Università degli Studi di Padova

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea Triennale in

DIRITTO E TECNOLOGIA

Il caso Twilio: data breach e sicurezza delle API alla luce della normativa californiana ed europea

Relatore: Filippo Viglione

Correlatrice: Giulia Binato

Laureando: Alberto Fabris

Matricola: 2038934

Anno accademico: 2023/2024

ABSTRACT

La digitalizzazione di ogni aspetto della quotidianità comporta il costante incremento delle tipologie di servizi fruibili nel contesto digitale, ai quali gli utenti, per esigenze contrattuali, si trovano a fornire dati personali. L'elaborato si propone di analizzare il caso di Twilio, un'azienda californiana che offre una molteplicità di servizi di comunicazione e autenticazione, attraverso servizi web API. Recentemente, l'azienda è stata interessata da una massiva fuga di dati degli user dei propri servizi.

La tesi effettua una disanima degli aspetti tecnici e di funzionamento delle piattaforme di comunicazione basate su cloud e degli API, analizzando il data breach dal punto di vista tecnico e legale. Vengono altresì individuate le possibili minacce connesse al breach, come, ad esempio, phishing e smishing. Successivamente, viene discusso il quadro normativo e la responsabilità per data breach nell'approccio statunitense, ed in particolare nella legislazione californiana contenuta nel CPRA (California Privacy Right Act) e CCPA (California Consumer Privacy Act). È poi proposta una disamina del caso alla luce del contesto europeo, con considerazione dell'assetto normativo derivante dal GDPR e delle direttive fornite dalla EDPB (European Data Protection Board) e dal Garante della Privacy italiano.

Da ultimo, si propongono alcuni spunti di riflessione per il futuro alla luce del caso Twilio. In particolare, ci si sofferma su alcune proposte pratiche volte ad aumentare la sicurezza e tutela dei dati personali per chi usufruisce di questi servizi, anche considerando il panorama dell'intelligenza artificiale e gli strumenti di machine learning.

INDICE

INTRODUZIONE

Negli ultimi anni, l'importanza dei servizi digitali offerti dalle piattaforme online è cresciuta in modo esponenziale. Dalla gestione delle comunicazioni, al trattamento di dati sensibili, fino al supporto per transazioni economiche, l'utilizzo di applicazioni basate su API (Application Programming Interface) è diventato essenziale per aziende e utenti. Queste tecnologie permettono a diversi sistemi di comunicare tra loro in modo rapido ed efficiente, integrando funzionalità complesse in vari settori, dalla sanità all'e-commerce.

Tuttavia, la crescente interconnessione di servizi ha portato a una maggiore esposizione dei dati personali degli utenti. Le API, in particolare, rappresentano spesso un punto vulnerabile se non adeguatamente protette. Nel caso analizzato, si andrà a comprendere come gli attacchi informatici, possono sfruttare falle nella sicurezza delle API per accedere illegalmente a informazioni sensibili, con conseguenze devastanti in termini di *data breach* sia per le aziende che per gli utenti finali.

In seguito, si provvederà ad analizzare la dottrina Californiana e quella Europea alla luce del caso, mostrando cosa l'approccio giurisprudenziale, relativamente nuove verte in materia di tutela dei dati della privacy.

CAPITOLO 1

LA PIATTAFORMA TWILIO E IL DATA BREACH SUBITO

Sommario: 1.1 L'azienda Twilio e l'applicazione di autenticazione a due fattori Authy. 1.2 L'attacco hacker a Twilio 1.3 La reazione dell'azienda e le conseguenze dell'attacco.

1.1 L'azienda Twilio e l'applicazione di autenticazione a due fattori Authy

L'azienda Twilio, con sede legale a San Francisco, California[1], è una piattaforma su cloud[2] che offre una molteplicità di servizi di comunicazione, come chiamate vocali, videochat, e-mail. Questi servizi sono integrabili in applicazioni di terze parti, sicché si rivolgono principalmente ad una clientela composta da sviluppatori ed aziende che vogliono implementare le funzioni nei propri sistemi.

Il 24 Febbraio 2015, l'azienda ha acquisito Authy[3], un servizio di autenticazione a due fattori integrabile in sistemi di terze parti, il quale garantisce un ulteriore livello di sicurezza rispetto all'uso della password tradizionale. L'autenticazione a due fattori (2FA) è un metodo di sicurezza che aggiunge un ulteriore livello di protezione alle password, richiedendo un secondo passaggio di verifica dell'identità dell'utente prima di consentire l'accesso a risorse o servizi.[4]

La forma più comune di 2FA è la forma più comune di autenticazione a due fattori (2FA) è basata sulle OTP (One-Time Password), ossia password temporanee a breve scadenza. Queste password vengono generate tramite apposite applicazioni o dispositivi, e hanno una durata limitata, solitamente di circa 30 secondi, dopodiché vengono automaticamente sostituite da una nuova. Tale dinamicità aumenta significativamente il livello di sicurezza,

---

[1] *UNITED STATES SECURITIES AND EXCHANGE COMMISSION*, « SEC», 26 maggio 2016, < https://www.sec.gov/Archives/edgar/data/1447669/000104746916013448/a2227414zs-1.htm>.

[2] Twilio nel panorama dell'offerta di servizi cloud si pone come magnate, avendo raggiunto nell'anno 2023 un fatturato pari a $ 4,154 miliardi e una quota di utenti attivi che supera le 300'000 persone.

[3] LARDINOIS F. *Twilio Acquires Two-Factor Authentication Service Authy,* «TechCrunch», 24 febbraio 2015, < https://techcrunch.com/2015/02/24/twilio-acquires-two-factor-authentication-service-authy/>, (ultimo accesso: 9 ottobre 2024).

[4] GADDE ET AL., *Secure Data Sharing in Cloud Computing*, 2023, p. 1468.

poiché risulta estremamente difficile indovinare una password che cambia così frequentemente.[5] Una tra i servizi più utilizzati di autenticazione a due fattori è "Authy", che, come si è visto, è offerto dall'azienda Twilio.

1.2 L'attacco hacker a Twilio

Il 27 giugno 2024 l'applicazione Authy ha subito un grave fuga di dati a causa di un attacco hacker, sferrato dal gruppo degli "ShinyHunters". Si tratta di un'organizzazione hacker che ricade sotto la catalogazione "blackhat"[6], ovvero un insieme di individui altamente preparati sotto il profilo tecnico che violano leggi o codici etici per commettere reati, con l'obiettivo di rubare ingenti quantità di informazioni personali per trarne profitto economico. [7]Il gruppo è noto per bersagliare compagnie di alto profilo: tra gli attacchi più noti vi è quello risalente al 2 Maggio 2020, effettuato ai danni di Tokopedia[8], lo store online più grande dell'Indonesia, con conseguente furto di 71 milioni di informazioni personali, tra cui indirizzi e-mail, numeri di telefono, dettagli anagrafici e anche password. Anche Microsoft è stata soggetta a violazioni da parte degli ShinyHunters, quando il 7 Maggio 2020 sono stati sottratti oltre 500 Gigabyte di dati provenienti dai repositories[9] GitHub private di Microsoft[10]

Nello specifico, l'attacco informatico a Twilio è avvenuto tramite lo sfruttamento di un *endpoint* API *(* acronimo, come noto, di *Application Programming Interface)* non autenticato[11]. Come noto, un *endpoint* API rappresenta una posizione digitale specifica in cui un'API riceve richieste per accedere o interagire con le risorse gestite dal server[12]. Per gli hacker, gli endpoint rappresentano uno dei punti di accesso più preziosi, poiché offrono la possibilità di ottenere dati aziendali o personali sensibili. Questi dispositivi, come computer, smartphone o tablet,

---

[5] GAO ET AL., *Information and Communications Security. Part 1,* 2021, p. 98.

[6]La controparte, I "white-hat" sono hackers che utilizzano gli stessi strumenti dei criminali informatici per testare la sicurezza nei sistemi informatici, scovando e risolvendo eventuali debolezze. Prasad, «Ethical hacking and types of hackers».

[7] CHNG ET AL., *Hacker Types, Motivations and Strategies*, 2022, p. 3.

[8] A. ELOKSARI E., *Tokopedia data breach exposes vulnerability of personal data*, «TheJakartaPost», 5 maggio 2020 , <https://www.thejakartapost.com/news/2020/05/04/tokopedia-data-breach-exposes-vulnerability-of-personal-data.html>, (ultimo accesso: 9.10.2024).

[9] Archivio digitale centralizzato che gli sviluppatori utilizzano per apportare e gestire le modifiche al codice sorgente di un'applicazione

[10] *MONTALBANO E., Report: Microsoft's GitHub Account Gets Hacked*, «Threatpost», 8 maggio 2020, <https://threatpost.com/report-microsofts-github-account-gets-hacked/155587/>, (ultimo accesso: 9.10.2024).

[11] IKEDA S., *Twilio Data Breach That Exposed 33 million Authy Phone Numbers Caused by Unsecured API Endpoint*, «CPO Magazine», 8 luglio 2024, <https://www.cpomagazine.com/cyber-security/twilio-data-breach-that-exposed-33-million-authy-phone-numbers-caused-by-unsecured-api-endpoint/>, (ultimo accesso: 9.10.204).

[12] IBM, *What is an API endpoint?,* «IBM», <https://www.ibm.com/topics/api-endpoint>, (ultimo accesso: 9.10.2024)

spesso si trovano al di fuori della protezione diretta delle reti aziendali e sono più vulnerabili. La loro sicurezza, infatti, dipende principalmente dalle precauzioni adottate dagli utenti stessi, come l'aggiornamento regolare dei software, l'utilizzo di antivirus e la gestione delle password, piuttosto che dalle misure di sicurezza centralizzate dell'azienda.

Utilizzando un endpoint specifico, il gruppo di hacker ha caricato una lista enorme di numeri di telefono per identificare quelli associati a un account Authy. Questa tecnica, nota come enumerazione degli account, consente di verificare se un determinato numero di telefono o indirizzo e-mail è collegato a un servizio specifico. In pratica, gli hacker cercano di scoprire quali numeri di telefono nell'elenco risultano registrati su Authy, utilizzando una sorta di "tentativo di enumerazione massiva." Attraverso questo approccio, sono riusciti a confermare e ottenere informazioni su 33,4 milioni di numeri di telefono. Questa tecnica può essere utilizzata anche con indirizzi e-mail per determinare quali tra di essi sono collegati a un determinato servizio online[13]

1.3 La reazione dell'azienda e le conseguenze dell'attacco

La reazione immediata da parte dell'azienda Twilio è stata provvedere prontamente ad un aggiornamento dell'applicazione Authy per risolvere la falla. Successivamente, l'azienda ha rilasciato uno statement nel quale afferma che: *"Anche se gli account Authy non sono compromessi, gli attori delle minacce possono tentare di utilizzare il numero di telefono associato agli account Authy per attacchi di phishing e smishing;*[14]*"*

L'esito dell'attacco è stato dunque una importante fuga di dati, successivamente rilasciati nel dark web, con la dispersione di circa 33 milioni di contatti telefonici. Anche individui che non hanno usufruito di Authy, ma hanno interagito con piattaforme che integrano i propri sistemi con i servizi offerti da Twilio sono stati colpiti. L'applicazione "Too Good to Go", a tal proposito, ha rilasciato il seguente comunicato tramite e-mail a vari utenti, in cui afferma: *" Too Good To Go utilizza Twilio come servizio di messaggi SMS per diverse notifiche agli utenti. Too Good To Go ha condotto un'analisi degli utenti che hanno utilizzato il servizio Twilio durante il periodo a rischio e il vostro numero di telefono è stato identificato. Si noti che la notifica di Twilio indica che Twilio non può escludere la possibilità che attori minacciosi abbiano avuto accesso ai dati*

[13] MACEIRAS ET AL., *Know Their Customers*, 2024, p. 37:3.

[14] TWILIO, Security Alert: Update to the Authy Android (v25.1.0) and iOS App (v26.1.0) «Twilio », 1 luglio 2024, <https://www.twilio.com/en-us/changelog/Security_Alert_Authy_App_Android_iOS>, (ultimo accesso: 9.10.2024).

interessati dalla violazione. Too Good To Go desidera pertanto sottolineare l'aumento del rischio che il numero di telefono possa essere utilizzato per attacchi di phishing e smishing[15]*."*
Il possesso di numeri di telefono personali da parte di terzi sconosciuti è infatti terreno fertile per attacchi di ingegneria sociale, termine con cui si fa riferimento a pericoli di cybersecurity che si fondano sullo sfruttamento dell'errore umano, tramite l'uso di artefici psicologici allo scopo di ottenere da parte dell'utente informazioni strettamente personali[16]. Tra le pratiche di ingegneria sociale più frequenti vi sono, come indicato anche dalle piattaforme interessate, il Phishing e lo Smishing, reati su cui si tornerà più ampiamente nel prosieguo.

[15] *Too Good To Go security data breach Jan 1-May 15, 2024*, luglio 2024, «Reddit», <https://www.reddit.com/r/TooGoodToGoCanada/comments/1e0msf4/did_any_else_get_a_too_good_to_go_user_security/>, (ultimo accesso: 9.10.2024) https://www.reddit.com/r/TooGoodToGoCanada/comments/1e7irh2/too_good_to_go_security_data_breach_jan_1may_15/>.
[16] PELTIER T., *Social engineering: Concepts and solutions*, 2006, p. 13.

CAPITOLO 2

PREMESSE TECNOLOGICHE: IL CLOUD, LE API E LA SFERA DEL DATA BREACH

Sommario: 2.1 Il Cloud. 2.2 Architettura: Back-End, Front-End. 2.3 Cloud Delivery Service: PAAS, SAAS, IAAS. 2.4 API. 2.5 Analisi tecnica del Data Breach. 2.6 Cenni: reati di Phishing e Smishing.

2.1 Il Cloud

Il termine *Cloud Computing* venne coniato nel 1996 dall'ex azienda americana[17] produttrice di computers Compaq, per riferirsi ad alcuni servizi che stavano progettando con l'obiettivo di archiviare informazioni online.[18]

Per Cloud, -conosciuto anche come Cloud Computing- oggi intendiamo sia le tipologie di piattaforme disponibili sia un tipo di applicazione. Quando ci riferiamo alle prime, affermiamo che una piattaforma Cloud fornisce, configura, riconfigura e svolge azioni di deprovisioning[19] in maniera dinamica, sui server come e quando ve n'è bisogno.

Se invece ci riferiamo all'aspetto applicativo del Cloud Computing, ci stiamo riferendo a quelle applicazioni che sono distribuite tramite internet e utilizzano enormi data center e server ad alte prestazioni. Queste infrastrutture consentono alle applicazioni e ai servizi web di essere eseguiti in modo efficiente, garantendo accessibilità globale, affidabilità e capacità di gestire grandi volumi di traffico[20].

La definizione differisce in base alla sfera coinvolta[21]. Ad esempio, il *Wall Street Journal*[22] afferma che il Cloud Computing sarebbe una modalità di incrementazione del potere computazionale per le imprese ma anche di spazio di archiviazione e applicazioni software.

---

[17] Nel 2002 fu acquistata da Hewlett Packard

[18] MOSCO V., *To the Cloud, 2016, pp. 15, 16.*.

[19] processo mediante il quale un amministratore di sistema toglie risorse e privilegi, non solo agli utenti di una rete ma anche a chi le utilizza da remoto

[20] HUAWEI TECHNOLOGIES CO., LTD., *Cloud Computing Technology, 2016, p 8*.

[21] Ibidem.

[22] Cloud Computing: A Top-Down View, «The Wall Street Journal», <https://deloitte.wsj.com/cio/cloud-computing-a-top-down-view-01671128650>, (ultimo accesso: 9.10.2024).

IBM, invece, sostiene che il Cloud Computing sia uno stile di computazione basato sulla consegna di servizi, software e potere di processazione su reti pubbliche o private, ponendo un forte accento sulla "user experience[23]".

Per una definizione più completa del Cloud, possiamo descriverlo come un insieme di risorse computazionali, sia software che hardware, che possono essere condivise e fornite su richiesta attraverso reti remote. Queste risorse, rese accessibili tramite tecnologie avanzate, consentono l'uso flessibile e scalabile delle capacità di elaborazione, memoria e dati, sia in modo condiviso che dedicato, ottimizzando l'efficienza e la disponibilità dei servizi.

2.2 Architettura: Back-End, Front-End

Con l'espressione architettura Cloud intendiamo il modo in cui vari componenti Cloud come hardware, software e risorse virtuali si combinano ed interagiscono per dar vita ad un ambiente di Cloud Computing.[24]La maggior parte dei servizi cloud è accomunata da una struttura tripartita, composta da *front-end*, *back-end* e dalla c.d. delivery basata sul cloud.

La parte *front-end* del Cloud computing è la parte interamente dedicata alla fruizione dell'utente finale (*consumer)*, quindi la parte con cui l'utente che fruisce del servizio può "interagire" (*interact)*[25] . Essa comprende elementi visivi come, ad esempio, caselle di controllo, pulsanti e, più in generale, la c.d. GUI (interfaccia grafica utente). Il front-end permette di gestire le interazioni fondamentali dell'utente, le quali verranno trasmesse al back-end[26].Il Back-end -detto anche *lato server* - è la parte che elabora la risposta alla richiesta effettuata dell'utente attraverso la parte front-end. La parte back-end è quella che comprende i server virtuali, la capacità di computazione e storage che garantiscono il funzionamento della struttura e permette l'archiviazione e l' elaborazione dei dati. L'architettura back-end del cloud adotta tecnologie di archiviazione e di gestione dei dati su database che ne consentono l'estrazione in maniera efficace, così come la definizione di schemi di archiviazione e l'implementazione di meccanismi di sicurezza dei dati, attraverso l'applicazione di protocolli

[23] relazione tra una persona e un prodotto, un servizio, un sistema con approccio olistico: cerca di comprendere tutto ciò che ruota attorno all'interazione di un utente con un'azienda, un marchio o un'istituzione.

[24] GOOGLE, What is Cloud Architecture?, «Google Cloud», <https://cloud.google.com/learn/what-is-cloud-architecture?hl=it>, (ultimo accesso: 9.10.2024)

[25] HPE, «Architettura cloud, <https://www.hpe.com/it/it/what-is/cloud-architecture.html>, (ultimo accesso: 7 ottobre 2024)».

[26] Google Cloud, «What is cloud architecture?, <https://cloud.google.com/learn/what-is-cloud-architecture?hl=it>, (ultimo accesso: 7 ottobre 2024)»

di autenticazione e un consapevole uso della crittografia. È grazie alla virtualizzazione delle risorse che si è verificato il passaggio dalla rigidità tradizionale tipica delle strutture "on premise" ad una scalabilità dei servizi in base alle continue e mutevoli esigenze, senza il pesante investimento in ulteriori apparecchiature[27].

2.3 Cloud Delivery Service: IAAS, SAAS, PAAS

La giuntura tra le due parti appena considerate, front-end e back-end, è effettuata dalla c.d. "Cloud service delivery" ovvero la delivery basata su cloud, che corrisponde alla modalità finale in cui i determinati servizi vengono forniti agli utenti. Se ne possono distinguere molteplici forme; le più usufruite sono le *Platform as a Service (Paas)* , le *Infrastructure as a Service (IaaS)* e le *Software as a Service (Saas)*. In tutte queste nomenclature, l'espressione "*as a service*" è volta a sottolineare la virtualizzazione della tipologia di servizio, che viene dunque offerto tramite il Cloud.

Le *IaaS* sono delle infrastrutture computazionali accessibili a richiesta, come server e capacità di storage. L'acquirente del servizio IaaS può gestire queste risorse in maniera molto simile a come gestirebbe un'infrastruttura fisica tradizionale, potendo configurare server, reti e ambienti di sviluppo a seconda delle proprie esigenze. Tuttavia, a differenza di un'infrastruttura fisica, l'utente non deve preoccuparsi della gestione e manutenzione dell'hardware sottostante, poiché questa è completamente a carico del cloud service provider. L'utente si limita ad accedere e utilizzare le risorse acquistate tramite una connessione internet, con la flessibilità di adattare dinamicamente la propria infrastruttura secondo le necessità operative, senza dover gestire direttamente l'hardware[28].

Con il termine SaaS si fa riferimento ad una applicazione software cloud-hosted[29], pronta all'uso. Per le aziende, la realtà delle SaaS risulta essere estremamente conveniente e versatile: essa consente di usufruire di un software a seconda delle proprie necessità, senza dover adottare precauzioni infrastrutturali - quali servers, archiviazione dati e mantenimento della connessione – che sono tutte a carico di colui che offre il servizio. Inoltre, chi acquista un

[27] AMAZON, *Qual è la differenza tra front-end e back-end nello sviluppo delle applicazioni?,* «AWS Amazon», https://aws.amazon.com/it/compare/the-difference-between-frontend-and-backend/, (ultimo accesso: 09.10.2024)

[28] HUAWEI TECHNOLOGIES CO., LTD., *Cloud Computing Technology, 2016, p 31*.

[29] applicazioni o risorse che vengono gestiti e ospitati su server remoti di un provider di servizi cloud, accessibili via internet.

servizio SaaS può usufruire dell'applicazione acquistata in una maniera con altri dati e applicazioni già presenti nel proprio 'ambiente. Infine, la modalità di pagamento più soventemente utilizzata è detta "pay-as-you-go": [1] un sistema di pagamento in cui si paga solo per le risorse effettivamente utilizzate[30], senza costi fissi o anticipati garantendo libertà e flessibilità nell'erogazione dei servizi delle SaaS[31].

Il modello di servizio Cloud di più recente formazione sono le PaaS (Platform as a Service). Si tratta di piattaforme virtualizzate su diversi server, le quali forniscono un largo numero di strumenti agli sviluppatori che fungono da basi per strutturare un'applicazione, testarla e svilupparla[32]. A tali strumenti, si affiancano anche servizi secondari, come ad esempio integrazioni per i servizi-web, grazie ai quali è possibile programmare e gestire applicazioni. Anche in questo caso, le PaaS offrono un elevato livello di convenienza e facilità d'uso grazie alla loro natura "Out-of-the-box". Il termine "Out-of-the-box" indica che la piattaforma è pronta all'uso immediatamente dopo l'acquisto o la sottoscrizione, senza richiedere complesse configurazioni o installazioni iniziali da parte dell'utente. Inoltre, con le PaaS, non è necessario installare o gestire middleware, ossia quei software che fungono da intermediari tra il sistema operativo e le applicazioni. Il middleware include strumenti e servizi come server web, database, sistemi di messaggistica o ambienti runtime[33].

Nelle soluzioni PaaS, queste componenti sono preconfigurate e integrate nella piattaforma, pronte per essere utilizzate senza ulteriori interventi tecnici da parte dell'utente. Un ulteriore vantaggio delle PaaS è che l'utente non deve preoccuparsi di "patchare" il sistema, ovvero applicare aggiornamenti di sicurezza e correzioni a eventuali bug nel software. Questo compito è gestito direttamente dal fornitore del servizio PaaS, che si occupa di mantenere la piattaforma aggiornata e sicura, eliminando il carico di gestione e manutenzione che normalmente graverebbe sugli utenti. Inoltre, lo sviluppo di applicazioni su piattaforme PaaS offre un notevole vantaggio in termini di *Time to Value* (TTV), ossia la rapidità con cui le applicazioni possono essere sviluppate, distribuite e iniziare a generare valore per l'azienda. Grazie agli strumenti preconfigurati e all'infrastruttura già predisposta, gli sviluppatori possono ridurre drasticamente i tempi di configurazione e setup, concentrandosi immediatamente

[30] *Differenza tra licenza cloud ad abbonamento, pay-as-you-go, pay-by-instances e BYOL*, «Informatica e Ingegneria Online», <https://vitolavecchia.altervista.org/differenza-tra-licenza-cloud-ad-abbonamento-pay-as-you-go-pay-by-instances-e-byol/ >, (ultimo accesso: 7 ottobre 2024)».

[31] SATYANARAYANA S., *Cloud computing: SAAS*, 2012, p. 77.».

[32] TSAI W., SUN X., BALAASORIYA J., *Service-Oriented Cloud Computing Architecture*, 2010, p. 684.

[33] YASRAB R., *Platform-as-a-Service (PaaS)*, 2018, p. 1.

sullo sviluppo delle funzionalità core dell'applicazione. Questo accelera il ciclo di vita dello sviluppo software, portando più rapidamente l'applicazione sul mercato[34].

Un altro vantaggio cruciale delle PaaS è la scalabilità. Le piattaforme PaaS consentono di aumentare o diminuire le risorse necessarie, come capacità di calcolo, storage o rete, in modo semplice e flessibile. Qualora il volume di utenti o la domanda per l'applicazione aumenti, è possibile acquistare ulteriori risorse senza interruzioni nel servizio e senza dover ridimensionare manualmente l'infrastruttura. Questa capacità di scalare istantaneamente e in base alle necessità è particolarmente vantaggiosa per le aziende che affrontano picchi di domanda imprevisti o crescita rapida, garantendo che le applicazioni possano adattarsi senza perdere prestazioni o stabilità[35].

2.4 API

Le persone interagiscono con il software attraverso un'interfaccia utente, ma anche le applicazioni possono sfruttare un software tramite un'API (Application Programming Interface). Un'API permette alle applicazioni di connettersi, integrarsi e utilizzare funzionalità o dati di un sistema software in modo efficiente. È come una presa di corrente a cui possono essere collegate facilmente diverse applicazioni, consentendo la condivisione e l'uso di risorse interne all'azienda con consumatori esterni. Le API, dunque, agiscono come un ponte tra chi fornisce e chi utilizza i dati, semplificando i processi di comunicazione tra i sistemi[36].

Le API sono sviluppate partendo dal principio “aperto/chiuso”[37], in particolare, in riferimento alla programmazione orientata agli oggetti, cioè un paradigma di programmazione che permette di definire oggetti software in grado di interagire gli uni con gli altri attraverso lo scambio di messaggi. In tale contesto, il principio “aperto/chiuso” afferma che i software dovrebbero essere aperti all’estensione, ma chiusi alle modifiche, cosicché il loro comportamento possa essere modificato senza però alterarne la natura stessa, quindi il codice sorgente[38]. Questo fa sì che le API possano essere estese ed applicate in moltissimi

[34] Ibidem.
[35] Ibidem.
[36] BIEHL M., *API architecture, 2015, p. 4.*
[37] Ibidem.
[38] OMENA J., CURRIE E., *Collecting Data Using APIs Part 1: How to Understand APIs and Navigating API Documentation*, 2022, P. 4.

contesti. Twilio, ad esempio, le sfrutta per fornire diverse possibilità di comunicazione, come l'inserzione di plug-in video o di messaggistica all'interno delle applicazioni.

Uno stile architettonico rappresenta una soluzione strutturale predefinita su larga scala. Utilizzare stili architettonici consente di sviluppare i sistemi in modo più rapido rispetto alla costruzione di tutto da zero. In particolare, Twilio si avvale delle REST API, ovvero di API che seguono i principi di progettazione architetturale "representational state transfer" (REST). Un sistema c.d. *"RESTful"* è progettato per sfruttare efficientemente le infrastrutture HTTP, e grazie all'estensivo uso del linguaggio HTTP nel Web, infrastrutture come servers, caches e proxies sono ampiamente disponibili. L'HTTP (HyperText Transfer Protocol) è un protocollo che definisce un insieme di procedure basate su un sistema di richieste e risposte per la trasmissione di informazioni sul web. Questo scambio di informazioni avviene generalmente quando un browser accede a un server web o quando un'app client interagisce con un'API.

Le API REST eseguono funzioni di creazione, lettura, aggiornamento e eliminazione di record* all'interno di una risorsa, utilizzando diversi comandi come GET per recuperare un record, POST per crearne uno nuovo, PUT per aggiornarlo e DELETE per eliminarlo.

L'architettura REST presenta diversi vantaggi grazie alla condizione stateless dei sistemi REST. Un server stateless non memorizza alcuna informazione riguardante le sessioni o le interazioni passate con i client. Invece, è il client a mantenere lo stato dell'applicazione. Ad ogni richiesta, il server deve ricevere dal client tutte le informazioni necessarie per elaborarla, e la risposta del server deve includere i dati aggiornati che consentono al client di mantenere lo stato dell'applicazione. Questo approccio garantisce che, anche in assenza di uno stato salvato sul server, il client abbia sempre le informazioni necessarie per continuare a funzionare correttamente. Questo garantisce anche un'alta tolleranza ai malfunzionamenti, disponibilità e affidabilità del sistema. Inoltre, l'architettura REST risulta molto semplice rispetto ad altre tipologie di architetture API.[39]

[39] BIEHL M., *API architecture, 2015, pp.49,50*.

2.5 Analisi tecnica del Data Breach

La fuga di data o "*data Breach*"[40] può essere definita come la perdita, distruzione, modifica, divulgazione non autorizzata oppure l'accesso - intenzionale o non intenzionale - di informazioni confidenziali da parti non autorizzate[41].

Complessivamente, esistono tre principali categorie di *data breach*: una violazione della riservatezza si verifica quando le informazioni personali vengono divulgate senza autorizzazione, che sia per errore o a seguito di un'azione deliberata. In pratica, dati sensibili possono essere esposti a persone non autorizzate, compromettendo la privacy degli individui coinvolti. Un esempio potrebbe essere l'invio accidentale di un'e-mail contenente informazioni riservate a un destinatario sbagliato. Una violazione della disponibilità si ha invece quando i dati personali non sono più accessibili o vengono persi, anche in modo accidentale. Questo tipo di violazione può creare notevoli disagi, specialmente se si tratta di dati fondamentali per il funzionamento di un servizio o per decisioni importanti. Infine, una violazione dell'integrità avviene quando i dati personali vengono alterati senza permesso. Questo include modifiche non autorizzate, intenzionali o accidentali, che potrebbero compromettere l'accuratezza e l'affidabilità delle informazioni[42].

Nel contesto di una fuga di dati, possono verificarsi diverse forme di violazione. Un esempio comune è la perdita o il furto di dati personali dovuti alla negligenza delle persone incaricate della loro protezione. Questo può avvenire quando coloro che gestiscono tali informazioni o i collaboratori coinvolti perdono il controllo sugli strumenti che contengono i dati. Un'altra possibilità è che informazioni sensibili vengano sottratte a causa di una gestione inadeguata o di misure di sicurezza insufficienti. Inoltre, si possono verificare accessi illegali da parte di soggetti non autorizzati ai sistemi informatici, come attraverso attacchi di ransomware, che mirano al furto di documenti e possono compromettere sia la disponibilità sia la riservatezza dei dati[43]. Attacchi come SQL injection[44] mirano a copiare e abusare dei dati personali,

---

[40] La National Association of Attorney General definisce un data breach come l'acquisizione illegale e non autorizzata di informazioni personali che ne compromette la sicurezza, la riservatezza o l'integrità. L'articolo 4 (12) del GDPR definisce data breach come una violazione della sicurezza che comporta la distruzione accidentale o illegale, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o altrimenti trattati

[41] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida per la gestione delle violazioni di dati personali e la loro eventuale comunicazione all'Autorità e ai soggetti interessati* , pp. 3, 4.

[42] ibidem

[43] Software malevolo che limita l'accesso del dispositivo che infetta.

[44] Attacco in cui il codice dannoso viene inserito in stringhe che vengono successivamente passate a un'istanza del Motore di database di SQL Server per l'analisi e l'esecuzione.

compromettendo sia la riservatezza che, talvolta, l'integrità dei dati. Infine, gli attacchi di phishing, che prevedono l'invio di email contraffatte per ingannare i destinatari a fornire dati riservati, rappresentano una grave violazione della riservatezza dei dati personali. [45].

2.6 Cenni: reati di Phishing e Smishing

È da prevedere che per queste numerose vittime avvengano attacchi phising e/o smishing: Il phishing è un attacco in cui l'aggressore sfrutta tecniche di ingegneria sociale[46] per compiere un furto di identità. Questo tipo di frode si svolge tipicamente attraverso l'invio massivo di email o messaggi (spamming) a una vasta platea di utenti.

Nella maggior parte dei casi, i messaggi segnalano un presunto accesso non autorizzato al all'area personale dell'utente, invitandolo a verificare o aggiornare le proprie credenziali, come nome utente e password. Questi messaggi reindirizzano le vittime a un sito web che appare identico a quello camuffato, ma è in realtà un sito fraudolento, progettato per catturare i dati inseriti.

Il phishing sfrutta l'ingenuità e l'inesperienza degli utenti, facendosi passare per comunicazioni affidabili, con l'obiettivo di ottenere l'accesso a informazioni personali o finanziarie sensibili.

Il reato di phishing, come previsto dal Codice Penale, può configurarsi sotto diverse fattispecie. In primo luogo, rientra nell'articolo 640-ter c.p., che disciplina la frode informatica. Questo reato punisce chiunque alteri o intervenga su un sistema informatico o telematico, o sui dati in esso contenuti, al fine di ottenere un ingiusto profitto a danno altrui[47]. L'elemento oggettivo del reato è costituito dall'intervento non autorizzato sui dati o sui programmi del sistema, il che comprende qualsiasi forma di interferenza illecita.

Inoltre, il phishing può essere ricondotto all'articolo 494 c.p., che tratta della sostituzione di persona. Questo si verifica quando l'autore del reato induce in errore qualcuno sostituendosi a un'altra persona, attribuendosi un'identità falsa o una qualità giuridicamente rilevante per ottenere un vantaggio o arrecare un danno[48].

---

[45] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida per la gestione delle violazioni di dati personali e la loro eventuale comunicazione all'Autorità e ai soggetti interessati*, pp. 3, 4.

[46]Pratica di manipolare le emozioni e il pensiero di un utente al fine di ottenere informazioni riservate o di indurlo ad agire in un certo modo.

[47] ART. 640-ter c.p.

[48] ART 494 c.p.

Infine, l'articolo 615-ter c.p. punisce l'accesso abusivo a un sistema informatico o telematico. Questo reato si configura quando una persona si introduce senza autorizzazione in un sistema protetto o vi si mantiene contro la volontà del legittimo titolare[49]. Le fattispecie legate al phishing, quindi, spaziano dalla frode all'accesso illecito e alla sostituzione di identità, coinvolgendo molteplici norme del Codice Penale. Lo smishing, una forma di Phishing che utilizza i servizi di messaggistica breve (SMS) o i messaggi di testo su telefoni cellulari e smartphone; il nome deriva dalla tecnologia di messaggistica di prova SMS (Short Message Service).

[49] ART 615-TER c.p.

CAPITOLO 3

IL DATA BREACH NELLA NORMATIVA CALIFORNIANA

Sommario: 3.1 La tutela giuridica dei dati personali negli Stati Uniti. 3.2 SB 1386: il primo approccio legislativo al Data Breach. 3.3 L'adozione del CCPA e CRPA. 3.4 il Data Breach nel contesto californiano e il caso Twilio.

3.1 La tutela giuridica dei dati personali negli Stati Uniti

Allo stato, come noto, non esiste una normativa statunitense onnicomprensiva in materia di protezione dei dati personali. I singoli Stati federati si sono talvolta dotati di proprie regole, le quali variano significativamente tra loro. Non si può inoltre parlare della presenza di uno standard minimo di cybersicurezza condiviso tra gli Stati, che appaiono dotarsi con maggiore frequenza di misure di reazione che di misure di prevenzione.[50]

La riflessione sull'esigenza di individuare alcuni principi federali di tutela dei dati personali viene avvertita negli Stati Uniti a partire dalla seconda metà del Novecento.

Nel 1973 il governo statunitense pubblica un rapporto indirizzato al Segretario del Dipartimento della Salute, Educazione e Benessere, intitolato "Records, Computers and the Right of the Citizens". Lo studio indirizza alcune problematiche che possono sorgere a seguito dall'utilizzo di computer per tenere traccia dei dati sanitari dei pazienti. Nel report viene consigliata da parte delle agenzie federali l'adozione di un Codice federale proposto[51]. Questo codice introduce per la prima volta le Fair information practices (FIP), una serie di principi che mira a tutelare gli utenti attraverso l'istituzione di c.d. requisiti di salvaguardia che definiscono gli standard minimi delle FIP[52]. Molte proposte presenti nel codice diverranno la base per lo sviluppo della giurisprudenza in materia di tutela dei dati personali.

Innanzitutto, troviamo una prima proposta di quello che diverrà il principio di trasparenza, il quale richiede alle agenzie governative di poter garantire all'individuo di conoscere quali

[50] MARCUS D., *The data breach dilemma,* 2018, p. 575.
[51] Ware, *Records*, *Computers and the Rights of Citizens,* 1973, p xxiii.
[52] Ibidem.

informazioni sue sono presenti in un registro e come vengono usate. Tale principio richiede altresì di fornire agli utenti un'informativa chiara e facilmente accessibile riguardo alla creazione, raccolta, utilizzo, trattamento, conservazione, gestione, condivisione e divulgazione delle PII[53]. Il coinvolgimento degli individui interessati nel processo di utilizzo delle PII rappresenta infatti un principio fondamentale per garantire la trasparenza e la fiducia nelle pratiche di gestione dei dati.

Secondo le FIPs, gli organi governativi devono adottare un approccio che consenta agli individui di partecipare attivamente al processo di gestione delle loro informazioni personali, oltre a doversi assicurare che i dati raccolti e trattati siano corretti ed attuali. Questo coinvolgimento non si limita al solo consenso iniziale, ma si estende anche alla capacità dell'individuo di controllare, monitorare e correggere i propri dati personali nei registri delle agenzie. Le agenzie governative devono quindi fornire meccanismi trasparenti per richiedere il consenso informato, consentendo agli individui di scegliere consapevolmente come e quando i loro dati saranno utilizzati[54]. Gli organi governativi devono anche porre adeguate misure di sicurezza in modo da tutelare le informazioni personali[55].

Questi oneri non solo promuovono la tutela della privacy degli individui, ma assicurano anche che le propagazioni del sistema pubblico rimangano responsabili nell'uso dei dati, mantenendo elevati standard di sicurezza e integrità nel trattamento delle informazioni. Infine, essi sono responsabili del rispetto di questi principi e dei requisiti applicabili in materia di privacy e devono monitorare, controllare e documentare adeguatamente la conformità[56].

Una tra le prime concretizzazioni di questi principi fu il Privacy Act del 1974: una legge che impone il rispetto delle FIPs alle attività di trattamento delle informazioni personali effettuate dalle agenzie governative federali. Appare altresì opportuno sottolineare che il Privacy Act del 1974 fornisce tutela agli interessati esclusivamente nei confronti degli organi governativi obbligati, lasciando comunque non regolamentato il settore dei privati. Il rapporto del 1973 proponeva linee guida, ma non aveva forza legale. Il *Privacy Act* del 1974 entra in effetto il 27 settembre 1975 ed ha reso i principi proposti dal report giuridicamente vincolanti per le agenzie federali.

[53] Ware, *Records*, *Computers and the Rights of Citizens,* cit. p. xxvi.
[54] Ware, *Records*, *Computers and the Rights of Citizens,* cit. p. xxvi.
[55] Ware, *Records*, *Computers and the Rights of Citizens,* cit. p. xxx.
[56] Ware, *Records*, *Computers and the Rights of Citizens,* cit. p. xxx.

Con questo atto viene aggiunto il principio di Data Minimization, il quale impone che vengano raccolti e utilizzati solo i dati strettamente necessari per raggiungere un obiettivo specifico. Di conseguenza, l'ente governativo deve garantire che l'uso dei dati personali sia proporzionato, evitando raccolte eccessive o non pertinenti rispetto alle finalità dichiarate. Questo rafforza la trasparenza e la protezione dei diritti individuali in materia di privacy[57]. Ulteriore elemento introdotto dal Privacy Act riguarda la c.d. accountability. Sulla base di tale principio, le agenzie e gli enti governativi devono garantire che le richieste degli individui siano gestite in modo tempestivo ed efficace, con procedure chiare per risolvere controversie o eventuali violazioni. Tale partecipazione attiva è essenziale per mantenere un livello elevato di conformità e per rafforzare la fiducia degli individui nei confronti delle organizzazioni che trattano i loro dati[58].Ad oggi, inoltre, alcune tipologie di consumatori – cosi quelli del settori finanziario - e gli individui interessati dal sistema sanitario ricevono una tutela particolarmente forte. Per esempio, il *Gramm-Leach-Bliley Act del 1999* impone a banche, assicurazioni e istituzioni finanziarie di stabilire standard per proteggere le informazioni finanziarie personali, garantendo la sicurezza e prevenendo accessi non autorizzati che potrebbero causare danni ai clienti[59]. Allo stesso modo, l'*Health Insurance Portability and Accountability Act* (HIPAA) del 1996 protegge le informazioni mediche dei consumatori, garantendo la sicurezza e riservatezza dei dati sanitari trattati fornitori di assistenza sanitaria, elaboratori di dati, farmacie e altre aziende che hanno bisogno di accedere alle informazioni mediche.[60]

Va infine segnalato che nell'aprile del 2014 era stato presentato al Senato americano un ambizioso progetti di legislazione federale in materia di tutela dei dati[61]. Gli obiettivi che questa proposta si proponeva erano diversi. Partendo con il fatto che la proposta era diretta a coinvolgere non solo le agenzie governative ma anche le istituzioni private, in apertura, vi era la proposta di inasprire le punizioni in caso di violazioni riguardanti la sicurezza e la privacy dei dati, soprattutto in caso di occultamento di una violazione di sicurezza riguardante dati sensibili[62]. Inoltre, veniva proposta una soglia oltre la quale coloro che mantengono e trattano i dati sensibili di più di 10'000 cittadini statunitensi dovevano conformarsi a requisiti legislativi

[57] Privacy Act sezione 552a, (e)(1).
[58] Privacy Act sezione 552a (d)(4).
[59] MARCUS D., *The data breach dilemma*, p. 576.
[60] ibidem
[61] Il senatore del Connecticut Richard Blumenthal ha presentato un disegno di legge intitolato "Legge sulla protezione dei dati personali e sulla responsabilità delle violazioni del 2014".
[62] Personal Data Protection and Breach Accountability Act of 2014, Title I.

di protezione dei dati, implementando un programma che garantisca la privacy, sicurezza e riservatezza, proteggendo da vulnerabilità prevedibili e accessi non autorizzati che possano causare rischi significativi per i consumatori[63]. Tuttavia, tale proposta di legge non è poi stata approvata, sicché gli Stati Uniti risultano tutt'ora sprovvisti di una regolamentazione generale federale in materia di privacy.

3.2 SB 1386: il primo approccio legislativo al Data Breach

Nella materia dei dati personali, lo Stato della California – dove d'altronde sono localizzate la gran parte delle multinazionali tech - si presenta come da sempre all'avanguardia nel panormana statunitense. Già nel 2003 la legge *SB 1386* – poi integrata nel codice civile californiano - segna una svolta cruciale nella protezione dei dati personali negli Stati Uniti. Innanzitutto, le disposizioni della legge si applicano non solo agli organi statali, ma hanno come destinatari (c.d. *covered parties*) anche chiunque - individuo o entità commerciale - operi in California per svolgere attività che comprendono il possesso o la licenza d'uso di dati informatici che contengono informazioni personali dei consumatori[64].

La neo-introdotta sezione 1789.82[65] del Codice Civile Californiano, infatti, afferma che quando si verifica un *data breach*, chi riveste la qualifica di covered party è tenuto a notificare qualsiasi violazione della sicurezza del sistema - in seguito alla scoperta o alla notifica della violazione della sicurezza dei dati - a qualsiasi residente della California le cui informazioni personali non criptate siano state acquisite, o si ritiene ragionevolmente che siano state acquisite, da una persona non autorizzata. Tale notifica agli interessati deve avvenire nel più breve tempo possibile e senza ritardi irragionevoli. La legge contiene anche un modello con le eventuali informazioni da fornire, il quale va rispettato per la notifica di data breach.[66]. Le disposizioni si applicano anche ai destinatari che non siano titolari dei dati, ma per qualsiasi ragione ne mantengano una copia.

Il bill del 2003 contiene anche una prima definizione dei dati personali che sono tutelati da data breach. In particolare, per "informazioni personali" si intendono: "il nome o l'iniziale del nome e il cognome di una persona in combinazione con uno o più dei seguenti elementi di dati, quando il nome o gli elementi di dati non sono criptati: numero di previdenza sociale. Numero

[63] Personal Data Protection and Breach Accountability Act of 2014, cit. Title II
[64] SB 1386, section 2(a).
[65] California Civil Code, section 1798.82.
[66] ibidem

di patente di guida o carta d'identità della California, il numero di carta d'identità della California, il numero di conto corrente, numero di carta di credito o di debito, in combinazione con qualsiasi codice di sicurezza, codice di accesso o password che consenta l'accesso al conto finanziario di un individuo"[67].

3.3 L'adozione del CCPA e CRPA

Nel secondo decennio degli anni 2000, l'attivista Alastair Mactaggart[68] porta alla luce la necessità di adottare nel contesto californiano una tutela comprensiva dei consumatori di servizi online. [69]. Come riportato dal "*The New York Times Magazine* In particolare, Mactaggart sosteneva che "le regole che esistevano erano in gran parte stabilite dalle stesse aziende, nelle proprie informative sulla privacy e negli accordi con gli utenti finali, documenti che la maggior parte delle persone non legge affatto. [70]".

Inizialmente la proposta incontrò una forte opposizione, finché non avvenne lo scandalo di Cambridge Analytica, società di analisi politica appartenuta alla piattaforma Facebook, al tempo con sede nella Silicon Valley. L'attività principale della società era quella di raccogliere immense quantità di dati per profilare gli utenti, ovvero crearne una identità comportamentale, per creare uno spettro degli utenti presenti in rete[71]. A seguito di segnalazioni riguardanti l'acquisizione e la conservazione illecita di dati personali degli utenti di Facebook, si è innescata un'ondata di inchieste giornalistiche, che hanno portato alla luce come oltre 50 milioni di utenti fossero stati vittime di una massiccia raccolta non autorizzata delle loro informazioni private.

Il caso Cambridge Analytica ha mobilitato la coscienza pubblica riguardo alla necessità di una tutela efficace dei diritti alla privacy. Questo scandalo ha esposto vulnerabilità significative nelle pratiche di gestione dei dati personali, spingendo i cittadini a richiedere maggiore protezione e trasparenza. In un contesto in cui il governo californiano si trovava a dover gestire

---

[67] SB 1386, SECTION 1, (e).

[68] Mactaggart viene oggi considerato il co-autore di questa legislazione, non solo per aver avviato il processo legislativo, ma anche per aver sostenuto la sua approvazione nonostante la forte opposizione delle grandi imprese tecnologiche. Fonte: BUKATY P., *The California Consumer Privacy Act (CCPA,),* pp. 9,10,11.

[69] BUKATY P., *The California Consumer Privacy Act (CCPA,),* p. 10.

[70] CONFESSORE N., The Unlikely Activists Who Took On Silicon Valley — and Won, «The New York Times Magazine», 14 agosto 2018, <https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html>, (ultimo accesso: 19/9/2024).

[71] DALLA PIAZZA S., *Lo scandalo di Cambridge Analytica, legato all'utilizzo dei dati personali ottenuti illecitamente da Facebook* «DirittoConsenso», 21 dicembre 2021 <https://www.dirittoconsenso.it/2021/12/21/il-caso-cambridge-analytica/>, (ultimo accesso: 25 settembre 2024)».

questa crescente esigenza popolare e, allo stesso tempo, il potere delle grandi aziende tecnologiche come Google, Facebook e Twilio, c'era un forte desiderio di evitare un referendum[72]. Infatti, ciò avrebbe comportato l'adozione di una legislazione meno flessibile, poiché qualsiasi modifica futura sarebbe stata possibile solo tramite il voto degli elettori, limitando le possibilità di adattamento della legge alle esigenze delle aziende e dei cittadini, andando a sfavore delle numerose aziende BigTech californiane[73].

Queste ragioni sono le ritenute uno dei principali fattori di influenza sull'approvazione della proposta di Mactaggart, che ha preso le vesti del c.d. CCPA (California Consumer Privacy Act) del 2018.[74] Il CCPA viene approvato con l'intenzione di rafforzare i diritti dei consumatori californiani, dando loro un maggiore controllo sui propri dati personali e garantendo che le aziende rispettino standard più elevati di trasparenza e sicurezza. Esso entra in vigore il 1° gennaio 2020 ed è la prima legislazione statale negli Stati Uniti a garantire diritti significativi ai consumatori in materia di protezione dei dati.

Il 4 novembre 2020 viene approvato il California Privacy Rights Act (CPRA), entrato in vigore il 1° gennaio 2023. Il nuovo atto amplia i diritti azionabili dai consumatori, includendo il diritto alla correzione e il diritto alla limitazione dell'uso dei dati sensibili. In particolare, l'emendato articolo 1789.106 del codice civile californiano[75] conferisce ai consumatori il diritto di correggere informazioni personali inaccurate, consentendo loro di richiedere alle aziende di rettificare eventuali errori nei dati che li riguardano, tenendo conto anche della natura e delle finalità del trattamento. Inoltre, l'articolo 1789.121 dello stesso codice introduce il diritto di limitare l'uso e la divulgazione delle informazioni personali sensibili. I consumatori possono chiedere alle aziende di limitare l'uso delle informazioni sensibili solo a ciò che è strettamente necessario per fornire i servizi richiesti o per adempiere a finalità ragionevolmente previste[76].

In particolare, il *California Privacy Right Act* rivede la sezione relativa alle definizioni ed introduce una più chiara definizione di "business". Ai sensi della sezione *1798.140 (d) del codice civile californiano,* per business si intendono tutte quelle persone giuridiche tra cui molteplici forme di aziende come società a responsabilità limitata , corporazioni, associazioni

[72]*Guardians of Privacy: Tracing the CCPA's Historic Journey*, «Keitaro», 23 ottobre 2023, < https://blog.keitaro.io/en/guardians-of-privacy-tracing-the-ccpas-historic-journey/>, (ultimo accesso: 10.10.2024).

[73] Costituzione Californiana, articolo 2 sezione 10.

[74] BUKATY P., *The California Consumer Privacy Act (CCPA,),* p. 11.

[75] California Civil Code, section 1789.106 (a).

[76]California Civil Code, section 1798.121 (a).

e società per azioni che operano a scopo di lucro o di garantire benefici patrimoniali per i propri soci e raccolgono informazioni personali dei consumatorie che determinino, da sole o congiuntamente ad altri, le finalità e i mezzi del trattamento delle informazioni personali dei consumatori[77].

È altresì essenziale che queste aziende operino in California e che soddisfino uno o più dei seguenti criteri: alla data del 1º gennaio, abbiano avuto un fatturato lordo annuo superiore a $25.000.000 di dollari nell'anno precedente, che acquistino, vendano o condividano, da sole o in combinazione, annualmente le informazioni personali di 100.000 o più consumatori o nuclei familiari ed infine che ottengano il 50 percento o più dei propri ricavi annui dalla vendita o condivisione di informazioni personali dei consumatori[78].

La sezione 1789.140 punto (v)(1) del Codice Californiano amplia la definizione del termine "informazioni personali". Il termine risulta molto vasto: qualsiasi tipo di informazione che identifichi, si colleghi o che possa essere condotta al soggetto risulta essere catalogato come informazione personale. Inoltre, vengono considerate tali anche le informazioni indirette[79].

Con il CPRA vengono introdotte le informazioni personali sensibili che comprendono informazioni biometriche, geolocalizzazione precisa e origine razziale ed etnica[80].

Infine, il CPRA ha introdotto la California Privacy Protection Agency (CPPA), autorità incaricata di far rispettare le disposizioni della legge, e ha arricchito la tutela dei consumatori attraverso la regolamentazione di nuovi aspetti, come il trattamento delle informazioni personali sensibili e la condivisione dei dati per scopi pubblicitari[81].

Di conseguenza, la normativa complessiva risultante in materia di privacy in California è oggi parte del Codice civile californiano (Civil Code of the State of California), al Titolo 1.81.5. (Sezioni 1798.100 - 1798.199.100), rappresentando un passo significativo verso una protezione più robusta della privacy in un contesto sempre più digitalizzato.

---

[77] California Civil Code - Section 1789.140(d).

[78] California Civil Code cit. (d) (1-2-3).

[79] California Civil Code cit. (v) (1)».

[80] *CCPA vs. CPRA – What has changed?,* «OneTrust», 10 novembre 2020, <https://www.onetrust.com/blog/ccpa-vs-cpra-what-has-changed/> (ultimo accesso: 24 settembre 2024)»

[81] Burke, «Examining the Difference Between CPRA and CCPA Regulations, 15 maggio 2023, <https://woodruffsawyer.com/insights/cpra-vs-ccpa-regulations>.».

3.4 Il Data Breach nel contesto californiano e il caso Twilio.

Per ciò che concerne la gestione dell'avvenuto data breach, la legislazione Californiana si avvale tutt'oggi dei contenuti del SB 1386 per quanto attiene all'attività di notifica. L'articolo 1789.82 codice civile californiano - discusso in precedenza[82] - rimane la fonte di riferimento.

Per quanto attiene alle attività di prevenzione, l'articolo 1798.100 sezione (e) del codice civile californiano stabilisce che ogni azienda che soddisfi i requisiti presentati ai sensi dell'articolo 1789.140 (d) e che raccoglie informazioni personali deve adottare procedure e pratiche di sicurezza ragionevoli, adeguate alla natura delle informazioni, per proteggerle da accessi, distruzione, uso, modifica o divulgazione non autorizzati o illegali. Nell'articolo non vengono inserite raccomandazioni o obblighi specifichi da ottemperare per garantire un adeguato livello di sicurezza.

La natura, le modalità e l'entità del breach subito da Twilio nell'estate del 2024 – il quale, come noto, ha coinvolto anche il servizio di autenticazione a due fattori Authy – permettono di dubitare che l'azienda si sia conformata a tali obblighi preventivi. L'aggiornamento dell'applicazione è stato effettuato solamente a posteriori del data breach, permettendo al gruppo hacker di appropriarsi dei numeri di telefono indicizzati agli account personali. In un attacco subito ad Agosto 2022, Twilio è stato colpito con un attacco di ingegneria sociale che ha sottratto l'account di un dipendente, permettendo l'accesso ai dati personali di alcuni user.

Nel caso in cui si verifichi un evento di sicurezza, l'organizzazione deve essere pronta a rispondere non solo all'incidente stesso. Idealmente, tutto il personale di un'organizzazione dovrebbe avere una conoscenza generale dei problemi di sicurezza delle informazioni e dei sintomi di un possibile attacco o evento. Per questo motivo, la formazione di sensibilizzazione è fondamentale per tutto il personale: tutti nell'organizzazione svolgono un ruolo nella gestione della sicurezza delle informazioni.

Sotto il profilo della responsabilità civile dell'azienda, va altresì considerato che il CCPA ha introdotto la possibilità per i consumatori di avviare un'azione legale contro le aziende che non adottano misure di sicurezza adeguate a proteggere i dati personali da accessi non autorizzati. In caso di violazione che comporti la divulgazione non autorizzata di informazioni personali, il consumatore ha diritto a un risarcimento fino a $750 per incidente, o a un risarcimento maggiore se i danni effettivi superano tale somma[83].Con riferimento a tali profili, tuttavia, non

[82] cfr. 3.2

[83] California Civil Code - TITLE 1.81.5. California Consumer Privacy Act of 2018 - Section 1789.150.

si può ignorare come, nel contesto statunitense, si arrivi spesso alla risoluzione alternativa delle controversie, a mezzo di patteggiamenti, i cui termini rimangono spesso privati[84].

[84] Casi come quelli di T-Mobile US e Dental expression sono rilevanti. Entrambi correlati ad incidenti di sicurezza dei dati personali, hanno risolto patteggiando. Il primo ha versato $31,5 milioni, il secondo $2,7. Fonti: LYONS J., *T-Mobile US to cough up $31.5M after that long string of security SNAFUs,* «The Register», 30 settembre 2024, <https://www.theregister.com/2024/09/30/tmobile_data_breaches_settlement/>, (ultimo accesso: 10.10.2024). ; *$2.7M Great Expressions Data Breach Settlement: Your Ultimate Guide to Claiming Your Share* «LawInc», 9 ottobre 2024, <https://www.lawinc.com/great-expressions-data-breach-settlement-guide>, (ultimo accesso: 10.10.2024).

CAPITOLO IV

IL DATA BREACH NEL CONTESTO EUROPEO

Sommario: 4.1 Le disposizioni del GDPR e le linee guida dell'European Data Protection Board (EDPB). 4.1.1 Articolo 32 GDPR: dovere di imporre adeguate misure di sicurezza. 4.1.2 Articoli 33 e 34 GDPR: dovere di notifica e comunicazione. 4.1.3 Articolo 82 GDPR: diritto alla compensazione. 4.2 analisi del caso Twilio secondo la normativa europea. 4.2.1 Adeguatezza delle misure di sicurezza e profili di prevenzione. 4.2.2. Profili di responsabilità nei confronti degli interessati. 4.2.3 Art. 33 e 34 GDPR: notifica della violazione e comunicazione

4.1 Le disposizioni del GDPR e le linee guida dell'European Data Protection Board (EDPB)

All' interno dell'Unione Europea, come noto, il Regolamento Generale sulla Protezione dei Dati rappresenta un'estesa normativa che mira a garantire una protezione uniforme dei dati personali all'interno dell'UE, rafforzando i diritti dei cittadini e imponendo obblighi rigorosi alle aziende.

Il GDPR[85] (Regolamento Generale sulla Protezione dei Dati) stabilisce le norme per la protezione delle persone fisiche in relazione al trattamento dei dati personali e ne regola anche la libera circolazione. Il Regolamento tutela i diritti e le libertà fondamentali degli individui, in particolare il loro diritto alla protezione dei dati personali. Si applica al trattamento dei dati personali sia effettuato tramite mezzi automatizzati che non automatizzati, purché facciano parte di un sistema di archiviazione o siano destinati a farne parte. Il GDPR si applica al

[85] Le radici di quest'opera risalgono al 1995, quando il 24 Ottobre viene introdotta la Direttiva 95/46/CE, che stabilisce regole comuni a livello europeo per garantire la protezione dei dati personali e la libera circolazione di tali dati all'interno dell'Unione Europea. Il 25 gennaio 2012 la commissione Europea, consapevole del contesto oramai ben diverso e digitalizzato, propone che l'ormai arretrata direttiva venga sottoposta ad una modernizzazione completa. Successivamente, il 12 marzo 2014 si mostra estremamente favorevole all'adozione del progetto fino a che, il 24 maggio 2016 il GDPR viene adottato ed infine applicato il 25 maggio 2018[85].

trattamento dei dati nell'ambito delle attività di un titolare o responsabile del trattamento all'interno dell'Unione Europea, indipendentemente dal luogo in cui avviene il trattamento. Inoltre, si estende al trattamento di dati personali di soggetti nell'UE da parte di titolari o responsabili non stabiliti nell'UE, se tali attività riguardano l'offerta di beni o servizi a tali soggetti o il monitoraggio del loro comportamento all'interno dell'Unione.

Dal 68 al 76esimo articolo del GDPR viene dato corpo e funzioni del Comitato Europeo per la protezione dei Dati (EDPB)[86]. Lo scopo principale della EDPB è quello di garantire che le norme sulla protezione dei dati personali vengano applicate in maniera omogenea nel contesto europeo. Inoltre, coordina le attività delle autorità nazionali per la protezione dei dati, fornisce linee guida e raccomandazioni su come interpretare il GDPR e risolve i conflitti tra le diverse autorità[87].

Il 28 marzo 2023 l'EDPB ha adottato le "linee guida 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del GDPR". Queste ultime forniscono indicazioni dettagliate sulla notifica delle violazioni dei dati personali ai sensi del GDPR, chiariscono quando una violazione deve essere notificata alle autorità di controllo e alle persone interessate, come valutare il rischio associato a una violazione, e quali informazioni devono essere incluse nelle notifiche. Il documento mira a uniformare l'approccio alla gestione dei data breach e garantire che le aziende rispettino i requisiti di sicurezza e notifica

4.1.1 Articolo 32 GDPR: dovere di imporre adeguate misure di sicurezza

L'articolo 32 del GDPR affronta il tema della sicurezza che il controllore e colui che processa i dati devono garantire. L'obbligo sussiste nell'assicurare un livello di sicurezza adeguato al rischio, implementando misure tecniche e organizzative come la cifratura ed un'elevata resilienza dei sistemi. Le misure di sicurezza dovrebbero inoltre garantire una continua confidenzialità, disponibilità ed integrità dei sistemi e servizi che processano le informazioni personali. Nel valutare il livello di sicurezza adeguato si tiene conto in particolare dei rischi che il trattamento comporta, in particolare la distruzione accidentale o illecita, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o altrimenti trattati[88].

[86] CNIL, «The European Data Protection Board (EDPB)».CNIL, «The European Data Protection Board (EDPB)».
[87] «Presidenza dell'EDPB, < https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_it>, (ultimo accesso: 6 ottobre 2024)».
[88] EU GDPR - Article 32.

4.1.2 Articoli 33 e 34 GDPR: dovere di notifica e comunicazione

Gli articoli 33 e 34 riguardano l'obbligo di comunicazione che deve essere adempiuto da parte dei processori dei dati quando si verifica una fuga di dati. l'articolo 33 afferma che In caso di violazione dei dati personali, il responsabile del trattamento notifica senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, la violazione dei dati personali all'autorità di controllo competente, a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche[89].

L'articolo 34 prosegue, affermando che se il breach presenta alti rischi per la libertà e i diritti della parte lesa, il titolare del trattamento deve comunicare la violazione dei dati personali all'interessato senza ingiustificato ritardo.

La comunicazione, sia che venga fatta all'autorità di controllo competente, che alle persone naturali deve descrivere in modo chiaro e comprensibile la natura della violazione ed includere: la descrizione della natura della violazione, specificando, le categorie e il numero approssimativo di soggetti coinvolti e di registri di dati interessati. Inoltre, deve spiegare le probabili conseguenze della violazione e le misure adottate o previste per affrontarla, incluse eventuali azioni per mitigare gli effetti negativi.

Tra i requisiti più rilevanti in materia di data breach, il GDPR include l'adozione per i responsabili del trattamento di misure di sicurezza efficaci per prevenire accessi non autorizzati, l'obbligo di notificare tempestivamente le violazioni alle autorità competenti e, in alcuni casi, agli individui coinvolti. Inoltre, prevede la possibilità di risarcimento per i soggetti danneggiati da un uso improprio o non sicuro dei loro dati personali, rafforzando il diritto alla tutela della privacy[90].

4.1.3 Articolo 82 GDPR: diritto alla compensazione

L'articolo 82 garantisce la possibilità di ottenere un risarcimento per chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento da parte del responsabile del trattamento. Il considerando (146) aggiunge che il titolare del trattamento

[89] EU GDPR - Article 33.
[90] EU GDPR - Article 34.

dovrebbe essere esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile[91].

4.2 Analisi del caso Twilio secondo la normativa europea

4.2.1 Adeguatezza delle misure di sicurezza e profili di prevenzione

Le Linee guida 9/2022 dell'EDPB enfatizzano l'importanza di attuare misure preventive adeguate a proteggere i dati personali. L'articolo 32 del GDPR stabilisce che titolari e responsabili del trattamento devono garantire un livello di sicurezza adeguato al rischio, implementando misure tecniche e organizzative come la cifratura e la resilienza dei sistemi[92].
La giurisprudenza della Corte di Giustizia dell'Unione europea, d'altronde, sostiene che la semplice esistenza di una "violazione dei dati personali" non implica automaticamente che le misure tecniche e organizzative adottate dal titolare del trattamento non siano adeguate[93]. Il giudice deve valutare concretamente sia il contenuto delle misure adottate sia la loro applicazione e gli effetti pratici.
Quanto si può rilevare, con riferimento al caso di Twilio è che l'azienda ha aggiornato Authy solo dopo il breach, evidenziando una mancanza nelle misure di sicurezza preventive che avrebbero potuto evitare l'incidente. Il data breach di agosto 2022 è stato un attacco di ingegneria sociale che ha permesso agli hacker di rubare le credenziali di un impiegato. Gli aggressori hanno poi utilizzato le credenziali rubate per accedere ad alcuni sistemi interni, dove hanno potuto accedere ad alcuni dati dei clienti. Gli attacchi di ingegneria sociale utilizzati in questo caso risultati efficaci mostrano come sia necessario implementare una formazione più solida e consolidata nei dipendenti dell'azienda[94].
In particolare, da parte di Twilio, vi è stata carenza di criptazione dei dati. Gli hacker hanno avuto accesso ai numeri di telefono per via di un punto di accesso non autenticato, nel quale

[91] EU GDPR -Article 82.
[92] EU GDPR - Article 32 (1).
[93] Causa C-340/21, *VB contro Natsionalna agentsia za prihodite*. La corte si èpronunciata sulle condizioni per il risarcimento dei danni immateriali derivanti dalla pubblicazione di dati personali su Internet a seguito di un attacco hacker, costituente una violazione di dati personali ai sensi del Regolamento (UE) 2016/679. La sentenza è reperibile: <https://curia.europa.eu/juris/document/document.jsf;jsessionid=DDCCF5FAFBC93C875584F8B7C3DB165F?text=&docid=272977&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=702058>
[94] Aleroud e Zhou, «Phishing environments, techniques, and countermeasures: A survey, pp 171.».

non hanno dovuto porre ulteriore sforzo per estrarre i numeri di telefono, esponendo gli utenti di Authy a possibili attacchi di Phishing e Smishing.

Il punto 2 dell'articolo 32 GDPR sancisce d'altronde che, nel determinare l'adeguato livello di sicurezza per i dati personali, si deve prestare particolare attenzione ai rischi legati al trattamento[95]. Questi rischi includono eventi come la distruzione, perdita, modifica, divulgazione o accesso non autorizzato - sia che si verifichino accidentalmente che illegalmente. - possono interessare dati trasmessi, conservati o altrimenti trattati e devono essere affrontati con misure tecniche e organizzative idonee a garantire la sicurezza delle informazioni.

Twilio, come piattaforma di comunicazione cloud, gestisce volumi enormi di dati degli utenti, tra cui SMS, chiamate vocali e altre interazioni digitali. Questo comporta la gestione continua di informazioni sensibili, comprese quelle personali e finanziarie, spesso utilizzate per autenticazione e transazioni. Per garantire la protezione di tali dati, Twilio deve adottare rigorosi sistemi di sicurezza. Data la sua natura di piattaforma di comunicazione globale, è essenziale implementare soluzioni proattive per prevenire accessi non autorizzati o violazioni di sicurezza, salvaguardando così le informazioni degli utenti e garantendo conformità normativa. Facendo un paragone con Microsoft, piattaforma che tratta anch'essa una quantità ingente di dati, quest'ultima ha adottato l'architettura Zero Trust per aumentare il suo grado di invulnerabilità agli attacchi informatici. L'Architettura Zero Trust (ZTA) non è un'unica soluzione ma un insieme di principi progettuali volti a rafforzare la sicurezza aziendale e industriale. Zero Trust si basa sull'idea di non fidarsi mai di un'entità fino a quando non è stata autenticata e ha dimostrato di avere diritto all'accesso. L'autenticazione è un elemento cruciale per una corretta implementazione dell'Architettura Zero Trust (ZTA), poiché determina se l'utente o il servizio richiedente è autorizzato e a quale risorsa può accedere. Essa consente di identificare utenti interni, esterni e servizi di terze parti, garantendo che l'accesso sia gestito secondo le politiche definite[96].

[95] EU GDPR - Article 32. (2).

[96]IGGBOM J., *Zero Trust Architecture is a Token-Based Architecture, 23 settembre* 2020, <https://curity.io/resources/learn/zero-trust-overview/>, (ultimo accesso: 6 ottobre 2024)».

4.2.2 Profili di responsabilità nei confronti degli interessati

Ai sensi dell'articolo 82 del GDPR, come noto, gli interessati dal trattamento hanno il diritto di ottenere un risarcimento per i danni subiti, materiali o immateriali, derivanti da una violazione del regolamento sulla protezione dei dati. Il titolare o il responsabile del trattamento è ritenuto responsabile, a meno che non dimostri che l'evento che ha causato il danno non dipenda da una sua responsabilità[97].Riguardo ciò, la Corte di giustizia Europea ha affermato che spetta a ciascuno Stato membro stabilire, all'interno del proprio ordinamento giuridico, i metodi di prova ammessi e il loro valore legale, compresi i mezzi istruttori che i tribunali nazionali possono o devono disporre. Questo processo è finalizzato a valutare se il titolare del trattamento dei dati personali abbia adottato misure adeguate in conformità al regolamento, garantendo il rispetto dei principi di equivalenza ed efficacia previsti dal diritto dell'Unione[98] Inoltre, il titolare deve essere in grado di dimostrare l'adeguatezza delle misure tecniche e organizzative adottate in conformità all'articolo 32, che impone l'adozione di misure di sicurezza adeguate al rischio.

L'articolo 83 del GDPR completa queste disposizioni stabilendo criteri per l'imposizione di sanzioni amministrative pecuniarie. Le sanzioni possono essere inflitte per violazioni degli obblighi previsti dal GDPR, inclusi quelli relativi alla sicurezza dei dati (art. 32) e al risarcimento (art. 82). Le multe possono raggiungere il 4% del fatturato annuo globale dell'azienda o fino a 20 milioni di euro, a seconda di quale somma sia maggiore. Le sanzioni sono calcolate considerando vari fattori, tra cui la natura, la gravità e la durata della violazione, il grado di responsabilità del titolare, e le misure adottate per mitigare i danni[99].

4.2.3 Art. 33 e 34 GDPR: notifica della violazione e comunicazione

Gli articoli 33 e 34 del GDPR trattano della notifica e comunicazione della violazione dei dati personali all'autorità di controllo e ai diretti interessati. L'articolo 33 sostiene che quando si verifica una violazione dei dati personali, il titolare del trattamento deve notificare l'accaduto all'autorità di controllo competente entro 72 ore dal momento in cui ne viene a conoscenza[100]. Se la notifica non viene fatta entro questo termine, devono essere fornite le ragioni del ritardo[101]. La notifica deve includere dettagli come la natura della violazione, le categorie di dati

[97] EU GDPR -Article 82.
[98] Causa C-340/21, *VB contro Natsionalna agentsia za prihodite*
[99] EU GDPR - Article 83.
[100] EU GDPR - Article 33 (1).
[101] Ivi (2).

personali compromessi, il numero di soggetti coinvolti, le conseguenze della violazione e le misure adottate per mitigare gli effetti[102]. L'articolo 34 invece tratta una situazione di violazione dei dati personali che va a ledere la libertà e i diritti della persona fisica. In tal caso, gli interessati vanno informati senza ritardo e informati riguardo alle conseguenze derivate dalla violazione[103].

Sotto questo punto di vista Twilio ha garantito un'informazione efficiente. Nel breach del primo luglio 2024, il giorno stesso ha rilasciato uno *statement* riguardo la causa della violazione - dovuta all'accesso all'endpoint API non autenticato - ed ha informato anche riguardo le conseguenze, in questo caso probabili attacchi Phishing e Smishing. Ha aggiunto inoltre che le precedenti falle di sicurezza sono state sistemate[104]. Ciò è in linea con quanto avvenuto anche in occasione del breach di Agosto 2022, per il quale l'azienda aveva rilasciato sul sito uno *statement* in cui spiegava in maniera esaustiva l'accaduto e avvisava gli utenti delle possibili minacce[105].

[102] Ivi. (3).
[103] EU GDPR - Article 34 (1).
[104] «Security Alert: Update to the Authy Android (v25.1.0) and iOS App (v26.1.0), < https://www.twilio.com/en-us/changelog?page=5>, (ultimo accesso: 6 ottobre 2024)».
[105] «Incident Report: Employee and Customer Account Compromise, 7 agosto 2022, < https://www.twilio.com/en-us/blog/august-2022-social-engineering-attack>, (ultimo accesso: 6 ottobre 2024)».

CONCLUSIONI

Nel contesto del caso Twilio, possiamo notare come l'azienda abbia dimostrato conformità a diverse disposizioni normative, sia secondo il diritto californiano che europeo. La CCPA e il GDPR condividono l'obiettivo di garantire una protezione adeguata dei dati personali, e in entrambi i casi è stato rispettato l'obbligo di notifica. Secondo il GDPR, l'articolo 33 richiede che le organizzazioni notifichino alle autorità competenti una violazione dei dati entro 72 ore dal momento in cui ne sono venute a conoscenza. Analogamente, la CCPA prevede che le aziende informino tempestivamente sia i consumatori che il California Attorney General in caso di violazioni che coinvolgano un numero rilevante di utenti.

Twilio ha adempiuto a questi obblighi, notificando correttamente la violazione alle parti interessate, evidenziando la conformità alle normative in termini di trasparenza e comunicazione. Tuttavia, emergono delle criticità in merito alla prevenzione. Sebbene la CCPA e il GDPR impongano alle aziende di adottare misure di sicurezza adeguate per proteggere i dati personali – come stabilito dall'articolo 32 del GDPR e dalla sezione 1798.100 del Codice Civile Californiano – Twilio ha aggiornato le sue misure di sicurezza solo dopo che l'incidente si è verificato. Questo solleva dubbi sull'efficacia delle misure preventive messe in atto dall'azienda prima dell'attacco, in quanto non risultano essere presenti normative di prevenzione che forniscano un quadro chiaro e solido alle quali le aziende possono conformarsi.

Pertanto, mentre dal punto di vista della conformità alle norme sulla notifica Twilio ha agito correttamente, la gestione delle misure preventive appare insufficiente sia sotto la prospettiva californiana che europea. Questo caso mette in luce l'importanza di una sicurezza proattiva e di politiche di prevenzione ben strutturate, conformi sia alla CCPA che al GDPR, che impongono alle aziende di garantire che i dati siano sempre protetti attraverso misure tecniche e organizzative appropriate.

L'introduzione di tecnologie come l'intelligenza artificiale (AI) e il machine learning (ML) ha rivoluzionato il campo della sicurezza informatica, offrendo nuove soluzioni per prevenire e rispondere ai data breach. Questi strumenti permettono di analizzare grandi quantità di dati, individuare schemi anomali e reagire rapidamente a minacce potenziali. In particolare, il Deep Learning, un sottocampo del machine learning, utilizza reti neurali profonde per rilevare minacce sofisticate, adattandosi continuamente a nuovi modelli di attacco.

Nel caso di Twilio, l'adozione di tali tecnologie avrebbe potuto migliorare le difese preventive e la risposta agli incidenti. Questo evento sottolinea l'importanza di un approccio integrato che combini tecnologia avanzata, governance e responsabilità legale, per garantire la protezione dei dati personali in un contesto digitale sempre più complesso.

BIBLIOGRAFIA

A. Eloksari, Eisya. *Tokopedia data breach exposes vulnerability of personal data*, «The Jakarta Post» .

ALEROUD A., ZHOU L., *Phishing environments, techniques, and countermeasures: A survey*, *Computers & Security* 68 (2017).

AMAZON, *Qual è la differenza tra front-end e back-end nello sviluppo delle applicazioni?*, « Amazon Web Services».

BIEHL M., *API architecture*. Vol. 2. API-University Press, 2015.

BUKATY P., *The California Consumer Privacy Act (CCPA): An implementation guide*, 2019.

BURKE D., *Examining the Difference Between CPRA and CCPA Regulations*, «Woodruff Sawyer», 15 maggio 2023.

CADAMURO E., *Slide n. 14 del corso di diritto penale, robotica e intelligenza artificiale*, 2024.

California Civil Code - TITLE 1.81.5. California Consumer Privacy Act of 2018 - Section 1789.150.

*CCPA vs. CPRA – What has changed?, «*OneTrust*»,* 10 novembre 2020.

CHNG S., HAN Y.L., KUMAR Y., YAU D., *Hacker Types, Motivations and Strategies: A Comprehensive Framework*, 2022.

Cloud Computing: A Top-Down View, «The Wall Street Journal».

CNIL. *The European Data Protection Board (EDPB)*.

CONFESSORE N., *The Unlikely Activists Who Took On Silicon Valley — and Won*, «The New York Times», 14 agosto 2018.

DALLA PIAZZA S., *Lo scandalo di Cambridge Analytica, legato all'utilizzo dei dati personali ottenuti illecitamente da Facebook*, «DirittoConsenso».

Differenza tra licenza cloud ad abbonamento, pay-as-you-go, pay-by-instances e BYOL., «Informatica e Ingegneria Online».

GADDE, Secure Data Sharing in Cloud Computing: A Comprehensive Survey of Two-Factor Authentication and Cryptographic Solutions, 2023.

DEBIN G., GUAN X., e XIAOFENG L., *Information and Communications Security. Part 1*, 2021.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. *Linee guida per la gestione delle violazioni di dati personali e la loro eventuale comunicazione all'Autorità e ai soggetti interessati*.

GOOGLE, *What is cloud architecture?*, «Google Cloud»,

Guardians of Privacy: Tracing the CCPA's Historic Journey, «Keitaro Blog».

European Data Protection Board, *Guidelines 9/2022 on personal data breach notification under GDPR*, 2023.

HIETALA J., KONTIO J., JOKINEN J.P., PYYSIAINEN J., *Challenges of software product companies: results of a national survey in finland*, *2004*.

HPE. «Architettura cloud», s.d. https://www.hpe.com/it/it/what-is/cloud-architecture.html, « Hewlett Packard Enterprise».

HUAWEI TECHNOLOGIES, Ltd, *Cloud Computing Technology*. Singapore: Springer Nature Singapore, 2023.

What is an API endpoint? , «IBM»..

IKEDA S., *Twilio Data Breach That Exposed 33 Million Authy Phone Numbers Caused by Unsecured API Endpoint*, «CPO Magazine», 8 luglio 2024.

LARDINOIS F., T*wilio Acquires Two-Factor Authentication Service Authy*, «TechCrunch».

MACEIRAS M., KAVOUS S. N., GAEL B. BENOIT G., CHERUBINI M., HUMBERT M., e HUGUENIN K., *Know Their Customers: An Empirical Study of Online Account Enumeration Attacks*. *ACM Transactions on the Web* 18, fasc. 3 (31 agosto 2024)

MARCUS D., *The data breach dilemma*, 2018

MONTALBANO E., *Report: Microsoft's GitHub Account Gets Hacked*, «ThreatPost».

MOSCO V., *To the Cloud: Big Data in a Turbulent World*, 2016.

OMENA J., CURRIE M., *Collecting Data Using APIs Part 1: How to Understand APIs and Navigating API Documentation*, 2022.

PELTIER T.R., *Social engineering: Concepts and solutions*, 2006.

Personal Data Protection and Breach Accountability Act of 2014.

PRASAD S. T., *Ethical hacking and types of hackers*, 2014

EUROPEAN DATA PROTECTION BOARD, *Presidenza dell'EDPB*.

SATYANARAYANA S., *Cloud computing: SAAS*, 2012.

STAMENKOV G., *Genealogy of the Fair Information Practice Principles*, 2023.

SUBASHINI S., KAVITHA V., *A Survey on Security Issues in Service Delivery Models of Cloud Computing*, 2011.

Too Good To Go security data breach Jan 1-May 15, 2024, «Reddit», 2024.

TSAI W., XIN S., JANAKA B., *Service-Oriented Cloud Computing Architecture*, 2010.

TWILIO, *Security Alert: Update to the Authy Android (v25.1.0) and iOS App (v26.1.0)*, 1 luglio 2024

UNITED STATES SECURITIES AND EXCHANGE COMMISSION, 26 maggio 2016.

WARE W., *Records, Computers and the Rights of Citizens - Transmittal Letter to Secretary*, 30 giugno 1973.

YASRAB R., *Platform-as-a-Service (PaaS): The Next Hype of Cloud Computing*., 2018.

IGGBOM J., *Zero Trust Architecture is a Token-Based Architecture*, 23 settembre 2020.

SITOGRAFIA

https://www.thejakartapost.com/news/2020/05/04/tokopedia-data-breach-exposes-vulnerability-of-personal-data.html.

https://aws.amazon.com/it/compare/the-difference-between-frontend-and-backend/.

https://woodruffsawyer.com/insights/cpra-vs-ccpa-regulations

https://www.onetrust.com/blog/ccpa-vs-cpra-what-has-changed/.

https://www.dirittoconsenso.it/2021/12/21/il-caso-cambridge-analytica/.

https://cloud.google.com/learn/what-is-cloud-architecture?hl=it.

https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html.

https://vitolavecchia.altervista.org/differenza-tra-licenza-cloud-ad-abbonamento-pay-as-you-go-pay-by-instances-e-byol/.

https://www.garanteprivacy.it/data-breach.

https://cloud.google.com/learn/what-is-cloud-architecture?hl=it.

https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf.

https://www.ibm.com/topics/api-endpoint

https://www.cpomagazine.com/cyber-security/twilio-data-breach-that-exposed-33-million-authy-phone-numbers-caused-by-unsecured-api-endpoint/.

https://techcrunch.com/2015/02/24/twilio-acquires-two-factor-authentication-service-authy/.

https://threatpost.com/report-microsofts-github-account-gets-hacked/155587/.

https://www.cnil.fr/en/european-data-protection-board-edpb.

https://www.congress.gov/bill/113th-congress/senate-bill/1995.

https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_it.

https://www.reddit.com/r/TooGoodToGoCanada/comments/1e0msf4/did_any_else_get_a_too_good_to_go_user_security/..

https://www.twilio.com/en-us/changelog/Security_Alert_Authy_App_Android_iOS

https://www.twilio.com/en-us

https://investors.twilio.com/node/9141/html

https://aspe.hhs.gov/reports/records-computers-rights-citizens.

https://curity.io/resources/learn/zero-trust-overview/