Cristina Vicarelli
Avvocato

Crittografia e pen test: la cyber security entra nel GDPR

Si è molto parlato di crittografia nel corso del 2016, soprattutto in contrapposizione alla sicurezza o alla possibilità per i governi o le forze dell'ordine di forzare le comunicazioni per poterne acquisire il contenuto. Per fronteggiare il terrorismo o altri gravissimi crimini si è discusso della possibilità di introdurre o creare delle backdoor nei nostri smartphone, dei passe-partout virtuali in grado di consentire alle forze dell'ordine o ai servizi segreti di "aprire" le nostre comunicazioni, le nostre agende, le nostre rubriche di contatti.

Lo scontro più famoso è certamente stato quello che ha opposto Apple all'FBI, ove a lungo si è discusso dei rischi connessi all'indebolimento della crittografia, e dei costi (in termini non solo economici, ma anche di sicurezza) dell'operazione (del tutto nuova nel suo genere) che apparivano, sul lungo termine, ben maggiori dei benefici.

Anche nel Regno Unito, durante la procedura di approvazione dell'IPBILL, tuttavia, si è assistito a un'aspra contrapposizione: le innumerevoli osservazioni alla bozza, presentate non solo dai giganti della Silicon Valley ma anche da attivisti e associazioni di difesa dei diritti umani, non si limitavano a porre sul piatto della bilancia privacy e sicurezza (anch'essa paradossalmente minata da proposte che ne sbandieravano la tutela) ma si estendevano alla libertà di espressione e alla tutela dei diritti inviolabili dell'uomo.

La crittografia è stata al centro del dibattito quindi, ma la discussione era incentra su interessi di rilevanza nazionale o sovranazionale, e poteva apparire lontana dalle istanze dei comuni cittadini. Eppure certamente ha contribuito ad alzare la sensibilità verso un tema che prima era noto solo agli addetti ai lavori, se è vero che, negli USA post elezioni,

la vittoria di Trump ha fatto registrare un incremento della domanda di servizi di comunicazione crittografati.

La crittografia nella normativa italiana

Davvero esiste una contrapposizione tra sicurezza e privacy che si combatte sul terreno della crittografia? Se guardiamo alla normativa italiana, in realtà sembra vero il contrario: alla crittografia si ricorrere per proteggere alcune particolari categorie di dati, che per la loro importanza e i rischi connessi alla loro perdita o sottrazione richiedono maggiori cautele.

Alla crittografia o cifratura, infatti, si fa cenno nel **Codice Privacy** (seppure in alternativa all'adozione di codici identificativi) all'art. 22 in ordine al trattamento di **dati sensibili e giudiziari,** all'art 34 in relazione ai trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari, e ancora nell'allegato B del Codice ove al punto 22 sotto la rubrica "Ulteriori misure in caso di trattamento di dati sensibili o giudiziari" si dispone che il **trasferimento dei dati genetici in formato elettronico è cifrato**.

È anche vero che, se, da un lato, le misure minime, imposte direttamente dal legislatore, sono obbligatorie, quelle idonee, invece, dipendono dalla sensibilità del titolare e dalla sua determinazione a sfuggire alle responsabilità civili derivanti da patologie del trattamento. Quella che nell'ottica delle misure minime appare una valida alternativa, nell'ottica delle misure idonee può apparire un'opportuna coesistenza.

La crittografia compare come misura di sicurezza in numerosi **provvedimenti del Garante** (se ne citano alcuni senza pretesa di esaustività): si fa cenno alla cifratura nel Provvedimento su Sicurezza dei dati di traffico telefonico e telematico – 17 gennaio 2008 [1482111], nel Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach) – 4 aprile 2013 [2388260], nel Provvedimento in materia di misure di sicurezza nelle attività di intercettazione da parte delle Procure della Repubblica – 18 luglio 2013 [2551507], nel Provvedimento generale

prescrittivo in tema di biometria – 12 novembre 2014, nelle Linee guida sul dossier sanitario elettronico [doc. web n. 4084632] 4 giugno 2015, in quello in ordine alle Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche – 2 luglio 2015 [4129029]. Non solo: il Garante raccomanda l'uso della crittografia anche nel cloud computing e vi accenna, seppure in modo informale, in ordine all'internet of things; il ricorso a tecniche di cifratura, infine, compare in molti provvedimenti tarati su casi concreti portati alla sua attenzione.

La crittografia pertanto non dovrebbe essere una misura di sicurezza del tutto ignota ai titolari italiani; soprattutto la grande diffusione del ransomware nell'ultimo anno avrebbe dovuto incoraggiare il ricorso a misure di protezione idonee: non sappiamo infatti, se pagando i "riscatti" richiesti per rendere nuovamente accessibili i dati questi tornino nelle esclusiva sfera di controllo del titolare o è possibile che invece gli siano stati sottratti e duplicati, diffusi o venduti. Qualora infatti venissero criptati dati già crittografati, resterebbe l'inconveniente di doverli ripristinare, ma se i dati venissero sottratti potrebbero restare efficacemente inintellegibili per i malintenzionati, riducendo il rischio di violazioni.

La crittografia nella normativa europea

La Direttiva 95/46/CE invece non faceva direttamente riferimento a tecniche di cifratura: l'articolo 17, rubricato "Sicurezza dei trattamenti" imponeva, in pratica, al Titolare l'attuazione di "misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali". Tali misure avrebbero dovuto "garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere".

La protezione dei dati e la sicurezza informatica non sono campi perfettamente coincidenti, e la sicurezza dei dati personali veniva tratteggiata in maniera generica, considerando nel bilanciamento da operare anche i costi materiali da sostenere.

Di interesse per il tema che si tratta appare il **"Manuale sul diritto europeo in materia di protezione dei dati"** elaborato nel 2014 da European Union Agency for Fundamental Rights (FRA), Corte europea dei diritti dell'uomo e Consiglio d'Europa (organi distinti quindi dall'UE) sulla scorta della considerazione che in ordine alla materia della protezione dei dati personali "L'Europa vanta uno dei sistemi più all'avanguardia in questo ambito, basato sulla **Convenzione n. 108 del Consiglio d'Europa,** sugli strumenti giuridici dell'Unione europea (UE) nonché sulla giurisprudenza della Corte europea dei diritti dell'uomo (Corte EDU) e della Corte di giustizia dell'Unione europea (CGUE)" e che "con l'entrata in vigore del **trattato di Lisbona,** nel dicembre 2009, la Carta dei diritti fondamentali dell'Unione europea è divenuta giuridicamente vincolante e con essa **il diritto alla protezione dei dati personali è assurto a diritto fondamentale a sé stante.** La tutela di questo diritto fondamentale esige una migliore comprensione della Convenzione n. 108 del Consiglio d'Europa e degli strumenti giuridici dell'Unione europea (UE), che hanno creato i presupposti per la protezione dei dati in Europa, nonché della giurisprudenza della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo".

Nel Manuale si tratta della crittografia come misura utile alla pseudonimizzazione: "Le informazioni personali contengono elementi identificativi come nome, data di nascita, sesso e indirizzo. Quando le informazioni personali vengono pseudonimizzate, gli elementi identificativi sono sostituiti da uno pseudonimo, che si ottiene, per esempio, crittografando gli elementi identificativi contenuti nei dati personali". Il dato pseudonimo è diverso dal dato anonimo: "i dati sono anonimizzati quando non contengono più alcun mezzo identificativo, mentre **sono pseudonimizzati se i mezzi identificativi sono criptati**".

Nel Manuale si dà atto del fatto che i dati pseudonimizzati non siano stati esplicitamente menzionati nelle definizioni giuridiche della Convenzione n. 108 o nella direttiva sulla protezione dei dati. Tuttavia si ritiene che la pseudonimizzazione rappresenti uno degli strumenti più importanti per ottenere la protezione dei dati su larga scala, laddove non si possa evitare completamente l'uso di dati personali.

Pertanto, nel manuale si rileva che "**l'articolo 42 del rapporto esplicativo alla Convenzione n. 108** stabilisce che "l'obbligo relativo ai termini per la conservazione dei dati in forma nominativa non significa che i dati debbano essere dopo qualche tempo irrevocabilmente separati dal nome della persona cui si riferiscono, ma soltanto che non dovrebbe essere possibile collegare facilmente i dati e gli elementi identificativi". Si tratta di un effetto che può essere ottenuto mascherando i dati mediante uno pseudonimo. Per chiunque non sia in possesso della chiave di decifratura, i dati pseudonimizzati sono identificabili con difficoltà; il collegamento a un'identità esiste ancora sotto forma di pseudonimo associato alla chiave di decifratura. Chi ha diritto a utilizzare la chiave di decifratura è in grado di risalire all'identità. **Occorre prestare particolare attenzione onde evitare l'uso di chiavi crittografiche da parte di persone non autorizzate**.

Si tratta di un aspetto molto importante, anche alla luce di quanto si dirà in ordine al Regolamento Generale sulla Protezione dei dati adottato in UE. Se la crittografia viene fatta poggiare sulla base della Convenzione 108, infatti, il novero dei soggetti internazionali tenuti ad adottarla si amplia e la sua efficacia come strumento di protezione travalica i limiti dell'Unione.

La crittografia nel Regolamento generale sulla protezione dei dati

Una novità importante, nel ravvicinamento tra protezione dei dati personali e cybersecurity si ha con il Regolamento Europeo. La crittografia, ad esempio, **viene menzionata diverse volte nel Regolamento**: si tratta di uno strumento di cui il titolare e il responsabile possono avvalersi per **mitigare i rischi connessi ai trattamenti** (fatto che, in ottica di accountability, va tenuto in adeguata considerazione). Si fa riferimento alla

crittografia ad esempio nel considerando n. 83 ove si dispone che "Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura". Il considerando viene poi tradotto nell'articolo 32 del regolamento medesimo, che, collocato nella sezione riferita alla sicurezza dei dati personali e rubricato sicurezza del trattamento dispone che "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali" (...).

La pseudonimizzaione e la cifratura, pertanto, sono misure che il titolare deve tenere in considerazione quando valuta i rischi di sicurezza ai quali sono concretamente esposti i dati e opera per predisporre un livello di sicurezza adeguato al rischio.

Nella medesima sezione si trova anche l'art. 34, che, pure, menziona la crittografia. In particolare, l'articolo 34 disciplina la "Comunicazione di una violazione dei dati personali all'interessato", come illustra efficacemente la sua rubrica. Ebbene, cosa esonera dal comunicare all'interessato il data breach? La cifratura! Dal comma 3 lettera a) infatti si deduce che **non è richiesta la comunicazione all'interessato** sei titolare "ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura". I vantaggi sul piano dell'immagine aziendale e della competitività rispetto ai concorrenti potrebbero essere significativi.

Un riferimento alla cifratura è contenuto anche nell'articolo 6 del Regolamento, in ordine alla liceità del trattamento. Nel caso in cui il titolare raccolga dei dati personali ma voglia

poi trattarli **per una finalità diversa** da quella per la quale siano stati originariamente raccolti, e non abbia il consenso dell'interessato o non possa fondarsi su una norma di legge, dovrà valutare che questa seconda finalità sia compatibile con la prima. Per compiere questa valutazione il titolare del trattamento tiene conto, tra l'altro, a norma del comm 4 lettera e) "dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione"

Il ricorso alla cifratura, perciò, assume grande rilievo nell'ambito del Regolamento: e molto viene lasciato all'iniziativa dei titolari, in un bilanciamento che sarà certamente rilevante in termini di responsabilità. Pertanto è possibile che si affermi come prassi consueta. Non solo: limitare la crittografia, pretendere la creazione di backdoor, indebolirla o infrangerla significa minare la protezione dei dati personali, diritto fondamentale dell'Unione, e mettere a repentaglio uno strumento che poggia sull'ampia base offerta dalla Convenzione 108. Si tratta di una barriera importante per il legislatore nazionale, figuriamoci per gli operatori privati: indebolire occultamente la crittografia senza una norma di legge che (pure con le cautele che si sono dette) autorizzi a ciò pare a chi scrive un illecito, che può esporre a conseguenze significative. Eludere o non adottare affatto la crittografia nei sistemi di comunicazione potrebbe invece rivelarsi una fonte importante di responsabilità.

Penetration test

Parlando di cifratura e pseudonimizzazione è obbligato il richiamo al Parere reso dal Gruppo di lavoro art. 29 n. 6/2013 sui dati aperti e sul riutilizzo delle informazioni del settore pubblico ("ISP"), ove in ordine alle procedure di pseudonimizzazione e anonimizzazione si evidenziava l'esigenza (che non può restare confinata a uno specifico settore, specie nel mutato quadro normativo) di **evitare i rischi di reidentificazione.** Il WP29 evidenziava come in alcune circostanze può essere difficile determinare il rischio di reidentificazione, in particolare quando c'è la possibilità che un terzo si serva di metodi statistici complessi per abbinare diversi dati anonimizzati. Pertanto, nel quadro di una valutazione globale per individuare il rischio di reidentificazione, è buona prassi ricorrere

al test di reidentificazione – una sorta di test di penetrazione – per rilevare e risolvere le vulnerabilità. Il Gruppo evidenzia come tale test non sia una panacea e non metta al riparo il titolare una volta per tutte: **il rischio di reidentificazione può variare nel tempo**, in base agli strumenti e alle tecniche di analisi dei dati che si hanno a disposizione ma che divengono sempre più potenti e abbordabili. Pertanto occorre rivedere periodicamente le policy adottate in merito e non bisognerebbe mai basare le proprie decisioni soltanto su minacce attuali, ma anche su minacce future prevedibili.

Si tratta evidentemente di suggerimenti facilmente mutuabili e adattabili al quadro delineato dal Regolamento Generale.

Già da qui si comprende come la crittografia non possa costituire l'unico presidio di sicurezza informatica attratto nella sfera di operatività della protezione dei dati personali dal Regolamento Generale.

Con maggiore attenzione occorrerebbe cominciare a familiarizzare anche con i **penetration test** generalmente intesi. Se infatti riprendiamo l'art 32 sopra citato sulla "Sicurezza del trattamento" vediamo che tra le misure di protezione adeguate che il titolare e il responsabile debbono adottare si trovano sia la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la *resilienza* dei sistemi e dei servizi di trattamento, sia l'adozione di una **procedura per *testare*, verificare e *valutare regolarmente l'efficacia* delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.**

Si tratta di procedure che andranno certamente valutate sulla scorta del principio di responsabilizzazione introdotto dal Regolamento, che imporrà un approccio organizzavo e strategico, da inquadrare in apposite linee di bilancio e assistere con adeguata **contrattualistica** (cfr C. 81 e art 28 GDPR), sia che si cerchino soluzioni interne sia che si cerchino soluzioni esterne all'ente titolare. Si accenna appena alle criticità che recano con sé queste pratiche, in ordine alle esigenze di riservatezza (in senso di segretezza), rischi connessi al danneggiamento, riparto delle responsabilità, implicazioni rispetto alla

generale disciplina dei dati personali. Implicazioni che in caso di esternalizzazione, si aggiungono all'obbligo di **selezionare un idoneo contraente**: come ricorda il considerando 81 del Regolamento, infatti, "*il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento*" (cfr anche Articolo 28- Responsabile del trattamento). Peraltro, ove si operi in ambiti innovativi, questi aspetti andranno contemperati con i **principi di privacy by design**, ossia con l'implementazione della protezione dei dati personali sin dalla progettazione. E, come è intuitivo, se la protezione dei dati include anche risorse ascrivibili all'ambito della sicurezza informatica, come crittografia e penetration test, occorrerà leggere la privacy by design anche come **security by design,** come ha già suggerito qualche attento commentatore.

I primi passi da muovere verso l'adeguamento al Regolamento generale sulla protezione dei dati, pertanto, passano anche dal terreno più solido delle buone prassi (e non da quello paludoso delle vacue parole) della sicurezza informatica.