Modelli organizzativi per la gestione dei rischi informatici. Il caso Rousseau

La conformità del trattamento dei dati personali alla disciplina del regolamento 2016/679 (e ad altre disposizioni del diritto europeo o nazionale) riposa sull'adozione di un modello organizzativo in cui, seguendo il noto princìpio della divisione del lavoro di **Adam Smith**, il titolare e il responsabile del trattamento definiscono compiti e funzioni connessi al trattamento per il cui svolgimento vengono opportunamente designate figure interne ed esterne all'organizzazione (responsabili del trattamento, amministratori di sistema, persone autorizzate al trattamento). La designazione – peraltro richiesta dal nuovo d.lgs. 196/2003 all'art. 2-*quaterdecies* nel caso in cui i citati titolari e responsabili prevedano un'organizzazione delle attività di trattamento[1] – appare opportuna sotto il profilo dell'*accountability*, rappresentando la testimonianza di uno sforzo organizzativo compiuto per conseguire i predetti obiettivi di *compliance*. Il d.lgs. 231/2001, con la previsione dell'organismo di vigilanza per l'attuazione, da parte dell'ente, del Modello di Organizzazione, Gestione e Controllo (art. 6, c.1, lett. b)), ci offre un ulteriore spunto circa l'opportunità di costituire una struttura di controllo del funzionamento del modello organizzativo per la protezione dei dati, e dunque dello stato di adeguamento alla normativa. In questa prospettiva, si delineano ipotesi di costituzione di "gruppi di lavoro privacy" indipendenti (con componenti esterni all'organizzazione del trattamento) o di organi di *staff* collocati in posizioni di terzietà, in cui cioè non vengono determinate le finalità e i mezzi del trattamento; strutture che peraltro sono chiamate a supportare la funzione del *data protection officer* nei casi in cui una tale figura

sia stata designata dal titolare o dal responsabile del trattamento[2]. Il modello organizzativo privacy (insieme alla struttura di controllo) descrive pertanto un assetto aziendale preordinato allo svolgimento della propria attività in chiave *data protection*, rappresentando in tale prospettiva un'evoluzione culturale dell'organizzazione con effetti favorevoli sul piano dell'immagine e dei requisiti di affidabilità attesi o richiesti dall'esterno, ad esempio, nei rapporti con le associazioni dei consumatori, nelle attività di *public affairs*, nelle procedure di gara.

Profili di sicurezza del modello organizzativo data protection

Con riguardo al profilo della sicurezza dei trattamenti, il modello dovrebbe integrare processi, *routine* organizzative e regolamenti interni a supporto della gestione dei rischi, connotandosi pertanto anche come *governance* del rischio; sotto questo aspetto, le attività operative principali indicate dalla prassi e dalla letteratura tecnica comprendono (i) l'individuazione degli asset informatici che intervengono nelle attività di trattamento e la valutazione delle loro vulnerabilità, (ii) l'individuazione delle minacce incombenti sui sistemi di Ict (con cui i dati sono trattati), (iii) la valutazione del rischio (nelle sue componenti di probabilità e gravità delle conseguenze) alla luce delle misure di sicurezza esistenti, per poi (iv) determinare gli eventuali interventi (misure) di variazione che, in linea con le previsioni dell'articolo 32 del regolamento, possano garantire un livello di sicurezza adeguato al rischio[3]. Il (sintetico) processo operativo appena tratteggiato lascia intuire il suo carattere dinamico in ragione del fatto che il "rischio residuo", ossia il rischio a cui sono esposti i dati con l'applicazione delle *ultime* misure di sicurezza, va necessariamente rivalutato in relazione a possibili modifiche del quadro di riferimento (cambiamenti organizzativi, evoluzione tecnologica, nuove

modalità di trattamento, passaggio da dati comuni a dati particolari)[4].

I processi e le procedure che caratterizzano il modello organizzativo per gli aspetti di sicurezza vanno, altresì, integrati in relazione alla gestione dei casi di violazione che possono riguardare i dati personali, in ragione del fatto che anche l'adozione di misure di sicurezza efficaci non esclude che la minaccia possa verificarsi producendo un impatto; l'intervento *ex post*, dunque, va sempre pianificato in considerazione di un rischio che non è completamente e permanentemente eliminabile. La gestione delle violazioni (in cui la minaccia si è verificata, ma va accertato se e in che misura questa ha interessato dati personali) si caratterizza pertanto come capacità di reazione dell'organizzazione, implicando la costituzione di una *data breach unit* per il coordinamento di un complesso di attività volte a rilevare gli eventi e i comportamenti (*alert*, tracciamento degli accessi)e valutarne le caratteristiche (apertura di una scheda descrittiva) per decidere in merito alla loro registrazione[5], all'attivazione di protocolli di risposta e alle comunicazioni all'autorità di controllo e agli interessati. Una tale gestione è tanto più complessa in relazione all'esternalizzazione del trattamento in cui gli accordi di appalto e subappalto di operazioni sui dati personali coinvolgono più responsabili esterni del trattamento. Simili situazioni richiedono l'integrazione nel modello organizzativo di attività di gestione e coordinamento dei casi di violazione della sicurezza esterni al titolare – che avvengono, cioè, presso i responsabili o sub-responsabili del trattamento – affinché lo stesso possa venirne a conoscenza nei tempi più brevi, per poi valutare come procedere nel quadro delle previsioni degli articoli 33 e 34 del regolamento[6]. Con riguardo alla valutazione del rischio *post*-violazione che, nell'ambito di tale quadro, il titolare è tenuto a svolgere, merita osservare come la disponibilità di una preventiva analisi del rischio – ad esempio, quella che

ricorre nella valutazione di impatto del trattamento sulla protezione dei dati – possa rappresentare una fonte utile da cui derivare il rischio che consegue a una violazione dei dati personali; ben inteso la necessità di effettuare una valutazione aggiuntiva in relazione alle specifiche circostanze della violazione[7].

Il caso della piattaforma Rousseau

Il caso *Rousseau* – la piattaforma tecnologica del **Movimento 5 Stelle** utilizzata, tra l'altro, per svolgere operazioni di votazione – mostra come una gestione 'occasionale' dei processi sottostanti la valutazione dei rischi, priva di un modello organizzativo di riferimento, possa essere all'origine delle vulnerabilità dei sistemi di Ict del Movimento 5 Stelle che, con ogni probabilità, sono state sfruttate per compiere l'intrusione informatica e determinare la violazione dell'agosto del 2017[8].

Sotto questo profilo, l'attività ispettiva del Garante ha fatto emergere un quadro della sicurezza dei siti web gestiti dal Movimento caratterizzato da misure tecniche obsolescenti e da misure organizzative che non garantivano un apprezzabile livello di riservatezza agli iscritti alla piattaforma di *e-voting*. Le *policies* adottate ammettevano l'uso di chiavi di identificazione di lunghezza inferiore a otto caratteri che, in tal modo, risultavano facilmente esposte ad azioni di tipo *brute force*[9]; le stesse politiche sono apparse limitate con riguardo all'*auditing* informatico in ragione del mancato tracciamento degli accessi effettuati dagli amministratori di sistema e la mancata configurazione di profili di autorizzazione differenziati e limitati ai soli trattamenti e dati necessari in relazione agli specifici ambiti di operatività.

Conclusioni

La vicenda appena tratteggiata, come altre (si pensi ai casi *Ashley Madison* del 2015, *Heartbleed* del 2014, *Target* del 2013), lasciano intuire come l'assenza di una *governance* del rischio ovvero l'adozione di soluzioni destrutturate e approssimate siano l'immagine di una vulnerabilità di tipo organizzativo prima ancora che tecnico-strumentale; e come tale condizione possa generare impatti sulla sfera giuridica delle persone (diritti e libertà) o su taluni loro aspetti e interessi comunque significativi (economico-finanziario, fisico, psicologico) che possono anche determinare azioni legali da parte degli interessati. Sotto altro profilo – se pure non rilevante ai fini del regolamento – non vanno sottaciute le conseguenze sulle stesse aziende (e pubbliche amministrazioni) derivanti dalla mancanza di modelli organizzativi privacy. A tal riguardo, il caso ***Yahoo****!* – la ***data breach*** più importante della storia (oltre un miliardo di account violati) – é emblematico; gli attaccanti avrebbero sottratto nomi, indirizzi e-mail, numeri di telefono, date di nascita, password criptate e in qualche caso anche domande di sicurezza cifrate o in chiaro, con le relative risposte; tali dati sarebbero stati messi in vendita nel dark web, per circa 300.000 dollari. Anche a causa di questa violazione (e di altre precedenti, non comunicate tempestivamente dall'azienda), secondo alcuni analisti finanziari la quotazione di Yahoo!, nell'ambito dell'acquisizione da parte di Verizon, avrebbe subìto un ribasso di circa 350 milioni di dollari[10].

La *governance* del rischio descrive un aspetto centrale del modello organizzativo per la protezione dei dati personali delineato dal regolamento; da essa promanano le decisioni sul trattamento (tecnologie utilizzate, valutazione di impatto) ovvero, nel caso di una violazione dei dati, sulla notifica al Garante e la comunicazione agli interessati, nonché sugli accordi con gli operatori esterni che dovrebbero trattare dati

per conto del titolare. Nella prospettiva del regolamento, un tale modello è destinato a diventare il *driver* di una cultura organizzativa della *data protection* che, dal vertice alle unità operative, pone al centro il rischio per i diritti e le libertà degli interessati attuando processi strutturati e mezzi del trattamento che incorporano nativamente misure di anonimizzazione o pseudonimizzazione o, ancora, di minimizzazione dei dati.

---

[1] Sul punto, il primo comma dell'art. 2-*quaterdecies* stabilisce che "*Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.*".

[2] Merita al riguardo osservare come la letteratura abbia accostato la funzione del *data protection officer* a quella dell'organismo di vigilanza *ex* d.lgs. 231, in ragione dei compiti di sorveglianza che gli sono stati attribuiti dal regolamento, ponendo tra l'altro il quesito circa una possibile sovrapposizione dei ruoli in quelle realtà in cui è stato costituito un Odv. Sul punto si veda, tra gli altri P. Ghini, *Data protection officer: ODV per la privacy?*, 3 settembre 2015, https://www.tavoli231.it/single-post/2015/09/03/Data-protection-officer-ODV-per-la-privacy A. Sannoner, *Il rapporto tra Organismo di Vigilanza e il nuovo GDPR*, 14 settembre 2018, https://www.portale231.com/il-rapporto-tra-organismo-di-vigilanza-e-il-nuovo-gdpr/

[3] Sappiamo, al riguardo, che l'art. 32 non prescrive "misure minime" ma elenca alcune misure attuative, segnatamente (i) la pseudonimizzazione e la cifratura dei dati personali, (ii) la capacità di assicurare su base permanente la riservatezza,

l’integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, (iii) la capacità di ripristinare tempestivamente la disponibilità e l’accesso dei dati personali in caso di incidente fisico o tecnico, (iv) una procedura per testare, verificare e valutare regolarmente l’efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

[4] Si pensi, ad esempio al disegno di legge appena approvato in via definitiva recante “Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell’assenteismo” in virtù del quale, ai fini della verifica dell’osservanza dell’orario di lavoro, le amministrazioni pubbliche (di cui all’articolo 1, comma 2, del decreto legislativo n. 165/2001) dovranno introdurre sistemi di identificazione biometrica e di videosorveglianza in sostituzione dei diversi sistemi di rilevazione automatica, attualmente in uso. Una tale modifica del trattamento di dati personali implica una rivalutazione del rischio residuo alla luce dell’introduzione di dati biometrici precedentemente non raccolti.

[5] È il caso previsto dall’art. 33, par. 5 del regolamento che, in altre parole, stabilisce l’obbligo per i titolari del trattamento di costituire un registro delle violazioni dei dati personali, indipendentemente dalla necessità di comunicazione all’autorità di controllo e agli interessati.

[6] A tal riguardo, va ricordato che, nel caso di violazione di dati personali, il responsabile del trattamento è tenuto a informare il titolare dopo essere venuto a conoscenza della violazione stessa (art. 33, par. 2); il che lascia ragionevolmente intendere che sia il responsabile del trattamento ad attuare le misure tecniche e organizzative per la rilevazione delle violazioni della sicurezza e le loro eventuali implicazioni sui dati personali.

[7] Al riguardo, si veda Gruppo di lavoro articolo 29 per la

protezione dei dati, *Linee-guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679*, p. 12.

[8] Cfr. Garante per la protezione dei dati personali, *Provvedimento su data breach – 21 dicembre 2017*, Provvedimento n. 548/2017, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-dis

play/docweb/7400401; *Provvedimento su data breach – 4 aprile 2019*, Provvedimento n. 83/2019, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9101974

[9] Il tempo necessario per compiere l'attacco aumenta esponenzialmente all'aumentare della lunghezza della password e della tipologia di caratteri. Per proteggersi da questo tipo di attacco è dunque opportuno utilizzare password molto lunghe e complesse contenenti caratteri maiuscoli, minuscoli, numerici, simboli e spazi. In tal modo il tempo necessario per completare l'attacco potrebbe passare da pochi minuti a settimane o addirittura anni secondo la velocità del calcolatore che esegue i tentativi e il tempo di risposta del server o servizio che si sta attaccando. Sull'argomento si veda A. Carriero, *Virus e sicurezza informatica: attacco Brute Force*, https://www.matematicamente.it/informatica/informatica-di-base/virus-e-sicurezza-informatica-at Si veda anche R. Rijtano, *Brute force: cosa sono, come fare e prevenire gli attacchi a forza bruta*, https://www.cybersecurity360.it/nuove-minacce/brute-force-cosa-sono-gli-attacchi-a-forza-bruta-come-farli-e-prevenirli/

[10] Cfr. Clusit, *Rapporto 2017 sulla sicurezza ICT*, Milano, 2017, 16.

https://www.key4biz.it/modelli-organizzativi-per-la-gestione-d

ei-rischi-informatici-il-caso-rousseau/261942/

Canadian City Loses $500,000 to Phishing Attack

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/vWkEt6j1Crc/canadian-city-loses-500000-phishing-attack

---

Hackers Behind ‘Triton’ Malware Target Electric Utilities in US, APAC

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/cCzHgTmoKcQ/hackers-behind-triton-malware-target-electric-utilities-us-apac

---

Cybersecurity, nelle PMI si

cercano 2,5 milioni di esperti (che non si trovano)

Il cybercrime potrebbe diventare una grande opportunità di carriera per tutti i professionisti del settore, ma anche un'importante sfida per le aziende che dovranno saper affrontare questa carenza di personale qualificato. A correre i rischi maggiori non sono solamente le multinazionali, ma anche le piccole e medie imprese italiane.

A sostenere questa tesi, come riportato dal **Sole 24 Ore,** è **Gianni Fenu**, prorettore **Ict dell'Università di Cagliari** intervenuto in occasione dell'evento "*Cybersecurity, la sfida della sicurezza: il prossimo livello*" di Cagliari, promosso da **Digital innovation hub Sardegna** e **Nòva24:** "*Il settore più a rischio è quello delle piccole e medie imprese* – dice Fenu – *meno quello finanziario.*

Ne è convinto **Paolo Prinetto,** direttore del **CIni**, che oltre a spiegare il ruolo del Comitato Nazionale per la ricerca in **cybersecurity** nell'ecosistema nazionale ricorda che legata alla **Cybersecurity** "*manca una forza lavoro di due milioni e mezzo di figure*" e non a caso è stata lanciata una campagna di scouting tra i giovani di età compresa tra i 18 e i 23 anni.

5 punti cardine per attirare professionisti qualificati in materia di Cybersecurity

Wyser, azienda di selezione del personale, ha recentemente realizzato e redatto una strategia rivolta alle aziende che riconoscono la rilevanza della sicurezza cibernetica e vogliono coltivare talenti al proprio interno, data l'assenza delle figure nel mondo lavorativo. Ecco i consigli per le aziende:

- Formazione e aggiornamento continuo: Prevedere piani di investimento strutturati per un costante aggiornamento del personale
- Flessibilità nella ricerca e selezione: Includere nella selezione anche candidati con background non strettamente tecnico
- Misure di conciliazione vita-lavoro: Garantire flessibilità di orario e altri benefit per rendere l'azienda più attrattiva rispetto ai competitor
- Opportunità di carriera all'interno dell'azienda: Dare alle risorse la possibilità di crescere all'interno dell'azienda evitando così un rapido turn-over
- Diffusione di una cultura della cybersecurity in azienda: Costruire una cultura della sicurezza informatica a tutti i livelli, riconoscendo il valore dello specialista

Cybersecurity, nelle PMI si cercano 2,5 milioni di esperti (che non si trovano)

Aircraft Parts Maker ASCO Severely Hit by Ransomware

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/L7E95MxBui4/aircraft-parts-maker-asco-severely-hit-ransomware

Senators Question FBI on Russian Hack of Voting Firm

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/caUj-B-24Vs/senators-question-fbi-russian-hack-voting-firm

---

Cybercrime, Raoul Chiesa: vi spiego perché è in atto l'Hackmageddon

Un team di hacker potrebbe mettere in ginocchio un Paese, bloccando autostrade, aerei, banche, treni. Insomma uno scenario apocalittico, uno scontro finale: il cosiddetto **Armageddon.**

Non è fantascienza, ma una possibilità, secondo **Raoul Chiesa**, uno dei primi hacker etici italiani, celebre con lo pseudonimo di "Nobody", che ha parlato di '**Hackmageddon**' durante l'evento **Connecting The Future,** del **Consortium Garr** organizzato dal **Politecnico di Torino.**

Durante il suo intervento, ripreso in un'articolo de **La Stampa, Chiesa** sostiene che "*La guerra mondiale è in atto e l'Italia è impreparata. Il nostro Paese subisce attacchi silenziosi e invisibili: ci vengono rubati dati e proprietà intellettuali* – spiega l'hacker etico -. *Purtroppo non*

contrattacchiamo come fanno le altre nazioni, e, invece, dovremmo andare a capire chi ci attacca e cosa ci ruba. Altrimenti rimaniamo in ginocchio, ammanettati e bendati.“

Poi aggiunge: ” *Non basta scoprire l’indirizzo Ip: servono tecniche di tracciamento per capire chi c’è dietro. Serve una nuova generazione di di diplomatici cibernetici che spiegano ai ministri come muoversi. Non c’è ancora una leglislazione di guerra applicata agli attacchi cyber*“.

Le infrastrutture critiche il vero obiettivo

Secondo l’esperto “*Le infrastrutture critiche sono i principali obiettivi del crimine informatico, in modo particolare porti, aeroporti e stazioni. Nessuno credeva sarebbe stato possibile sabotare una centrale energetica, fino a quando è successo in* ***Ucraina****. Con l’Internet Of Things saremo sempre più esposti. Le vittime però non sono solo le infrastrutture critiche. Abbiamo dimostrato* – continua Chiesa – *che è possibile da remoto variare i dosaggi di una pompa di insulina e uccidere il paziente. Si può entrare nel sistema di un ospedale. cambiare una cartella medica o rubare informazioni e venderle alle assicurazioni”.*

Secondo l’hacker bisogna passare da un approccio teorico a uno pratico. “*Perché il web è come la sabbia: non è stato progettato per la sicurezza, ma per essere sempre disponibile. E’ un errore pensare che la sicurezza risieda in un software, che è un insieme di approcci e processi. I cittadini non capiscono che, se una cosa è gratis, è il perché il prodotto è l’utente. Scrivere sui social ciò che si fa alimenta il sistema che usa i nostri dati*“.

https://www.key4biz.it/cybercrime-raoul-chiesa-vi-spiego-perche-e-in-atto-lhackmageddon/261511/

Radiohead Defies Hackers, Releases Trove of Stolen Music

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/nx8OxxLFelk/radiohead-defies-hackers-releases-trove-stolen-music

---

Riconoscimento facciale, attacco hacker alla frontiera Usa. Rubate 100mila foto

Come non detto. Il dibattito sull'utilizzo della tecnologia per il riconoscimento facciale da parte delle forze dell'ordine americane è più acceso che mai.

Qualche ora fa il **Washington Post** ha diffuso la notizia di un attacco hacker ha preso di mira un contractor della **Us Customs and Border Protection (Cbp)**, la principale agenzia Usa per la sicurezza delle frontiere, in servizio di controllo doganale e di transito presso i varchi di confine nazionale. Secondo le stime sarebbero coinvolte 100.000 persone da questo attacco

informatico.

I rischi legati alla sicurezza del riconoscimento facciale

La società hackerata (un'azienda terzista) aveva archiviato i dati raccolti dalla Cbp, ovvero le informazioni personali dei viaggiatori, comprese le foto, i passaporti, le impronte digitali.

L'agenzia americana è venuta a conoscenza del 31 maggio che il subappaltatore aveva trasferito le immagini sulla sua rete. Il CBP non ha dichiarato quando la società ha trasferito le fotografie o quando si è verificato l'attacco informatico.

Il CBP aveva raccolto le immagini dei viaggiatori negli aeroporti e ai valichi di frontiera. Ha anche iniziato a utilizzare il riconoscimento facciale per identificare i viaggiatori, compresi quelli che cercano di entrare illegalmente nel paese.

L'attacco informatico si è verificato proprio mentre "*La Cbp sta espandendo il suo enorme apparato per il riconoscimento facciale e per la raccolta di informazioni sensibili dei viaggiatori, come le informazioni sulle targhe o gli identificatori sui social media*", ha denunciato **Neema Singh Guliani,** dell'American Civil Liberties Union (Aclu). "*Il modo migliore per evitare questo tipo di violazioni* – ha aggiunto – *è non raccogliere ed archiviare questi dati*".

Facial ID: un problema di privacy

Negli Usa, l'uso del riconoscimento facciale da parte delle agenzie governative, sta sollevando nuove domande sulla

privacy e sulla sicurezza dei dati. Ieri abbiamo dato la notizia del lancio di un nuovo sito chiamato AirlinePrivacy.com ad opera di un gruppo di attivisti della privacy, che mostra agli utenti quali compagnie aeree utilizzano il riconoscimento facciale per verificare l'identità dei passeggeri prima dell'imbarco in aeroporto.

Il progetto, nato a difesa e tutela dei diritti dei viaggiatori, aiuta inoltre i clienti a prenotare voli direttamente con compagnie aeree che non utilizzano questo tipo di tecnologie invasive.

Lo scorso maggio la città di **San Francisco** ha votato per metterne al bando l'utilizzo da parte della polizia. E' la prima città Usa ed altre municipalità americane stanno pensando di seguirne le orme.

Per approfondire

https://www.key4biz.it/riconoscimento-facciale-attacco-hacker-alla-frontiera-usa-rubate-100mila-foto/261291/

"MuddyWater" Cyberspies Update PowerShell Backdoor

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/fSja-1Luqkg/muddywater-cyberspies-update-powershell-backdoor