GDPR e cifratura: concetti base e approcci pratici

La definizione delle misure di sicurezza da applicare al proprio sistema di gestione dei dati personali rappresenta una delle sfide principali, se non la più importante, posta ai titolari del trattamento dal Regolamento UE sulla protezione dei dati – *General Data Protection Regulation*, comunemente noto come GDPR.

A complicare il panorama, l'abrogazione dell'ex Allegato B al Codice Privacy (D.Lgs. 196/2003) che conteneva un elenco dettagliato di misure minime di sicurezza, unanimemente considerato esaustivo.

L'**attuale quadro normativo**, invece, affida al titolare il compito e la responsabilità di decidere quali misure di sicurezza possano essere considerate idonee al fine di garantire un'adeguata protezione ai dati personali trattati. Tale libertà di scelta ha portato, nel corso dell'ultimo anno – il primo da quando il GDPR è divenuto pienamente applicabile – a considerare la cifratura quale misura "regina" atta a garantire riservatezza, integrità e disponibilità dei sistemi e dei servizi di trattamento.

All'interno del testo del Regolamento UE, il concetto di cifratura viene citato a più riprese.

Si parte dal *Considerando 83* ove è previsto che i titolari o i responsabili del trattamento dovrebbero valutare i rischi delle loro varie attività di trattamento dei dati e attuare misure per mitigare tali rischi, come la cifratura, in modo da:

- mantenere la sicurezza;
- impedire trattamenti non conformi al GDPR[1].

Pertanto, tale valutazione dovrebbe partire dall'individuazione dei **tipi di dati personali coinvolti** per arrivare all'effettivo **danno** che potrebbe essere causato agli interessati in assenza di idonee misure di sicurezza.

L'**art. 32**, poi, annovera la cifratura tra le misure tecniche e organizzative a disposizione del titolare, per garantire un livello di sicurezza adeguato al rischio. Ancora, l'**art. 34**, focalizzato sulla comunicazione di un'eventuale violazione di dati ai soggetti interessati, menziona nuovamente la cifratura come esimente per il titolare che abbia implementato misure adeguate a rendere i dati, oggetto della violazione, incomprensibili a chiunque non sia autorizzato ad accedervi.

L'esplicito riferimento alla cifratura nel GDPR ha però **causato** confusione circa la sua configurazione quale requisito essenziale. L'impiego di tecniche di cifratura, oltre ad essere impegnativo, può risultare talvolta inefficace poiché non necessario o sproporzionato rispetto alle tipologie di trattamenti effettuati e di dati trattati.

In linea generale, possiamo dunque considerare questo come uno strumento certamente utile ma, di certo, non l'unico da implementare. Va ricordato, infatti, che **le modalità di compromissione dei dati sono molteplici** e la crittografia blocca solo alcune di queste.

Pur non essendo una misura "obbligata", rimane comunque "caldamente consigliata" per limitare i rischi impattanti sui dati personali. Il ricorso alla cifratura viene dunque rimesso all'iniziativa dei titolari del trattamento, in forza di quel principio di *accountability* che sta alla base del nuovo approccio promosso dalla normativa.

Appurata quindi la necessità di introdurre – all'interno dei propri processi – meccanismi di crittografia, è conveniente partire dai concetti base e dare le opportune definizioni.

Crittografia: maneggiare con cura

La cifratura è essenzialmente quel processo che rende un determinato dato incomprensibile, al fine di garantire la sua confidenzialità. I concetti alla base di questo processo sono l'informazione da proteggere, l'algoritmo di cifratura, il crittogramma *(cypher-text)* e un valore segreto definito chiave *(key).* La crittografia *dovrebbe* garantire che, senza conoscere la chiave, non si possa mai avere la possibilità di ottenere il messaggio in chiaro da cui proviene il crittogramma.



Link 1 – https://bit.ly/2XbJXSk

Il lettore attento avrà notato che è stato utilizzato il condizionale *dovrebbe,* in quanto l'utilizzo della crittografia ad oggi è in un certo senso idealizzato. La crittografia **in teoria** è un meccanismo forte e affidabile, soprattutto perché è basato su teorie e concetti matematici dimostrabili e dimostrati. In pratica, invece, è potenzialmente affetta da tutti i problemi che affliggono le implementazioni di tutti gli altri sistemi di sicurezza. Questo è ancora più evidente quando i sistemi di cifratura vengono, in qualche modo, ideati o concepiti da persone non esperte che, in un impeto di creatività – e forse anche egocentrismo – immaginano di aver inventato l'algoritmo di crittografia perfetto.

Appurato quindi che la creazione di algoritmi di cifratura dovrebbe essere sempre dominio di professionisti esperti, cosa significa in realtà avere una cifratura **sicura**? In maniera molto intuitiva, dato un crittogramma generato da un certo algoritmo di cifratura, il sistema non permette, in un determinato intervallo di tempo, di risalire al testo in chiaro se non conoscendo la relativa chiave di cifratura utilizzata.

Crittografia: tante tipologie, un unico scopo

Come abbiamo già accennato, il fine ultimo della crittografia è proteggere un'informazione. Permettere a questa informazione di essere condivisa solo tra i soggetti interessati e proteggerla da occhi indiscreti. Che sia un'informazione di guerra, un'informazione elettorale, dati personali o anche una lettera d'amore, il fine rimane lo stesso: che sia garantita la sua confidenzialità. A questo fine si può arrivare in modi diversi, ci limiteremo a presentare quelli più noti ed utilizzati.

Crittografia simmetrica

Questo tipo di crittografia è quella classica, quella che intuitivamente possiamo immaginare ed utilizzare nella vita di tutti i giorni. Facciamo un **esempio**:

Mario e Anastasia hanno un'informazione da scambiare; un'informazione che reputano così importante da non poter rischiare che qualcun altro possa conoscerla. Mettiamo che tale informazione sia un documento testuale che Mario deve inviare ad Anastasia in modo che possa revisionarlo prima di inviarlo a un cliente.

Il concetto alla base della crittografia simmetrica è che **la chiave usata per cifrare il documento è la stessa utilizzata per decifrarlo**. Quindi, Mario non dovrà fare altro che scegliere una chiave di cifratura, magari di un certo livello di complessità, cifrare il documento utilizzando un software adeguato e inviarlo ad Anastasia. Quest'ultima, con un software compatibile (non per forza lo stesso) decifrerà il documento, fornendo la chiave di cifratura utilizzata da Mario e potrà quindi leggere il documento in chiaro. La confidenzialità dell'informazione è quindi garantita in quanto, se anche un utente malintenzionato fosse in grado di rubare e/o copiare l'informazione, non avrebbe modo di

decifrarla senza conoscere la chiave. A prima vista tutto sembra funzionare correttamente, ma resta un problema: in che modo Mario e Anastasia hanno condiviso la chiave di cifratura utilizzata? Di certo non possono condividerla tramite lo stesso canale che utilizzano per scambiarsi l'informazione. A tal fine, potrebbero incontrarsi o telefonarsi e scambiarla a voce, inviarla via sms o utilizzare un altro sistema di messaggistica. In questi casi, diciamo che i due hanno scambiato la chiave in modalità **OOB** (Out Of Band): hanno utilizzato quindi un canale diverso da quello in cui viaggia l'informazione da proteggere, in modo da rendere *più complicata* la vita al malintenzionato. Attenzione: diciamo più complicata, non impossibile. Le motivazioni risiedono tutte nell'importanza dell'informazione da proteggere. Se questa ha un'elevata importanza, diciamo di sicurezza nazionale, è probabile che sia Mario, sia Anastasia, possano essere tenuti sotto controllo e spiati. Non si può quindi considerare sicuro il canale che hanno utilizzato per scambiare la chiave. Il **problema** da risolvere è quello di **proteggere il modo in cui i due attori si scambiano la chiave di cifratura.**

Un esempio pratico di crittografia simmetrica è quello che utilizza, come algoritmo di cifratura, il **DES** (Data Encryption Standard). Nel mondo finanziario, la cifratura DES è stata utilizzata per anni per proteggere la sicurezza delle transazioni, come quelle relative alle nostre carte di credito. Tuttavia, negli ultimi decenni è stato dimostrato che tale algoritmo ha delle debolezze matematiche che possono essere sfruttate per decifrare l'informazione che esso protegge, anche non conoscendo la chiave di cifratura utilizzata. Si parla, in questo caso, di attacchi basati sulla *crittoanalisi* e cioè *lo studio dei metodi per ottenere il significato di informazioni cifrate senza avere accesso all'informazione segreta che è di solito richiesta per effettuare l'operazione****[2]****.* Al DES è seguita poi una sua versione più complessa, il **3DES** (Triple Data Encryption Standard) e cioè l'applicazione del DES per tre volte.

Oggigiorno, è praticamente l'algoritmo di cifratura più utilizzato nel mondo finanziario, bancario e assicurativo.

Crittografia asimmetrica

Il problema della condivisione della chiave di cifratura è stato risolto, in maniera davvero elegante, dalla crittografia definita asimmetrica. Proprio nel termine *asimmetrica* risiede la vera novità di questo nuovo tipo di crittografia: si usano due chiavi diverse per cifrare e decifrare l'informazione. Ogni attore ha quindi due chiavi: una per cifrare, definita chiave pubblica o *pubkey,* una per decifrare, definita chiave privata. Quindi, tornando ai due attori di prima, Mario userà la chiave pubblica di Anastasia per cifrare il messaggio; Anastasia userà la sua chiave privata per decifrarlo. Non c'è più il problema della condivisione della chiave di cifratura perché, per definizione, questa è pubblica: tutti possono vederla. Ma per decifrare, bisognerà utilizzare la chiave privata, quella che ognuno dovrà gelosamente custodire e che non dovrà mai condividere con nessuno.

Link 2 – https://bit.ly/2HR8Wqx

Ma cosa garantisce questo legame tra chiave pubblica e chiave privata? Sempre la matematica! Noi comuni mortali non siamo tanto interessati a capire il funzionamento intimo degli algoritmi e teoremi matematici che garantiscono l'affidabilità di questo sistema, ci basti pensare che funziona, che è sicuro e che la nostra chiave privata è, per definizione, personale: **non va condivisa con nessuno al mondo. Mai. In nessun caso.**

Il primo sistema basato sulla crittografia asimmetrica a chiave pubblica vede la luce alla fine degli anni '70 nei laboratori del MIT, grazie al lavoro di un geniale gruppo di ricerca formato da R. Rivest, A. Shamir e L. Adleman che ideano il famoso algoritmo **RSA**. Alla base del funzionamento di

questo algoritmo c'è un concetto molto semplice, presente in bibliografia sin dai tempi dei matematici greci: **i numeri primi**. Semplificando veramente di molto, possiamo pensare che è computazionalmente molto facile moltiplicare due numeri primi di grandezza arbitraria, mentre è molto difficile (e computazionalmente molto oneroso) risalire ai due numeri primi che, moltiplicati tra loro, danno il numero in questione. In questo contesto, possiamo identificare la chiave privata come la coppia di numeri primi, mentre la chiave pubblica come il loro prodotto.

Tale algoritmo protegge la nostra vita di tutti i giorni: dalle applicazioni presenti nei chip delle nostre carte di credito, ai famosi certificati SSL che assicurano la riservatezza dei nostri dati di navigazione.

Quindi la crittografia asimmetrica ha risolto tutti i problemi della confidenzialità nello scambio delle informazioni? Effettivamente ne risolve tanti, ma **non proprio tutti**. Per sua stessa natura, è molto lenta e dunque poco utilizzabile all'interno di processi che richiedono prestazioni *real-time,* quali quelli autorizzativi nei pagamenti elettronici. Cosa che non capita con la cifratura simmetrica, che invece è semplice e, quindi, veloce. Ecco perché il connubio tra le due è la soluzione scelta unanimemente: si può utilizzare la crittografia a chiave pubblica per trasmettere la chiave di cifratura per poi proseguire con la crittografia simmetrica.

Approcci pratici

Tornando ai titolari del trattamento, cosa dovranno fare quindi questi poveri malcapitati che si troveranno a dover gestire in modo pratico e reale il **problema crittografia?** Ecco alcuni consigli basati sulla nostra personale esperienza:

- affidarsi a prodotti basati su algoritmi standard di mercato e non cadere nell'errore di adottare soluzioni raffazzonate e fatte in casa da sconosciuti, benché auto

conclamati geni e professori emeriti di crittografia, inventori del sistema di cifratura perfetto (…);

- non sempre i prodotti commerciali sono la scelta migliore in ogni contesto: il mondo *Open Source* è costellato di eccellenti soluzioni che possono essere adottate anche in particolari ambienti dove è richiesto il supporto del fornitore;
- studiare e definire bene l'architettura del sistema di cifratura utilizzato: una scelta approssimativa prima si trasformerà certamente in un problema enorme, e costoso, da gestire in seguito;
- non sottovalutare mai la gestione delle chiavi crittografiche: il loro ciclo di vita, il loro backup, la loro gestione e la loro manutenzione. Definire, prima di adottare qualunque soluzione di cifratura, come si andranno a gestire le chiavi;
- non applicare la crittografia subito su tutto: partire da pochi processi, coinvolgere pochi dipartimenti alla volta, capire il contesto in cui impatterà l'introduzione della crittografia;
- utilizzare un approccio basato sul rischio, come sempre;
- formare i collaboratori: importantissimo spiegare i veri motivi del perché un'informazione deve essere protetta.

Non sempre la soluzione più complessa e costosa è quella giusta: ad esempio, in determinati semplici contesti, anche l'utilizzo di archivi compressi protetti da password può risolvere in maniera veloce il problema, abbassando il rischio di *data breach* a livelli accettabili. D'altronde, il **cambio di approccio del legislatore** è stato proprio in questa direzione: non dettare regole precise, ma lasciare ai singoli la scelta del migliore sistema di protezione dei dati, compatibilmente con il proprio contesto.

Questi pochi semplici accorgimenti, che possono sembrare banali e normali, purtroppo raramente appaiono ben applicati nelle realtà organizzative. Si commette spesso l'errore di

affidarsi a entità esterne che, condotte dalle buone intenzioni di introdurre in azienda un software di ultima generazione, provocano un abbattimento drastico della produttività, cosa che oggi poche aziende possono permettersi.

Note

[1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Regolamento generale sulla protezione dei dati).

[2] https://it.wikipedia.org/wiki/Crittoanalisi.

Articolo a cura di **Anastasia Ambesi** e **Mario Ciccarelli**

https://www.ictsecuritymagazine.com/articoli/gdpr-e-cifratura-concetti-base-e-approcci-pratici/