UNIVERSITA' DEGLI STUDI DI ROMA TOR VERGATA

***European Digital Law of the Person, of the Contract and of the Technological Marketplace* - EUDILA**
Cattedra Jean Monnet del Progetto ERASMUS +

Utilizzo illecito di dati personali:

il phishing tra GDPR, PSD2 e tecniche di MACHINE LEARNING

Ilenia Bergamasco

Matricola studente

Anno accademico 2023/2024

Sommario

Abstract

Negli ultimi anni, la digitalizzazione ha rivoluzionato la nostra società, portando ad un aumento esponenziale dell'uso di dati personali online. Questa tendenza ha creato nuovi rischi legati all'uso illecito di tali dati, tra cui il phishing. Il phishing è una tecnica di frode informatica che mira ad ottenere informazioni sensibili, come password e dati delle carte di credito, sfruttando la fiducia delle vittime. Con l'introduzione del Regolamento Generale sulla Protezione dei Dati (GDPR) e della Direttiva sui Servizi di Pagamento (PSD2), l'Unione Europea ha cercato di rafforzare la sicurezza e la privacy degli utenti. Inoltre, l'avanzamento delle tecnologie di machine learning offre nuove opportunità per prevenire e contrastare il phishing. Questo elaborato ha l'obiettivo di esaminare come il GDPR e la PSD2 proteggono i dati personali e la sicurezza delle transazioni, e come il machine learning, tramite l'uso di dati sintetici, possa contribuire a prevenire il phishing.

1. Introduzione

Lo sviluppo di nuove tecnologie ha posto un particolare accento sulla necessità di dover tutelare la persona umana e i suoi dati personali, resi accessibili a chiunque ed ovunque grazie all'avvento di Internet.

Con *dato personale* si indica una qualsiasi informazione relativa ad una persona fisica identificata o identificabile. Nello specifico, con *persona identificabile,* si indica una persona che possa essere identificata direttamente o indirettamente, utilizzando identificatori quali ad esempio il nome, il codice fiscale o i dati relativi alla residenza e alla condizione fisica o economica.

La *protezione del dato personale* non nasce però, con l'avvento della tecnologia, in quanto il concetto di riservatezza ha origine in America come diritto "*ad essere lasciato solo*" alla fine dell'Ottocento. In Italia, invece, il concetto di riservatezza ha acquisito valenza giuridica negli anni Sessanta.

Il *diritto alla riservatezza*, inteso come "*ius excludendi alios*", indica il diritto di un individuo di escludere soggetti terzi dalla propria sfera privata, limitando la libertà di espressione ed il diritto all'informazione di colui che viene escluso. Per tale motivo esso assume un'accezione negativa.

Al giorno d'oggi, il *diritto alla privacy* ha subito molte trasformazioni fino a diventare un diritto positivo attivo, ovvero il diritto ad avere il controllo sui propri dati personali. In quest'ottica, infatti, il diritto alla privacy viene inteso come il diritto di poter esercitare degli strumenti e ad attivare delle procedure per mantenere il controllo sulla circolazione dei nostri dati personali.

Il diritto alla riservatezza è strettamente legato al diritto della protezione dei dati personali, garantito da numerose norme internazionali, europee e nazionali. In particolare, l'articolo 7 della Carta dei diritti dell'Unione europea sancisce il rispetto della vita privata e familiare, mentre l'articolo 8 tutela i dati di carattere personale. In Italia, il diritto alla riservatezza è riconosciuto dalla Costituzione e dalla Carta dei diritti fondamentali dell'Unione Europea. La tutela dei dati personali è regolata dal Codice in materia di protezione dei dati (d.lgs. 30 giugno 2003, n. 196), che sancisce il diritto di ogni persona a proteggere le proprie informazioni. Tuttavia, il diritto alla riservatezza può

subire deroghe o limitazioni, che devono ispirarsi ai principi di proporzionalità, pertinenza e non eccedenza nel trattamento dei dati personali. Queste limitazioni sono necessarie per raggiungere obiettivi legittimi, come la pubblicità e la trasparenza, che sono fondamentali per il buon funzionamento della pubblica amministrazione e per la gestione dei dati che essa possiede e controlla. Inoltre, la Corte costituzionale italiana ha ribadito che la dignità umana è comprensiva del diritto alla riservatezza e che tale diritto è garantito dall'articolo 21 della Costituzione, che riconosce la libertà di manifestare il proprio pensiero con qualsiasi mezzo di diffusione.

Nell'ambito del panorama normativo attuale, il *Regolamento Generale sulla Protezione dei Dati* (GDPR) e la *Direttiva sui Servizi di Pagamento* (PSD2), rappresentano due pilastri fondamentali nella regolamentazione della privacy e della sicurezza finanziaria. Il GDPR, entrato in vigore nel maggio 2018, ha introdotto nuovi standard per la protezione dei dati personali, rafforzando i diritti degli individui e ponendo nuovi obblighi sulle organizzazioni che trattano informazioni private all'interno dell'Unione Europea. La PSD2 ha ulteriormente innovato il settore dei pagamenti, promuovendo la concorrenza e l'innovazione attraverso l'introduzione dell'Open Banking e rafforzando la sicurezza nelle transazioni online.

La protezione dei dati personali nell'era digitale è diventata una questione di primaria importanza, considerando l'enorme quantità di informazioni che vengono generate, raccolte e analizzate ogni giorno. Questi dati, che spaziano dalle informazioni personali di base alle abitudini di consumo, sono essenziali per le aziende che desiderano offrire servizi personalizzati e per gli enti governativi che mirano a migliorare i servizi pubblici. Tuttavia, la raccolta e l'utilizzo di tali dati devono essere bilanciati con il diritto alla privacy degli individui.

Il GDPR ha introdotto concetti chiave come il consenso esplicito, il diritto all'oblio, la portabilità e la notifica di violazione dei dati, che hanno significativamente aumentato il controllo degli utenti sulle proprie informazioni. Le organizzazioni sono ora tenute a implementare misure tecniche e organizzative adeguate per garantire un livello di sicurezza proporzionato al rischio, includendo la valutazione dell'impatto sulla protezione dei dati e la nomina di un responsabile della protezione degli stessi (DPO).

Parallelamente, la PSD2 ha imposto requisiti rigorosi per l'autenticazione forte del cliente (SCA) nelle transazioni online, riducendo il rischio di frodi e aumentando la fiducia dei consumatori nei servizi di pagamento digitali. Ha anche aperto il mercato a nuovi attori, come i fornitori di servizi di pagamento di terze parti (TPP), che possono accedere ai dati dei conti bancari dei clienti con il loro consenso, stimolando così l'innovazione e offrendo ai consumatori più scelta e controllo sulle proprie informazioni finanziarie.

Il GDPR e la PSD2 sono esempi emblematici di come l'Unione Europea stia affrontando le sfide poste dalla digitalizzazione, equilibrando la necessità di proteggere i diritti dei cittadini con la promozione di un mercato digitale unico e competitivo. La loro implementazione efficace richiede una comprensione approfondita non solo delle normative stesse, ma anche delle tecnologie sottostanti e delle dinamiche del mercato.

Il diritto privato e il diritto civile tradizionale hanno dunque dovuto fare i conti non solo con l'elemento tecnologico, ma anche con tutta una serie di normative speciali che insistono sulla dimensione digitale. Ci sono un'infinità di fonti normative trasversali a tutti i settori, che si affiancano a normative speciali come quelle del settore bancario, che hanno lo scopo di declinare le regole specifiche che si applicano solo in quel settore.

Il tema delle problematicità legate agli strumenti di pagamento è uno dei più importanti nel mercato, poiché gli investimenti in questo settore sono significativi e l'industria ha investito in infrastrutture tecnologiche che fondono la tecnologia alla finanza. Il PSD2 introduce nuove norme per la protezione dei dati personali e finanziari degli utenti, come ad esempio la necessità di ottenere il consenso esplicito degli utenti per il trattamento delle loro informazioni. Queste norme sono state introdotte per contrastare le minacce di phishing e altre forme di frode informatica che possono compromettere la sicurezza dei dati personali e finanziari degli utenti.

Il *phishing* non è altro che una pratica ingannevole, una truffa informatica, realizzata al danno degli utenti. Attraverso l'invio di e-mail, provenienti soprattutto da istituti finanziari fittizi o da siti web che necessitano dell'accesso previa registrazione, i criminali cercano di convincere il mal capitato a fornire loro informazioni riservate, attraverso messaggi che sembrano provenire da fonti attendibili. Così facendo i criminali si appropriano indebitamente dei dati personali dell'utente.

2. Gli strumenti di tutela dei dati personali dell'utente ai sensi del GDPR

Il Regolamento UE 679/2016, noto comunemente come GDPR, è entrato in vigore nel 2018 in tutti gli Stati membri. La decisione di adottare una fonte regolamentare riflette l'intenzione del legislatore europeo di passare dall'armonizzazione delle diverse normative nazionali all'uniformazione delle stesse. Tuttavia, spesso gli articoli del GDPR permettono ai singoli Stati membri di disciplinare in modo diverso alcuni aspetti. Il regolamento Generale sulla Protezione dei Dati (GDPR) rappresenta un pilastro fondamentale nella tutela della privacy e nella gestione dei dati personali all'interno dell'Unione Europea. Adottato il 27 aprile 2016 e applicato dal 25 maggio 2018, il GDPR ha introdotto un nuovo paradigma nel trattamento dei dati personali, ponendo l'accento sui principi di legalità, equità e trasparenza. Questi principi non sono solo linee guida astratte, ma requisiti concreti che ogni organizzazione deve soddisfare per garantire che il trattamento delle informazioni sia effettuato in modo legittimo. La legalità si riferisce all'obbligo di gestire i dati personali in conformità con la legge, ciò significa che ogni trattamento deve avere una base legale, come il consenso esplicito dell'interessato, la necessità di eseguire un contratto, l'obbligo legale, l'interesse vitale della persona o l'interesse pubblico. L'equità implica che la gestione deve essere giusta per l'individuo, senza causare ingiustizie o discriminazioni. La trasparenza richiede che l'individuo sia informato in modo chiaro e comprensibile su come le sue informazioni vengano raccolte, utilizzate, consultate o altrimenti trattate, nonché sulla finalità di tale trattamento.

Gli obiettivi del GDPR sono:

1. Definitiva armonizzazione della regolamentazione in materia di protezione dei dati personali.
2. Creare un mercato unico digitale europeo, dove i dati personali possano circolare liberamente.
3. Restituire ai cittadini il controllo sui propri dati.

L'art.1 comma 2, del GDPR sancisce che: "Il *presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.* L'art.1 comma 3, invece, ratifica che: "La *libera circolazione dei dati personali nell'Unione non può*

essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali."

Principio fondamentale del GDPR è il c.d. *principio del consenso* che stabilisce l'importanza di proteggere i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali e assicurare la libera circolazione di tali dati nell'Unione Europea. Il consenso deve essere *espresso*, non può quindi consistere in una mera deselezione di caselle online (cfr. la sentenza n.61 del 11/11/2020 della Corte di giustizia UE sez.II). Il consenso deve essere *inequivoco*, cioè deve essere chiaramente espresso per quel trattamento che ha quelle determinate finalità e caratteristiche. Il consenso deve essere *informato*, la persona deve conoscere il trattamento al quale si fa riferimento, e le modalità con cui viene fatto. L'omissione dell'informativa può comportare il risarcimento del danno da mancata informazione. Il consenso deve essere *liberamente prestato*, l'autorizzazione al trattamento di dati per finalità non attinenti all'esecuzione del contratto non è obbligatorio e, se invece vi è l'obbligo di fornire il permesso per queste finalità allora questo non è più liberamente prestato. Inoltre, il consenso deve essere *revocabile*, cioè il soggetto ha il diritto a revocare la propria approvazione in qualsiasi momento (art.7 co.3 GDPR). Se invece il permesso è necessario per l'esecuzione di un contratto, laddove venisse revocato, il servizio non sarebbe più gratuito.

Il considerando 10 evidenzia la necessità di un'applicazione coerente delle norme per garantire un elevato livello di protezione dei dati personali e la libera circolazione degli stessi all'interno dell'Unione Europea, "*Al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri. È opportuno assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione.*
[...]gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del presente regolamento. [...]".

Il GDPR fa riferimento alla tutela dei dati delle persone fisiche e non delle persone giuridiche anche se vengono più volte citate in tale Regolamento, che sposta l'attenzione dai diritti dei soggetti sottoposti al servizio, ai doveri dei titolari del trattamento.

Il GDPR contiene numerosi articoli fondamentali che stabiliscono i principi e le regole per la protezione dei dati personali. Di seguito i titoli degli articoli più importanti:

Articolo 5: Principi relativi al trattamento dei dati personali.
Articolo 6: Liceità del trattamento.
Articolo 7: Condizioni per il consenso.
Articolo 12-23: Diritti dell'interessato, tra cui diritto di accesso, rettifica, cancellazione (diritto all'oblio), limitazione del trattamento, portabilità dei dati e opposizione.
Articolo 24: Responsabilità del titolare del trattamento.
Articolo 25: Protezione dei dati fin dalla progettazione e per impostazione predefinita.
Articolo 32: Sicurezza del trattamento.
Articolo 33-34: Notifica di una violazione dei dati personali all'autorità di controllo e all'interessato.
Articolo 35: Valutazione d'impatto sulla protezione dei dati.
Articolo 37-39: Designazione, posizione e compiti del responsabile della protezione dei dati (DPO).
Articolo 44-50: Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali.

In particolare, gli articoli 25-32-35-37-39 introducono diversi strumenti e misure per la tutela delle proprie informazioni. Con l'art. 25 si richiede che i principi di protezione dei dati siano integrati nei sistemi e nei processi fin dalla fase di progettazione; invece, l'art. 32 richiede misure di sicurezza tecniche e organizzative per proteggere le informazioni, ed è necessaria inoltre una valutazione dei rischi per la protezione dei dati personali e l'adozione di misure per mitigarli, come dichiarato nell'art. 35. Infine, è prevista la nomina di un DPO per monitorare la conformità al GDPR (art. 37-39). Questi articoli coprono la maggior parte delle aree critiche relative alla protezione dei dati e forniscono un quadro normativo per affrontare le sfide moderne come il phishing e il machine learning. Il GDPR non tratta direttamente il tema del phishing, ma si occupa della sicurezza delle informazioni personali e delle violazioni delle stesse, che possono includere attacchi di phishing. In riferimento, l'art. 32 stabilisce che i titolari e i responsabili del trattamento devono adottare misure tecniche e organizzative adeguate a garantire un determinato livello di sicurezza, che può includere

la prevenzione contro attacchi di phishing. Nel caso in cui il phishing causi una violazione dei dati, questa deve essere notificata all'autorità di controllo (art. 33) e l'uso del machine learning è regolato per decisioni automatizzate che hanno effetti legali o significativi sugli individui (art.22).

Le organizzazioni sono tenute a implementare misure tecniche e organizzative adeguate per garantire e dimostrare che il trattamento sia effettuato in conformità con il regolamento, e devono seguire il principio di "*privacy by design*" e "*privacy by default*".

La violazione di questi principi può comportare sanzioni significative, che possono raggiungere fino al 4% del fatturato globale annuo dell'organizzazione o 20 milioni di euro, a seconda di quale sia maggiore.

Il GDPR stabilisce principi e requisiti generali per la protezione dei dati personali che richiedono l'adozione di misure adeguate. Di seguito un elenco degli strumenti e pratiche menzionati che sono riconosciuti o impliciti nel GDPR:

1. **Autenticazione a Due Fattori (2FA)**: Implicitamente supportato dai principi di sicurezza stabiliti nell'art. 32, che richiede misure tecniche adeguate per garantire la sicurezza dei dati personali.

2. **Software Anti-Phishing**: Anche se non menzionato specificamente, l'uso di software di sicurezza rientra nell'ambito dell'art. 32 per garantire la sicurezza del trattamento.

3. **Firewall e Sistemi di Prevenzione delle Intrusioni (IPS)**: Misure tecniche e organizzative adeguate, come descritto nell'art. 32.

4. **E-mail Filtering e Spam Protection**: Parte delle misure tecniche e organizzative per garantire la sicurezza delle informazioni, definito nell'art.32.

5. **Crittografia**: Specificamente menzionata nell'art. 32 come una misura per proteggere i dati personali.

6. **Token di Sicurezza**: Implicitamente supportato come parte delle misure tecniche adeguate a garantire la sicurezza dei dati.

7. **Formazione e Sensibilizzazione del Personale**: Implicito nell'art. 39, che descrive i compiti del responsabile della protezione dei dati (DPO), inclusa la formazione del personale coinvolto nel trattamento delle informazioni.

8. **Politiche di Sicurezza dell'Informazione**: Implicitamente richiesto dall'art. 24, che richiede ai titolari del trattamento di implementare misure tecniche e organizzative adeguate.

9. **Simulazioni di Phishing**: Parte delle misure di formazione e sensibilizzazione per il personale.

10. **Gestione delle Password**: Rientra nelle misure tecniche e organizzative adeguate per garantire la sicurezza dei dati.

11. **Valutazione dei Fornitori**: Specificato nell'art. 28, che richiede ai titolari del trattamento di garantire che i responsabili della gestione delle informazioni adottino misure adeguate.

12. **Sistemi di Monitoraggio e Rilevamento delle Minacce**: Implicito nelle misure tecniche e organizzative per garantire la sicurezza del trattamento (art. 32).

13. **Risposta agli Incidenti**: Specificamente richiesto dagli articoli 33 e 34, che riguardano la notifica di violazioni dei dati personali.

Altri consigli pratici per la protezione dei propri dati sono ad esempio la verifica delle e-mail, azione implicita nel GDPR nella sensibilizzazione e formazione del personale, l'uso di account separati e aggiornamento regolare del software.

Di conseguenza, molti degli strumenti e delle pratiche elencati sono in linea con i requisiti del regolamento, anche se non sono menzionati specificamente.

3. Le regole della PSD2 sulla sicurezza e la responsabilità dei fornitori di servizi di pagamento per le operazioni non autorizzate

La Direttiva sui Servizi di Pagamento (PSD2) rappresenta un cambiamento significativo nel panorama dei servizi finanziari, introducendo nuovi standard per la sicurezza e l'innovazione nel settore bancario. Questa direttiva ha l'obiettivo di aumentare la concorrenza e la trasparenza nel mercato, permettendo ai consumatori di beneficiare di servizi più efficienti e sicuri. Uno degli aspetti fondamentali della PSD2 è il requisito del consenso esplicito per l'accesso ai dati finanziari dei clienti, che deve essere fornito dalle banche a terze parti qualificate, come i fornitori di servizi di pagamento (PSP). La normativa vigente, come il Decreto Legislativo n. 11 del 2010 e la Direttiva PSD2, stabilisce chiare disposizioni per proteggere gli utenti da operazioni non autorizzate. In particolare, il fornitore di servizi di pagamento ha l'obbligo di impedire l'accesso non autorizzato a tali dispositivi e di rimborsare immediatamente l'utente in caso di operazioni non autorizzate. Inoltre, in caso di contestazione di un'operazione da parte dell'utente, spetta al prestatore di servizi di pagamento dimostrare che l'operazione sia stata autenticata e correttamente registrata. Queste misure sono fondamentali per mantenere la fiducia nel sistema dei pagamenti elettronici e per garantire che gli utenti siano tutelati in caso di frodi o uso improprio dei loro strumenti. Inizialmente, in Italia, la normativa che disciplina la responsabilità della banca in caso di operazioni di pagamento non autorizzate è stata emanata con il Decreto Legislativo 27 gennaio 2010, n. 11, che recepisce la Direttiva 2007/64/CE sui servizi di pagamento nel mercato interno (PSD1), successivamente sostituita con la direttiva PSD2.

Una delle principali novità introdotte dalla PSD2 è il concetto di "*Open Banking*", che permette di condividere tutti i dati presenti dell'ecosistema digitale senza che sia il cliente a doverli recuperare. Le banche sono obbligate a fornire accesso alle informazioni sui conti dei clienti a terze parti autorizzate, come le aziende Fintech, tramite API (Application Programming Interface). La tecnologia finanziaria, nota come *Fintech* (financial technology), rappresenta l'innovazione nel settore dei servizi finanziari. Questo settore sta trasformando il modo in cui le persone e le aziende interagiscono con le attività finanziarie, rendendole più accessibili, efficienti e sicure. Questo apre enormi opportunità per le aziende Fintech di sviluppare nuove applicazioni e servizi basati sui dati dei clienti, come aggregatori di conti, servizi di gestione delle finanze personali e piattaforme di

pagamento innovative. La direttiva impone requisiti di Strong Customer Authentication (SCA) per aumentare la sicurezza delle transazioni elettroniche. Questo ha portato allo sviluppo di tecnologie avanzate di autenticazione, come "*l'autenticazione biometrica*" e "*i token di sicurezza*". Il settore degli strumenti di pagamento elettronici ha rappresentato in Italia forse la prima palestra di digitalizzazione del mercato e di disciplina di sviluppo della normativa.

La PSD2 introduce due nuovi tipi di terze parti che possono operare nei servizi di pagamento: PISP (Payment Initiation Service Providers), entità che possono avviare pagamenti per conto dell'utente; AISP (Account Information Service Providers), entità che possono accedere ai dati dei conti bancari per fornire servizi di gestione finanziaria. La PSD2 facilita l'ingresso di queste nuove entità nel mercato, promuovendo la concorrenza e l'innovazione. La direttiva introduce requisiti per una maggiore trasparenza nelle tariffe e nei costi dei servizi di pagamento, nonché diritti più forti per i consumatori in caso di transazioni non autorizzate o fraudolente. Le aziende Fintech devono adeguarsi a questi requisiti di trasparenza e protezione dei consumatori, migliorando la fiducia degli utenti nei nuovi servizi finanziari. Questo comporta l'adozione di misure di sicurezza avanzate e la fornitura di informazioni chiare e complete sui costi dei servizi.

La PSD2 è una direttiva che risponde alle crescenti esigenze dei clienti per esperienze di pagamento rapide, personalizzate e senza soluzione di continuità. Le banche e gli altri PSP devono adattarsi rapidamente a queste nuove regole per non perdere terreno rispetto ai nuovi entranti nel mercato e per sfruttare le opportunità offerte da questa regolamentazione. La PSD2 non solo stimola l'innovazione nel settore dei pagamenti, ma offre anche ai clienti un maggiore controllo e permette ai commercianti e alle banche di trasformarla in un vantaggio competitivo. È imperativo per le aziende adottare un approccio olistico alla sicurezza, che non solo protegga i dati dei clienti ma garantisca anche la conformità alle leggi vigenti. Il GDPR impone rigide regole sulla gestione e protezione dei dati personali, mentre la PSD2 introduce requisiti specifici per il settore dei pagamenti elettronici, inclusa l'obbligatorietà dell'autenticazione forte del cliente. Le aziende devono quindi sviluppare strategie di sicurezza che integrino entrambi i regolamenti, assicurando che i processi aziendali siano trasparenti e che i diritti dei soggetti dei dati siano rispettati. Questo include la realizzazione di sistemi di gestione dei dati che siano sia robusti che agili, capaci di adattarsi ad un panorama normativo in continua evoluzione. Inoltre, è essenziale che le aziende

promuovano una cultura della sicurezza tra i dipendenti, attraverso la formazione continua e la sensibilizzazione alle minacce alla sicurezza dei dati.

Secondo la PSD2 fornitori di servizi di pagamento (PSP - Payment Service Providers) hanno specifiche responsabilità in merito alle operazioni di pagamento non autorizzate. Secondo l'art. 73 sul rimborso per transazioni non approvate, i PSP sono obbligati a rimborsare immediatamente l'utente pagatore per l'intero importo del movimento illegittimo. Il rimborso deve essere effettuato entro la fine del giorno lavorativo successivo al momento in cui il PSP viene a conoscenza del fatto della notifica da parte dell'utente. L'utente pagatore è responsabile fino a un massimo di 50 euro per perdite derivanti dall'uso di uno strumento di pagamento smarrito o rubato, a meno che:

4. la perdita, il furto o l'appropriazione indebita dell'elemento di autenticazione non sia stata rilevata dall'utente prima dell'operazione;
5. la perdita sia stata causata da azioni o omissioni di dipendenti, agenti o filiali del PSP (art. 74 - Limiti di responsabilità per le operazioni di pagamento non autorizzate).

Se il PSP non ha richiesto una forte autenticazione del cliente (SCA) come previsto dalla PSD2, non può addebitare alcun costo all'utente per le operazioni non autorizzate. L'utente non è responsabile per le transazioni illegittime che si verificano dopo che abbia notificato al PSP la perdita, il furto o l'appropriazione indebita dello strumento di pagamento.

Il garante della privacy ha pubblicato recentemente le linee guida per la corretta conservazione delle password. Se l'utente è in grado di dimostrare che non poteva evitare e che comunque ha adottato tutte le misure possibili e immaginabili, allora il rischio si sposta sull'operatore che quindi dovrà poi risponderne. Un sistema del genere deve assicurare un livello di invulnerabilità molto alto.

Per dimostrare la liceità dell'operazione (art. 72 - Prova dell'autenticazione e dell'esecuzione delle operazioni di pagamento) il PSP deve dimostrare che l'operazione di pagamento sia stata autenticata, correttamente registrata e contabilizzata e che non sia stata influenzata da guasti tecnici o altre carenze.

Gli utenti devono notificare tempestivamente al loro PSP, senza indebito ritardo, le operazioni non autorizzate o eseguite in modo inesatto, e comunque non oltre 13 mesi dalla data di addebito (art 71 - Notifica tempestiva delle operazioni non autorizzate o eseguite in modo inesatto). Se un'operazione di pagamento non è stata eseguita correttamente, il PSP del pagatore deve restituire l'importo della transazione finanziaria senza indebito ritardo (art. 75 - Rimborso per operazioni di pagamento non eseguite correttamente).

Il settore degli strumenti di pagamento elettronici ha rappresentato in Italia forse la prima palestra di digitalizzazione del mercato e di sviluppo della normativa, nata dall'esigenza europea di regolamentare le transazioni commerciali. Questa normativa disciplina l'uso di strumenti come bancomat, carte di credito e altri strumenti identificati come moneta elettronica, che utilizziamo quotidianamente. Questi strumenti non solo sollevano questioni legate alle infrastrutture tecnologiche, ma anche una serie di questioni legali relative al loro funzionamento e ai problemi che possono emergere, soprattutto nel contesto digitale, dove le truffe sono in aumento.

Per prima cosa, è necessario analizzare la panoramica degli strumenti di pagamento, poi esaminare le tipologie ricorrenti di truffe che coinvolgono questi strumenti e infine capire come la normativa risponde a queste problematiche.

Ad esempio, American Express è stata la prima a introdurre il concetto di pagamento a distanza, permettendo l'acquisto di beni senza l'uso di contanti. Una delle prime truffe note era chiamata "il ferro da stiro", in cui i truffatori mettevano una carta velina sopra ad una carta bancomat e passavano un ferro da stiro per copiare i dati.

Negli anni '70 si è assistito all'introduzione delle prime carte di credito con banda magnetica, le prime a racchiudere informazioni all'interno di un dispositivo plastificato. Queste carte memorizzavano già allora tutte le informazioni rilevanti, come nome, cognome, codice della carta e dati relativi alle autorizzazioni.

Per consentire il pagamento con carta, vennero realizzati i primi terminali POS, che collegavano a distanza i commercianti con le banche dei pagatori. Questo permetteva di vendere beni senza

incassare materialmente la somma, grazie a un segnale che confermava il trasferimento di fondi dal conto dell'acquirente a quello del venditore.

Ad oggi, è obbligatorio accettare pagamenti con carta, che nel nostro ordinamento sono equivalenti ai pagamenti in contante. È vietata l'imposizione di sovrapprezzi in base al tipo di strumento di pagamento utilizzato, questo perché, in passato, si tendeva a non accettare pagamenti con carta per evitare di emettere scontrini.

Oggigiorno, i POS e i pagamenti avvengono tramite dispositivi collegati alla rete 4G. In trent'anni di innovazione tecnologica e giuridica, è stato necessario capire come sostituire lo scambio di denaro fisico con transazioni a distanza e, soprattutto, come rendere sicure queste transazioni. Con l'evoluzione delle transazioni moderne, si è velocizzato il meccanismo di pagamento, ma sono emerse sempre più questioni legate alla sicurezza. Ad esempio, una carta contactless nella borsa può essere vulnerabile a dispositivi magnetici avvicinati da persone con cattive intenzioni. La protezione è garantita da sistemi di sicurezza progettati per prevenire tali eventi. Ad esempio, per le transazioni contactless, il sistema non legge la stessa transazione più volte. Se si passa la carta due volte in un breve lasso di tempo, la seconda transazione viene bloccata per evitare duplicazioni. Ad esempio, se aprendo il banking si nota un addebito di 1.700 € per un volo Roma-San Pietroburgo che non è stato acquistato volontariamente dal possessore della carta, l'ordinamento prevede una serie di coperture normative. Queste regole tecniche sono imposte al mercato per agevolare il sistema di pagamenti e proteggere gli utilizzatori dal rischio di truffe.

Il sistema dei pagamenti è estremamente complesso e coinvolge molti attori: la banca dell'acquirente che chiede alla banca del commerciante di incassare una somma; un circuito che permette alle diverse banche di comunicare tra loro e di far avanzare la procedura. Questa infrastruttura consente il flusso delle transazioni. Questi pochi secondi di esecuzione del pagamento sono protetti da una serie di regole, come ad esempio, la strong customer authentication, un sistema diventato obbligatorio nel nostro paese, che impone agli operatori di adottare metodi di autenticazione basati su diversi fattori.

In passato, si utilizzava una pennetta che generava un codice OTP da inserire per completare l'operazione. Questo sistema è stato progressivamente abbandonato poiché la chiavetta poteva

essere facilmente sottratta. Ora, il sistema di autenticazione si basa su più livelli, che rispettano il parametro della conoscenza, ossia qualcosa che solo l'utente conosce. Ad esempio, non basta solo il PIN, ma serve anche qualcosa che solo l'utente possiede, come un token o uno smartphone.

Oggi, molte banche utilizzano app per autenticare le transazioni, che funzionano solo tramite il cellulare dell'utente. Questi elementi devono essere indipendenti tra loro, affinché la violazione di un dispositivo non comprometta la sicurezza dell'intero sistema. Se una transazione non autorizzata avviene, ci sono meccanismi di controllo interno che le banche devono adottare per proteggere il cliente. Il sistema deve non solo fornire una carta sicura, ma anche avvisare l'utente ogni volta che viene effettuata un'operazione sul conto, permettendo un monitoraggio costante della regolarità delle transazioni.

In termini di sicurezza della carta di pagamento, essa ad oggi presenta una serie di caratteristiche che rendono la transazione più sicura, ovvero dei fattori di autenticazione di sicurezza per gestire le transazioni in modo sicuro, come un numero, una data di scadenza e un codice CVC a tre cifre.

Esistono fondamentalmente due tipologie di carte di pagamento: la carta bancomat, collegata ad un conto corrente, una sorta di salvadanaio; la carta di credito, ancorata ad una linea di credito o linea di fido. Se viene effettuata una truffa su una carta bancomat, il plafond di aggressività sarà limitato, invece se la truffa viene fatta ad un soggetto che possiede una carta di credito, si ha potenzialmente una disponibilità molto più ampia di denaro.

Le forme più ricorrenti di truffa che molto spesso bypassano la copertura normativa sono il phishing, lo smishing e il vishing, ovvero tecniche di truffa che mirano a ingannare le persone per ottenere informazioni sensibili come numeri di carta di credito, credenziali di accesso o altre informazioni personali. Il phishing è una tecnica di truffa in cui gli aggressori inviano e-mail che sembrano provenire da fonti legittime (come banche, servizi online o altre istituzioni fidate) per indurre le vittime a rivelare informazioni sensibili. Le e-mail di phishing spesso contengono link a siti web falsi che sembrano autentici. Quando la vittima inserisce le proprie credenziali o altre informazioni sul sito falso, queste vengono inviate all'aggressore. Lo smishing è una variante del phishing che utilizza messaggi di testo (SMS) per ingannare le vittime. Gli aggressori inviano SMS contenenti link a siti web falsi o numeri di telefono falsi. Le vittime sono indotte a cliccare sui link o a chiamare i numeri,

rivelando così informazioni sensibili. Il vishing (Voice Phishing) è una tecnica di truffa che utilizza chiamate telefoniche per ottenere informazioni sensibili dalle vittime. Gli aggressori chiamano le vittime fingendosi rappresentanti di istituzioni fidate (come banche o aziende) e le convincono a fornire informazioni personali o finanziarie. Queste tecniche di inganno sono particolarmente pericolose perché spesso fanno leva sulla fiducia e sulla mancanza di consapevolezza delle vittime riguardo ai metodi di sicurezza online.

Il sistema ha adottato una serie di misure a livello tecnologico che permettono oggi di segnalare al sistema bancario e al sistema telefonico eventuali furti di identità proprio per allertare e capire cosa stia succedendo. Il sistema giuridico si preoccupa di creare delle regole che possano cercare di indennizzare l'utente ogni qualvolta rimane vittima di questo sistema. Regole di natura giuridica, cioè paracaduti normativi che si aprono ogni qualvolta si verificano fattispecie che permettono poi di aprire dei diritti speciali.

Il sistema si pone l'obiettivo di facilitare l'utilizzo di questi strumenti proprio allo scopo di abbattere le criticità tipiche del contante e quindi facilitare le transazioni.

L'open banking è un esempio di digitalizzazione del settore mentre il crowdfunding ha rivoluzionato il sistema del credito, e in tutto ciò il diritto cerca di trovare la regola applicabile.

La cosiddetta PSD2, in fase di sostituzione con la PSD3, si pone proprio l'obiettivo di dettare quelle regole organizzative e di tutela per permettere di far sviluppare un sistema di pagamenti elettronici in sicurezza. Molto spesso il sistema è talmente complesso nella filiera di responsabilità che non si sa mai dove si è realmente realizzata l'anomalia. La PSD3 dovrebbe risolvere anche questo tema, assicurando una maggiore tutela degli utenti.

La tecnologia è troppo avanzata rispetto alle norme, quindi le questioni pratiche non hanno sempre una risposta dal punto di vista giuridico.

4. Il machine learning nella prevenzione del phishing: il potenziale dei dati sintetici

L'integrazione del machine learning nel settore finanziario promette miglioramenti nell'efficienza operativa, nella personalizzazione dei servizi e nella capacità predittiva, ma solleva anche questioni complesse relative al consenso dei dati, alla privacy e alla non discriminazione. Ad esempio, i modelli di machine learning possono potenzialmente amplificare i pregiudizi esistenti nei dati, portando a decisioni automatizzate che potrebbero violare i principi del GDPR. Pertanto, è fondamentale sviluppare algoritmi che siano trasparenti, spiegabili, per garantire che i diritti dei soggetti dei dati siano salvaguardati.

I *dati sintetici* sono dati generati artificialmente che non rappresentano direttamente informazioni reali, ma sono invece creati per avere determinate caratteristiche o proprietà statistiche simili a quelle delle informazioni reali. Questi dati possono essere utilizzati per scopi di testing, addestramento di algoritmi di machine learning, o per proteggere la privacy delle informazioni sensibili.

Ad esempio, nel contesto della privacy, è possibile generare dati sintetici che preservano le proprietà statistiche di quelli reali ma non contengano informazioni personali identificabili, consentendo così le analisi senza il rischio di rivelare informazioni riservate.

I dati sintetici possono essere creati utilizzando diverse tecniche, come la generazione casuale, l'uso di modelli statistici o l'applicazione di algoritmi di machine learning. L'obiettivo principale è quello di garantire che i dati generati conservino le caratteristiche essenziali di quelli reali, ma senza contenere informazioni sensibili o identificabili.

Addestrare un modello in machine learning significa insegnare al modello il riconoscimento del pattern e le relazioni nei dati al fine di fare previsioni o prendere decisioni. Questo processo coinvolge l'utilizzo di algoritmi e tecniche per regolare i parametri del modello in modo che sia in grado di produrre output accurati quando presentato con nuovi dati di input.

Il phishing rappresenta una delle minacce più insidiose e pervasive nel panorama della sicurezza informatica. Gli attacchi di phishing sono notoriamente difficili da rilevare, poiché i malintenzionati utilizzano messaggi e siti web che appaiono legittimi per ingannare le vittime. Le implicazioni di tali attacchi sono gravi: possono portare al furto di identità, perdite finanziarie significative e danni alla reputazione delle persone e delle organizzazioni colpite.

Le tecniche di phishing si sono evolute nel tempo, diventando sempre più sofisticate. Inizialmente, gli attacchi erano per lo più e-mail generiche inviate a un ampio numero di destinatari, oggi, i cybercriminali impiegano strategie mirate, come lo spear phishing, che prevede l'invio di messaggi personalizzati a singoli individui o organizzazioni, aumentando così le probabilità di successo.

La sicurezza dei dati personali e finanziari è fondamentale, poiché la loro compromissione può avere ripercussioni a lungo termine. Pertanto, è essenziale adottare misure di prevenzione efficaci. Queste includono la formazione degli utenti sui segnali di allarme degli attacchi di phishing, l'implementazione di soluzioni tecnologiche come filtri anti-phishing e sistemi di autenticazione a più fattori, e la creazione di politiche aziendali che promuovano pratiche di sicurezza consapevoli.

Il machine learning rappresenta una frontiera avanzata nel campo della sicurezza informatica, offrendo strumenti potenti per la rilevazione di attività sospette e il rafforzamento delle misure di protezione dei dati. Attraverso l'analisi di grandi volumi di informazioni e l'apprendimento da pattern complessi, gli algoritmi di machine learning sono in grado di identificare anomalie e comportamenti che si discostano dalla norma, spesso indicativi di potenziali minacce o intrusioni. Questa capacità di apprendimento automatico consente di adattarsi rapidamente a nuove strategie messe in atto da attori malevoli, mantenendo i sistemi di difesa sempre un passo avanti rispetto alle tecniche di attacco.

Inoltre, il machine learning può essere impiegato per migliorare la sicurezza dei dati attraverso meccanismi di autenticazione più sofisticati, come il riconoscimento biometrico, che apprende e si adatta alle variazioni fisiologiche degli utenti autorizzati. Allo stesso modo, sistemi di crittografia potenziati da algoritmi di apprendimento possono generare chiavi di sicurezza più complesse e difficili da decifrare. La capacità di questi sistemi di apprendere ed evolversi con l'uso, li rende strumenti preziosi nella lotta contro il cybercrime, che è in continua evoluzione.

Tuttavia, l'implementazione del machine learning nella sicurezza dei dati presenta anche delle sfide. La necessità di disporre di grandi quantità di informazioni per l'addestramento degli algoritmi solleva questioni relative alla privacy e alla gestione dei dati stessi. Inoltre, la complessità degli algoritmi di machine learning richiede una competenza tecnica elevata per la loro configurazione e manutenzione, oltre ad una costante vigilanza per evitare errori che potrebbero compromettere l'efficacia del sistema.

Nonostante queste sfide, il potenziale del machine learning come strumento di difesa è immenso. Con l'avanzare della ricerca e lo sviluppo di nuove tecniche, si aprono scenari promettenti per la sicurezza informatica. La collaborazione tra esperti di sicurezza e specialisti di machine learning è fondamentale per sfruttare appieno le capacità di questi strumenti, garantendo al contempo il rispetto delle normative sulla privacy e la protezione dei dati degli utenti. Sebbene le sfide siano significative, l'approccio proattivo e l'adattabilità offerti da questi sistemi intelligenti promettono di rivoluzionare il modo in cui proteggiamo le nostre informazioni nell'era digitale.

La protezione dei dati è un aspetto cruciale in questo contesto, poiché il machine learning può elaborare enormi quantità di informazioni personali, spesso senza il consenso esplicito degli utenti. Le aziende devono quindi assicurarsi di rispettare le normative sulla privacy, come il GDPR nell'Unione Europea, che impone rigidi requisiti per il trattamento dei dati personali. Inoltre, devono considerare le implicazioni etiche dell'uso dei dati, come la potenziale discriminazione che può derivare da algoritmi prevenuti o da una cattiva gestione dei dati.

Dunque, le aziende che implementano queste tecnologie devono navigare in un complesso panorama di obblighi legali, che spesso variano significativamente da una giurisdizione all'altra. Allo stesso tempo, esiste un crescente consenso sul fatto che oltre alla conformità legale, le aziende debbano adottare un approccio etico che consideri l'impatto delle loro tecnologie sulla società e sugli individui.

Un approccio responsabile richiede una comprensione approfondita non solo delle tecnologie di machine learning, ma anche delle leggi e delle normative pertinenti. Le aziende devono lavorare a stretto contatto con esperti legali, etici e tecnici per sviluppare politiche e procedure che garantiscano l'uso etico e legale del machine learning. Questo include la realizzazione di valutazioni

d'impatto sulla privacy, la progettazione di algoritmi trasparenti e responsabili, e l'implementazione di misure di sicurezza robuste per proteggere i dati dagli accessi non autorizzati o dagli abusi.

Inoltre, le aziende dovrebbero impegnarsi in un dialogo aperto con le parti interessate, inclusi i clienti, i dipendenti e la società civile, per comprendere meglio le preoccupazioni etiche e per costruire una fiducia reciproca. La formazione e l'educazione dei dipendenti sull'importanza della protezione dei dati e delle pratiche etiche nel machine learning sono altresì fondamentali per promuovere una cultura aziendale che valorizzi la responsabilità e la trasparenza.

In conclusione, la responsabilità etica e legale nell'uso del machine learning è un campo complesso e in continua evoluzione, che richiede un impegno costante da parte delle aziende per rimanere aggiornate sulle migliori pratiche e per garantire che le loro tecnologie siano utilizzate in modo benefico e giusto. Con un approccio olistico che integra considerazioni legali, etiche e tecniche, le aziende possono guidare l'innovazione in modo responsabile e guadagnarsi la fiducia del pubblico.

5. Conclusioni

In un'era in cui la digitalizzazione permea ogni aspetto della vita quotidiana, l'importanza di un approccio integrato alla protezione dei dati assume una rilevanza cruciale. La gestione responsabile delle informazioni personali non è soltanto una questione di conformità alle normative vigenti, come il Regolamento Generale sulla Protezione dei Dati (GDPR), ma rappresenta anche un imperativo etico fondamentale per le organizzazioni che mirano a preservare la fiducia dei loro utenti. Un approccio sistemico alla protezione dei dati richiede una comprensione approfondita delle tecnologie emergenti, come l'intelligenza artificiale e il machine learning, che possono sia potenziare che minare la sicurezza dei dati.

Dunque, l'adozione di un approccio integrato e responsabile alla protezione dei dati è indispensabile per navigare nel complesso panorama delle normative e delle tecnologie in continua evoluzione.

6. Sitografia

1. https://digitallibrary.cultura.gov.it/notizie/cyber-security-intelligenza-artificiale-machine-learning-e-scenari-di-rischio-sempre-piu-complessi/
2. https://def.finanze.it/DocTribFrontend/getAttoNormativoDetail.do?ACTION=getArticolo&id=%7BF41B9D1B-4DBB-4431-AE8E-3A8D708FED24%7D&codiceOrdinamento=200001200000000&articolo=Articolo%2012
3. https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32015L2366&from=EN
4. https://eur-lex.europa.eu/eli/reg/2016/679/oj/ita?uri=CELEX%3A32016R0679
5. https://legalblink.it/post/linee-guida-cnil-privacy-e-intelligenza-artificiale.html
6. https://yesnology.com/diritto-alla-riservatezza-cosa-e-e-cosa-comporta/
7. https://www.acronis.com/it-it/blog/posts/role-of-ai-and-ml-in-ransomware-protection/
8. https://www.agendadigitale.eu/cultura-digitale/machine-learning-i-problemi-per-la-privacy-e-le-possibili-soluzioni/
9. https://www.bancaditalia.it/media/notizia/entra-in-vigore-nuova-direttiva-europea-sui-servizi-di-pagamento-nel-mercato-interno-psd2/?dotcache=refresh
10. https://www.commissariatodips.it/approfondimenti/phishing/phishing-che-cose/index.html
11. https://cyberment.it/sicurezza-informatica/algoritmi-di-machine-learning-applicati-alla-sicurezza-informatica/
12. https://www.fondazioneconilsud.it/wp-content/uploads/2020/04/Vademecum-sulla-gestione-della-privacy-3.pdf
13. https://www.garanteprivacy.it/regolamentoue
14. https://www.itgovernance.eu/it-it/gdpr-testo-completo