza imprescindibile per organizzazioni di grandi dimensioni o per quelle che hanno server accessibili da Internet e che, dunque, espongono dati al pubblico. Infatti, è stato espressamente statuito che la conduzione di *vulnerability assessments* contribuisce ad assicurare un livello costantemente adeguato di protezione dei dati personali[30], e che l'assenza o l'inadeguatezza degli *scan* comporti un aumento dei rischi legati alla sicurezza dei dati[31].

Secondo l'ICO e il Garante italiano, i *vulnerability scan* dovrebbero essere effettuati regolarmente, ed, in ogni caso, a seguito di cambiamenti importanti[32]. Ovviamente, l'ICO ha giudicato non sufficiente un lasso di tempo di tre anni fra due test perché «in considerazione della quantità e della natura dei dati personali conservati da Cathay Pacific, e della velocità con la quale le minacce di cybersecurity si evolvono e diventano più sofisticate, questo è un periodo ingiustificatamente lungo senza un penetration test»[33].

b) La gestione dei messaggi di *log*

La conservazione e l'analisi dei messaggi di *log* costituisce una misura di sicurezza essenziale in quanto non solo permette al titolare di essere sempre a conoscenza degli eventi che si verificano nei propri sistemi (ad esempio, accessi o operazioni compiute dagli utenti)[34], ma soprattutto di essere sempre in grado di dimostrare l'adeguatezza delle misure di sicurezza implementate. Conseguentemente, la registrazione e la conservazione dei *log* è espressamente richiesta in diversi provvedimenti settoriali emanati dalle autorità di controllo[35]. In assenza di *log* non è possibile individuare vulnerabilità, né per quanto riguarda il titolare, né per quanto riguarda le autorità di controllo[36]. Inoltre, in assenza di *log*, non è possibile analizzare ex post le modalità di un attacco[37] e, soprattutto, le conseguenze con riguardo ai dati personali conservati. Pertanto, l'incertezza causata dall'assenza di *log* crea un rischio di sicurezza[38] come stabilito dal Garante, secondo il quale «il mancato completo tracciamento degli accessi al database [...] configura la violazione [...] dell'obbligo di assicurare più adeguate garanzie di riservatezza agli iscritti alla piattaforma medesima»[39].

Perciò, come ogni dato, e soprattutto nella misura in cui contengano dati personali, anche i *log* devono essere adeguatamente conservati e protetti. Ad esempio, secondo il Garante, l'inclusione nei *log* di informazioni non indispensabili per finalità di controllo e sicurezza può determinare una duplicazione di dati e quindi l'incremento del rischio di trattamento illecito[40].

3. Gestione degli accessi

Una seconda violazione delle misure di sicurezza frequentemente riscontrata dalle autorità di controllo riguarda la gestione degli accessi (c.d. *access control*). È opportuno notare che tale misura non è di natura esclusivamente informatica, ma, in primo luogo, di tipo organizzativo. Una corretta gestione degli accessi permette di limitare l'accesso a determinati dati (tra cui ovviamente anche dati personali) unicamente agli utenti che ne hanno bisogno per il compimento delle proprie funzioni o necessità. Inoltre, è opportuno notare che la gestione degli accessi non compie distinzioni tra categorie di persone che accedono ad un dato, e si applica tanto ad utenti interni ad un'organizzazione (come, ad esempio, dipendenti e consulenti) quanto ad utenti esterni (fornitori, clienti o semplici visitatori).

a) L'autenticazione degli utenti

In caso di controlli di accesso interni, l'autenticazione presuppone, di regola, che ciascun utente di un sistema sia dotato di un proprio account individuale, specialmente quando tale utente abbia responsabilità aziendali particolari. Tramite l'autenticazione è infatti possibile ricondurre con certezza le azioni compiute dall'account all'utente, facilitando il rispetto del principio di *accountability*. La connessione fra autenticazione e *accountability* è stata sottolineata dal Garante italiano, per il quale «la condivisione delle credenziali impedisce di attribuire le azioni compiute in un sistema informatico a un determinato incaricato, con pregiudizio anche per il titolare, privato della possibilità di controllare l'operato di figure tecniche così rilevanti»[41]. In conseguenza, «l'avvenuta condivisione delle credenziali di autenticazione tra più soggetti legittimati alla gestione della piattaforma rappresent[a] una violazione dell'obbligo di predisposizione, da parte del responsabile del trattamento, di misure tecniche e organizzative adeguate»[42]. Tale adempimento è, d'altra parte, incluso negli standard di sicurezza pubblicati dalle organizzazioni internazionali più prestigiose[43], e non richiede alcun costo aggiuntivo, poiché la maggior parte dei sistemi e applicativi informatici prevedono la possibilità di creare e gestire facilmente i profili di autenticazione degli utenti.

In caso di accesso esterno, occorre che l'utente sia autenticato in modo corretto. Può accadere che un'errata o mancata configurazione di un'applicazio-

ne permetta la messa a disposizione di dati riservati a terzi non autorizzati (o, peggio ancora, al pubblico). La Commission Nationale Informatique & Libertés (CNIL), autorità di controllo francese, ha avuto modo di affrontare due casi di configurazione errata di un'applicazione web (di una società assicurativa in un caso, e di gestione immobiliare nell'altro) che consentiva l'accesso a dati personali contenuti in aree clienti riservate a terzi non autorizzati. Dopo aver ricordato che «quando una richiesta di accesso a una risorsa è indirizzata ad un server, quest'ultimo deve verificare che il richiedente sia autorizzato ad accedere alle risorse richieste»[44], la CNIL ha qualificato tali accessi non autorizzati come violazione grave delle norme di sicurezza in quanto astrattamente sfruttabile da qualunque persona, anche non esperta in informatica.

È quindi nell'ambito delle modalità di autenticazione che sembra possibile rilevare un primo disallineamento fra i requisiti di sicurezza ritenuti adeguati dalle diverse autorità di controllo europee. Premesso che ai fini di un'autenticazione sicura può essere opportuno prevedere più di un fattore di autenticazione[45], come d'altronde già previsto da alcune normative settoriali[46], i requisiti di robustezza delle password individuati dalle diverse autorità non sembrano pienamente corrispondere. Infatti, se l'autorità italiana stabilisce che la lunghezza minima di una password debba essere di 8 caratteri, con un controllo automatico di qualità che impedisca l'uso di password costituite da parole reperibili in dizionari[47], l'autorità francese, in assenza di un sistema di autenticazione in grado di prevenire attacchi *brute-force*, richiede una lunghezza minima di 12 caratteri alfanumerici, con carattere maiuscolo, minuscolo e un carattere speciale[48]. Ancor diversamente, secondo le linee guida dell'autorità britannica, la lunghezza minima della password dovrebbe essere di 10 caratteri, senza necessariamente richiedere un carattere speciale. Tale difformità applicativa, seppur minima e priva di conseguenze particolari, dimostra nondimeno la possibilità astratta che possano in futuro verificarsi nuovamente divergenze su requisiti tecnici specifici. Al fine di assicurare uniformità di applicazione, il buon funzionamento del meccanismo di cooperazione e coerenza previsto dal GDPR[49] sarà di fondamentale importanza al fine di evitare tali asimmetrie applicative[50].

In ogni caso, l'assegnazione di account individuali o l'autenticazione di un utente costituisce solo una prima misura di sicurezza, che deve essere naturalmente seguita dall'individuazione delle categorie di dati accessibili dagli account rilevanti, e, dunque, dalle autorizzazioni assegnate.

b) L'autorizzazione degli utenti

La necessità di prevedere autorizzazioni specifiche (quantomeno interne ad un'organizzazione) emerge implicitamente[51] dall'articolo 29 GDPR, ai sensi del quale chi agisce sotto l'autorità del titolare o del responsabile non può trattare dati personali se non è istruito in tal senso.

Tale misura di sicurezza consente di restringere l'accesso ai soli dati essenziali per i quali viene effettuato l'accesso, ed è importante quanto l'autenticazione, in quanto quest'ultima sarebbe inutile se tutti gli utenti fossero autorizzati ad accedere a tutti i dati, circostanza che, secondo la CNIL, costituisce una violazione dell'art. 32 del GDPR[52]. In maniera similare, secondo il Garante italiano, la mancata implementazione di sistemi di autorizzazione integra la violazione dell'articolo 5(1)(f) del GDPR[53].

A livello informatico, l'autorizzazione all'accesso a dati viene di regola impostata sulla base dell'appartenenza di un utente ad un determinato gruppo[54], ma altre tecniche possono essere implementate, come ad esempio la restrizione di accesso al di fuori di determinati orari[55]. Secondo il Garante italiano, «la mancata definizione e configurazione dei differenti profili di autorizzazione in modo da limitare l'accesso ai soli dati necessari nei diversi ambiti di operatività»[56] configura una violazione dell'obbligo di predisposizione di misure tecniche adeguate.

Ovviamente, lo scopo dell'autorizzazione può essere vanificato ove troppi utenti vengano autorizzati ad accedere a documenti sensibili o quando utenti siano dotati di autorizzazioni particolarmente ampie, fenomeno che tende a verificarsi frequentemente in particolar modo con riguardo a profili di amministratori di sistema[57] (spesso per comodità e rapidità di assistenza ed intervento a distanza). Secondo l'ICO, pertanto, occorre valutare il rischio di aggiungere utenti al gruppo di amministratori di dominio e mantenere un numero limitato di autorizzazioni.

4. Utilizzo di applicazioni obsolete o non aggiornate

Una terza categoria di vulnerabilità affrontata dalle autorità di controllo riguarda l'utilizzo di applicazioni non aggiornate o obsolete. Può accadere che successivamente al rilascio di un'applicazione vengano scoperte vulnerabilità[58] che rendono le applicazioni non sicure. In tali casi, solitamente gli sviluppatori rilasciano un aggiornamento che, una volta installato, corregge la vulnerabilità identificata. Se l'aggiornamento non viene effettuato, il sistema rimane estremamente vulnerabile, non solo perché presenta una vulnerabilità, ma soprattutto

perché quest'ultima diventa di dominio pubblico e, dunque, facilmente sfruttabile da un grande numero di malintenzionati.

Al termine del ciclo vita di un'applicazione, gli aggiornamenti di sicurezza vengono sospesi dallo sviluppatore ed in conseguenza qualsiasi vulnerabilità successivamente individuata non viene di regola più corretta. Pertanto, l'applicazione, benché ancora utilizzabile rimane vulnerabile, a meno che sviluppatori interni procedano autonomamente alla sua manutenzione, cosa di regola dispendiosa e riservata a personale esperto.

a) Utilizzo di applicazioni non aggiornate

Il continuo aggiornamento delle applicazioni costituisce una misura di sicurezza idonea a correggere vulnerabilità di volta in volta rese note al pubblico e corrette dagli sviluppatori. Per dare un'idea della frequenza con cui dovrebbero essere aggiornati i sistemi, l'ICO ha rilevato in un procedimento sanzionatorio che in un periodo di 8 mesi sono stati rilasciati 17 aggiornamenti che risolvevano vulnerabilità note per un server, e che se il titolare avesse implementato una gestione delle *patch* più efficace, gli hacker avrebbero avuto meno opportunità di sfruttare tali vulnerabilità[59]. A dire il vero, emerge dai provvedimenti analizzati una grave negligenza da parte dei titolari che risulta a volte da vulnerabilità presenti nei sistemi IT addirittura per più di 4 anni[60]. Pertanto, se necessario, in aggiunta alla regolare installazione di *patch* e aggiornamenti, può essere opportuno implementare una procedura di tipo organizzativo che permetta di verificare il regolare e corretto svolgimento di tali operazioni[61].

b) Utilizzo di applicazioni obsolete

L'assenza di aggiornamenti di sicurezza per applicazioni o sistemi obsoleti crea un rischio aggiuntivo di sicurezza che rende tali sistemi un obbiettivo ovvio per degli *hacker*[62].

Ove venissero usate applicazioni obsolete, pertanto, il rischio di compromissione di un sistema IT[63] sarebbe incrementato, perché, in assenza di supporto da parte degli sviluppatori ufficiali, sarebbe necessario l'intervento ad hoc degli sviluppatori del titolare del trattamento per correggere le vulnerabilità eventualmente individuate, che, però, potrebbe non essere tempestivo[64]. Perciò, anche l'utilizzo di applicazioni obsolete è idoneo a configurare una violazione dei criteri di sicurezza del trattamento dei dati personali.

5. La sicurezza dei dati

L'ultima categoria di vulnerabilità frequentemente identificata dalle autorità di controllo è quella relativa alla sicurezza dei dati, in particolare per quanto riguarda le modalità della loro conservazione e condivisione. Nonostante esista una grandissima varietà di misure di sicurezza implementabili per proteggere i dati, come ad esempio la pseudonimizzazione o la cifratura, che sono espressamente previste dall'articolo 32(1)(a) del GDPR, per motivi pratici o tecnici non sempre è possibile implementarle o garantire il massimo livello di sicurezza possibile. Ad esempio, benché la cifratura asimmetrica sia ritenuta più sicura della crittografia simmetrica, essa richiede una potenza di calcolo per cifrare e decifrare un dato molto superiore rispetto alla seconda, rendendola inadeguata alla cifratura di grandi quantità di dati in trasmissione[65]. Sicché, la tecnica di protezione dei dati dovrebbe essere adeguata al trattamento dei dati che viene effettuato.

Occorre premettere che nell'ambito della sicurezza informatica si suole catalogare i dati a seconda che siano correntemente usati nelle operazioni quotidiane, che siano in trasmissione a terzi, o che siano invece archiviati[66]. Tale distinzione, che è stata riconosciuta a livello normativo dall'EBA nelle linee guida sul *risk management* in ambito bancario[67], non sembra esser stata ad oggi condivisa da nessuna autorità di controllo[68], ma è importante perché i sistemi di protezione dei dati presentano ciascuno specifici vantaggi ed inconvenienti in funzione dello stato in cui si trova il dato da proteggere, e non possono essere applicati universalmente.

Poiché è evidente che i dati trattati attivamente da un'azienda non possano essere né pseudonimizzati né cifrati (essendo necessario utilizzare i dati, essi devono spesso essere disponibili "in chiaro", preferendosi in tali casi misure di sicurezza relative all'accesso ai dati), la maggior parte delle decisioni delle autorità si sono focalizzate sulla sicurezza della trasmissione dei dati e sulla loro archiviazione.

a) La protezione dei dati trasmessi a terzi

Quando un dato viene condiviso con terzi, vi è il rischio di una violazione di confidenzialità. Ove il dato venga trasmesso su Internet, chiunque sia in grado di intercettare la comunicazione elettronica può, in assenza di misure di cifratura, accedere al dato in chiaro. Benché la maggior parte delle comunicazioni via Internet avvenga ormai tramite modalità criptate, esistono ancora servizi che non prevedono la cifratura dei dati, come ad esempio il protocollo *http*, il quale ovviamente «non garantisce una comunicazione sicura sia in termini di riservatezza e integrità dei dati scambiati che di autenticità del sito web visualizzato»[69]. Pertanto, in generale, il Garante stabilisce che «il mancato utilizzo di strumenti di crittografia per il trasporto dei dati si pone in contrasto con l'ar-

ticolo 32 del Regolamento». Tale argomento si applica, ovviamente, anche alle e-mail. Secondo l'autorità danese, l'utilizzo di protocolli di cifratura, come il protocollo TLS e la cifratura end-to-end delle e-mail in trasmissione costituisce una misura di sicurezza adeguata ai sensi dell'articolo 32 del GDPR[70].

b) La protezione dei dati archiviati

Quando un dato, a seguito del trattamento attivo, deve essere conservato, deve essere adeguatamente protetto.

Sul punto è opportuno menzionare che la prima misura di sicurezza implementabile può essere certamente costituita dall'implementazione e dal rispetto di una *data retention policy* perché eliminando dati non più necessari da un sistema è possibile eliminare il corrispondente di rischio di violazione o, quantomeno, è possibile ridurre la quantità di dati esposti alla violazione[71].

In secondo luogo, anche i dati personali archiviati e non attivamente utilizzati dovrebbero essere criptati. Ad esempio, secondo l'autorità danese, l'assenza di cifratura di un hard disk di un computer portatile che contiene dati personali costituisce una vulnerabilità che permette una facile violazione di dati[72]. Tale misura è sempre prescritta (e la sua assenza sanzionata) dalle autorità di controllo per quanto riguarda credenziali[73] e password[74] o dati identificativi[75].

Infine, la protezione dei dati con sistemi di cifratura è richiesta laddove il dato personale, per sua natura, sia particolarmente sensibile. Nel contesto della sicurezza informatica, però, il criterio di sensibilità del dato non segue necessariamente la distinzione operata dal GDPR fra categorie particolari di dati personali, dati relativi a condanne penali e altri dati. Mentre il Garante ad esempio ha emesso un provvedimento correttivo nel quale ha stabilito che la mancata protezione di dati relativi alla salute con una password costituisca una violazione dell'articolo 32 del GDPR[76], la CNIL ha recentemente esteso tale requisito anche ai dati bancari, che invece non rientrano in categorie particolari di dati[77].

6. Conclusioni

Analizzando le decisioni emesse dalle autorità europee da un punto di vista tecnico, emerge in modo chiaro che i provvedimenti hanno riguardato falle di sicurezza particolarmente gravi, benché di facile identificazione e gestione. Particolarmente significativa è l'affermazione fatta in questo senso dall'ICO che, nell'ambito di un provvedimento sanzionatorio, ha statuito che «è particolarmente preoccupante che una serie di inadeguatezze fossero relative a misure basiche e banali per tali sistemi [informatici]»[78] identificando tali misure in segregazione di rete, *patching*, testing delle vulnerabilità, attività di *logging*, gestione degli account[79], software obsoleti e assenza di antivirus[80]. Nessun provvedimento ha sanzionato una vulnerabilità non di dominio pubblico alla data della violazione[81]. Inoltre, la predisposizione di misure di sicurezza adeguate e la reazione immediata da parte del titolare del trattamento ha spesso costituito un'argomentazione valida per evitare un provvedimento correttivo o sanzionatorio[82].

Da un punto di vista più giuridico, invece, diverse considerazioni possono essere fatte. In primo luogo, occorre interrogarsi sul grado di certezza (e uniformità) del diritto offerto dall'impianto normativo dell'articolo 32 che, come detto, àncora l'adeguatezza delle misure di sicurezza a sei parametri diversi, di cui solamente uno di natura parzialmente oggettiva (lo stato dell'arte). In tale contesto, le autorità di controllo europee assumono una grande responsabilità, godendo di una discrezionalità estremamente ampia nell'interpretazione e nell'applicazione della norma. Delegare interamente alle autorità di controllo l'individuazione delle specifiche misure di sicurezza appropriate permette senz'altro di garantire una disciplina giuridica al passo con la costante evoluzione tecnologica sia dei rischi che delle corrispondenti misure di protezione, oltre a garantire un buon grado di flessibilità nell'applicazione della norma. Tuttavia, tale scelta presenta l'inconveniente di precludere un'informazione per le imprese facilmente accessibile sui requisiti di sicurezza applicabili, in particolare per quelle che, pur non essendo dotate di personale particolarmente qualificato, offrono servizi su canali telematici e vorrebbero conformarsi a dei requisiti giuridici chiari e precisi, senza dover incorrere in costi aggiuntivi. Inoltre, è teoricamente possibile che il giudizio di inadeguatezza di una misura di sicurezza espresso da un'autorità di controllo possa confliggere con quello di un'altra autorità, o essere (eventualmente a ragione) contestato da un punto di vista strettamente tecnico in sede di ricorso. Ad oggi, tale scenario non sembra ancora essersi presentato, ma la giurisprudenza relativa all'adeguatezza delle misure di sicurezza informatica sembra certamente destinata a mantenere un'importanza primaria nella precisazione del contenuto della norma e, probabilmente, anche ad assumere il ruolo di guida per le future politiche legislative relative alla sicurezza informatica.

Sempre in ottica futura, non può non rilevarsi una profonda distinzione nella tecnica normativa usata per quanto riguarda la sicurezza informatica fra il regime previsto dal GDPR e quello della direttiva PSD2 sui servizi di pagamento, fondato invece su linee guida emanate dall'Autorità bancaria europea

(EBA) che includono requisiti di sicurezza specifici, seppur *high level*. Tale soluzione, che lascia agli operatori un margine discrezionale sulle modalità concrete dell'implementazione delle misure, fornisce allo stesso tempo indicazioni tecniche chiare cui attenersi, facilitando i processi di *compliance* delle organizzazioni. Su questo punto è doveroso rilevare che tutti i principi espressi dalle autorità di controllo nelle decisioni analizzate trovano preciso riscontro normativo nelle linee guida dell'EBA[83]. Benché l'ambito di applicazione particolarmente ampio del GDPR[84] rappresenti certamente un inconveniente significativo all'adozione di tale sistema, in quanto non si può pretendere un livello di sicurezza omogeneo fra organizzazioni radicalmente diverse, come multinazionali e piccole e medie imprese, una riflessione sulla migliore soluzione per implementare un impianto normativo relativo alla sicurezza informatica potrebbe essere utile, soprattutto in considerazione della sicura centralità ed importanza della sicurezza informatica nei prossimi anni.

In conclusione, è possibile rilevare una politica fino ad oggi complessivamente tollerante da parte delle autorità di controllo europee, soprattutto dal punto di vista sanzionatorio, rispetto a violazioni riscontrate particolarmente gravi. A fronte di servizi forniti ormai quasi esclusivamente via Internet, la sicurezza informatica sta rapidamente diventando un requisito legale di primaria importanza non solo nel contesto della normativa a protezione dei dati personali, ma trasversalmente in tutti i settori economici[85] e sociali[86], come testimoniato dalla pubblicazione del *Cybersecurity Act* europeo[87], che ha (re)istituito l'Agenzia dell'Unione europea per la cibersicurezza (ENISA), rafforzandone notevolmente poteri e competenze. Dunque, diventa di fondamentale importanza per le organizzazioni approcciare la questione della sicurezza dei dati con la dovuta attenzione e con la massima responsabilità, sia in ottica di protezione dei propri beni aziendali che, soprattutto, dei dati personali dei propri dipendenti, collaboratori e clienti che con fiducia glieli affidano.

Note

[1]CISCO, *Data Privacy Benchmark Study 2019*, p. 5.

[2]La formulazione esatta dell'articolo 32 del Regolamento (UE) 2016/679 è: «1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. 2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. 3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri».

[3]La formulazione esatta dell'articolo 17 della direttiva 95/46/CE era: «1. Gli Stati membri dispongono che il responsabile del trattamento deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali. Tali misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere. 2. Gli Stati membri dispongono che il responsabile del trattamento, quando quest'ultimo sia eseguito per suo conto, deve scegliere un incaricato del trattamento che presenti garanzie sufficienti in merito alle misure di sicurezza tecnica e di organizzazione dei trattamenti da effettuare e deve assicurarsi del rispetto di tali misure. 3. L'esecuzione dei trattamenti su commissione deve essere disciplinata da un contratto o da un atto giuridico che vincoli l'incaricato del trattamento al responsabile del trattamento e che preveda segnatamente: - che l'incaricato del trattamento operi soltanto su istruzioni del responsabile del trattamento; - che gli obblighi di cui al paragrafo 1, quali sono definiti dalla legislazione dello Stato membro nel quale è stabilito l'incaricato del trattamento, vincolino anche quest'ultimo. 4. A fini di conservazione delle prove, gli elementi del contratto o dell'atto giuridico relativi alla protezione dei dati e i requisiti concernenti le misure di cui al paragrafo 1 sono stipulati per iscritto o in altra forma equivalente».

[4]Commissione Europea, *Proposta di Regolamento del Parlamento europeo e del Consiglio* concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati) COM(2012) 11 final, par. 3.4.4.2.: «L'articolo 30 impone al responsabile del trattamento e all'incaricato del trattamento di mettere in atto misure adeguate per la sicurezza dei trattamenti, ai sensi dell'articolo 17, paragrafo 1, della direttiva 95/46/CE, estendendo l'obbligo agli incaricati del trattamento, indipendentemente dal contratto che hanno sottoscritto con il responsabile del trattamento».

[5]Legge no 78-17 del 6 gennaio 1978 e successive modifiche.

[6]Data Protection Act 1998.

[7]Decreto legislativo n. 196/2003.

[8]L. Bolognini, E. Pelino, C. Bistolfi, *Il Regolamento Privacy Europeo*, Giuffrè, 2016, p. 409.

[9]Artt. 33, 34 e 35 del d.lgs. n. 196/2003 e Disciplinare Tecnico contenuto nell'Allegato B del Decreto.

[10]Sulle divergenze di implementazione tra Stati membri, si veda Parlamento europeo, *Prima relazione sull'applicazione della direttiva sulla tutela dei dati (95/46/CE)*, COM(2003) 265 final, 2004; sulla diversità tra il regime della direttiva trasposta in Italia e il GDPR nell'ambito della sicurezza del trattamento si veda G.M. Riccio, G. Scorza, E. Belisario, *GDPR e Normativa Privacy, Commentario*, Wolters Kluwer, 2018, I ed., pp. 300-301.

[11]*Ex multis*, Garante per la Protezione dei Dati Personali, *provv. n. 99, docweb n. 9429195*, 10 giugno 2020.

[12]Prima di esso, del regime previsto dalla *Direttiva 96/45/CE*.

[13]Tra le autorità che hanno intrapreso iniziative, si segnala l'Autorità di controllo francese: CNIL, *Security of personal data*, 2018.

[14]Ad esempio, si pensi ai rapporti con i responsabili del trattamento e relativa *third-party compliance*, già analizzati dalla CNIL, *Décision n° MED 2019-025*, 5 novembre 2019 e dal Garante per la Protezione dei Dati Personali, *provv. n. 87, docweb n. 9104006*, 28 marzo 2019.

[15]Information Commissioner Office (ICO), *Penalty Notice to Doorstep Dispensaree Ltd*, 17 dicembre 2019, relativa ad un titolare sanzionato per conservazione di documenti sanitari in un cortile accessibile al pubblico.

[16]IBM Managed Security Services, *IBM Security Services 2014 - Cyber Security Intelligence Index*, p. 4.

[17]Tramite azioni di *social engineering*.

[18]L'interconnessione tra sicurezza informatica e misure organizzative è d'altronde evidenziata dalla previsione di specifici requisiti organizzativi in capo alle istituzioni finanziarie nel contesto della loro sicurezza ICT, previsti dalla European Banking Authority, *Guidelines on ICT and security risk management*, sez. 3.2 *Governance and Strategy*, 2019.

[19]Giunti, nel 2019, a 8.5 miliardi, in aumento del 200% rispetto al 2018, *IBM X-Force Incident Response and Intelligence Services, X-Force Threat Intelligence Index 2020*, 2020.

[20]ICO, *Monetary Penalty Notice to Cathay Pacific Airways Limited*, 10 febbraio 2020, p. 14

[21]Garante per la Protezione dei Dati Personali, *provv. n. 143, docweb n. 9435753*, 9 luglio 2020.

[22]Gruppo di lavoro Articolo 29 per la protezione dei dati, *Parere 3/2010 sul principio di responsabilità*, 13 luglio 2010.

[23]G.M. Riccio, G. Scorza, E. Belisario, *op. cit.*, p. 237. Sulla necessità di dimostrare il rispetto delle disposizioni applicabili, si veda anche Garante per la Protezione dei Dati Personali, *provv. n. 143/2020*, cit.

[24]ICO, *Monetary Penalty Notice to the Carphone Warehouse Limited*, 8 gennaio 2018, p. 12; Id., *Monetary Penalty Notice to DSG Retail Limited*, 7 gennaio 2020, p. 21.

[25]Principio del *single point of failure*.

[26]Garante per la Protezione dei Dati Personali, *provv. n. 87/2019*, cit.

[27]Mentre un *vulnerability scan* ha l'obiettivo di testare l'efficacia di ciascuna misura di sicurezza, i *penetration test* hanno l'obiettivo di simulare un vero e proprio attacco, sfruttando qualsiasi vulnerabilità identificata per creare il maggior danno possibile all'organizzazione, e così individuare precisamente il danno potenziale che potrebbe essere causato dallo sfruttamento di una vulnerabilità.

[28]Garante per la Protezione dei Dati Personali, *provv. n. 83, docweb n. 9101974*, 4 aprile 2019.

[29]ICO, *Monetary Penalty Notice to DSG Retail Limited*, cit., p. 11.

[30]Garante per la Protezione dei Dati Personali, *provv. n. 83/2019*, cit.

[31]ICO, *Monetary Penalty Notice to DSG Retail Limited*, cit., p. 11.

[32]Id., *Monetary Penalty Notice to Cathay Pacific Airways Limited*, cit., p. 14.

[33]*Ibidem*.

[34]Garante per la Protezione dei Dati Personali, *provv. n. 83/2019*, cit.

[35]Tra gli altri, Id., *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema, docweb n. 1577499*, 27 novembre 2008; Id., *Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie, docweb n. 1813953*, 12 maggio 2011.

[36]L'ICO è stata impossibilitata a verificare il corretto *patching* di un server a causa dell'assenza di *log* in ICO, *Monetary Penalty Notice to Cathay Pacific Airways Limited*, cit., p. 8.

[37]Garante per la Protezione dei Dati Personali, *provv. n. 83/2019*, cit.

[38]ICO, *Monetary Penalty Notice to DSG Retail Limited*, cit., p. 12.

[39]Garante per la Protezione dei Dati Personali, *provv. n. 83/2019*, cit.

[40]Id., *provv. n. 228, docweb n. 9283040*, 18 dicembre 2019.

[41]Id., *provv. n. 83/2019*, cit.

[42]*Ibidem*. Anche secondo l'ICO l'utilizzo del medesimo account e password da più membri dello staff costituisce una violazione delle misure di sicurezza adeguate, ICO, *Monetary Penalty Notice to the Carphone Warehouse Limited*, cit.

[43]ISO 27001:2013 A. 9.

[44]CNIL, *Délibération n° SAN-2019-007*, 18 luglio 2019; Id., *Délibération n° SAN-2019-005*, 28 maggio 2019.

[45]C.d. *multifactor authentication*.

[46]Ad esempio, un'autenticazione a due fattori è richiesta per l'autenticazione degli incaricati che trattano dati di traffico dei fornitori di servizi di comunicazione elettronica, Garante per la Protezione dei Dati Personali, *Allegato A, docweb n. 1538237*, 17 gennaio 2008. Nel contesto della direttiva PSD2, gli utenti dei servizi bancari devono essere autenticati con un'autenticazione a due fattori: European Banking Authority, *Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under article 98 of Directive 2015/2366 (PSD2)*.

[47]Garante per la Protezione dei Dati Personali, *provv. n. 548, docweb n. 7400401*, 21 dicembre 2017.

[48]CNIL, *Délibération n° SAN-2020-003*, 28 luglio 2020.

[49]Regolamento (UE) 2016/679, Capo VII.

[50]Il meccanismo di cooperazione sembra esser stato efficacemente usato nella decisione CNIL n. SAN-2020-003, nell'ambito del cui procedimento ha raccolto e incluso nel provvedimento finale le osservazioni delle autorità italiana, portoghese e della Bassa Sassonia.

[51]G.M. Riccio, G. Scorza, E. Belisario, op. cit., p. 276.

[52]CNIL, *Décision n° MED 2019-025*, 5 novembre 2019.

[53]Garante per la Protezione dei Dati Personali, *provv. n. 18, doc. web n. 9269629*, 23 febbraio 2020.

[54]Si pensi ad esempio ad uno scenario in cui il personale del dipartimento *marketing* non possa accedere ai dati di fatturazione cliente trattati dal dipartimento *finance*.

[55]Come suggerito dal Garante per la Protezione dei Dati Personali, *provv. n. 18/2020*, cit.

[56]Id., *provv. n. 83/2019*, cit.

[57]Ad esempio, in ICO, *Monetary Penalty Notice to Cathay Pacific Airways Limited*, cit., p. 13.
[58]Garante per la Protezione dei Dati Personali, *provv. n. 548/2017*, cit., secondo cui le vulnerabilità possono essere causate, ad esempio, da un'insufficiente metodologia di sviluppo software.
[59]ICO, *Monetary Penalty Notice to Cathay Pacific Airways Limited*, cit., p. 8.
[60]Si veda, ad esempio, Id., *Monetary Penalty Notice to DSG Retail Limited*, cit., p. 10.
[61]Id., *Monetary Penalty Notice to the Carphone Warehouse Limited*, cit., pp. 8-9.
[62]Id., *Monetary Penalty Notice to Cathay Pacific Airways Limited*, cit., p. 10.
[63]Id., *Monetary Penalty Notice on DSG Retail Limited*, cit., p. 12.
[64]Garante per la Protezione dei Dati Personali, *provv. n. 83/2019*, cit.
[65]Sulla distinzione fra crittografia simmetrica e asimmetrica si veda, ad esempio, CNIL, *Comprendre les grands principes du chiffrement*, 2016.
[66]Rispettivamente tecnicamente definiti *active data*, *data in trasmission* e *data at rest*.
[67]European Banking Authority, *Guidelines on ICT and security risk management*, cit., sez. 3.4 *Information security*, p. 18.
[68]Seppure la CNIL impieghi una struttura tripartita di archiviazione di dati, distinguendo fra archiviazione di dati attivi, archiviazione intermedia e archiviazione definitiva, si veda CNIL, *Les durées de conservation des données*, 2020.
[69]Garante per la Protezione dei Dati Personali, *provv. n. 17, docweb n. 9269618*, 23 gennaio 2020; CNIL, *Décision n° MED 2019-025*, 5 novembre 2019.
[70]Datatilsynet, *Tilsyn med behandlingssikkerhed hos advokatfirma*, journalnummer 2019-41-0026; Id., *Tilsyn med behandlingssikkerhed hos revisionsfirma*, journalnummer 2019-41-0027.
[71]ICO, *Monetary Penalty Notice to Cathay Pacific Airways Limited*, cit., p. 14.
[72]Datatilsynet, *Gladsaxe og Horsholm Kommune*, 10 marzo 2020.
[73]Garante per la Protezione dei Dati Personali, *provv. n. 2282019*, cit.
[74]CNIL, *Délibération n° SAN-2018-011*, 19 dicembre 2018.
[75]Garante per la Protezione dei Dati Personali, *provv. n. 17/2020*, cit.
[76]Id., *provv. n. 142, docweb n. 9446166*, 9 luglio 2020.
[77]CNIL, *Délibération n° SAN-2020-003*, cit.
[78]ICO, *Monetary Penalty Notice to DSG Retail Limited*, cit.
[79]*Ibidem*.
[80]ICO, *Monetary Penalty Notice to the Carphone Warehouse Limited*, cit.
[81]*0 day vulnerability* in linguaggio tecnico.
[82]Agencia Espanola de Proteccion de Datos, *Procedimiento n. PS/00431/2018*, p. 3.
[83]In ordine di discussione, con corrispondente paragrafo del documento European Banking Authority, *Guidelines on ICT and security risk management*, cit., *vulnerability testing* alla sez. 3.4.6., *logging* alla sez. 3.4.2 (d), *autenticazione* alla sez. 3.4.2 (g), *autorizzazione* alla sez. 3.4.2 (a), *utilizzo di applicazioni obsolete* alla sez. 3.4.5.
[84] Che si applica indifferentemente ad organizzazioni di dimensioni e con interessi non comparabili.
[85]Ad esempio il settore bancario, già discusso; in ambito reti e sistemi informativi si pensi alla direttiva (UE) 2016/1148 "NIS".
[86]In tema di sicurezza nazionale si veda la direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.
[87]Regolamento (UE) 2019/881.

* * *

Breach of security requirements under Article 32 of GDPR

Abstract: According to a recent survey, organizations revealed that the biggest challenge they face related to compliance with GDPR provisions is to align their security measures to the requirements established by Article 32 of the GDPR. This difficulty may derive from some particular aspects of security measures, such as their very broad implementation scope, the great diversity of existing measures to be implemented, and the need to engage several professionals with different backgrounds for their implementation. Among legal difficulties, it is argued that Article 32 of the GDPR does not identify specific measures to be implemented, or those which could be deemed appropriate, but only provides a list of recommended measures. In addition, the requirement of appropriateness of the security measures depends on a number of subjective factors, which therefore leaves broad discretion to European supervisory authorities to rule on which measures may be deemed appropriate and which may not. In order to provide precise guidance to organizations, the article conducts an analysis of the decisions of selected European supervisory authorities related to IT security to identify which measures were deemed appropriate and which inappropriate. The decisions were grouped based on the types of security measures analyzed by the authorities: accountability, access management, use of obsolete applications and protection of data. The analysis shows that European supervisory authorities adopt a uniform approach towards the definition of appropriateness of security measures. However, given the importance of cybersecurity in the near future and the importance of protection of personal data, such uniformity shall be preserved to ensure legal certainty and a uniform application of GDPR security requirements across Europe.

Keywords: GDPR – Security measures – Article 32 – Cybersecurity Compliance – Europe