

Premessa: La libertà non è uno spazio libero (cit G.Gaber)

L'essenza della legalità è l'osservanza delle leggi e la tutela dei diritti in caso di violazione.

Rispettare le leggi, le regole, i principi giuridici, è un limite o è una condizione per la libertà?

In realtà, il loro rispetto è la condizione di una libertà ordinata: l'alternativa è la legge del più forte, che pretende che la sua libertà non sia ostacolata da quella degli altri, con il conseguente venir meno della tutela delle persone vulnerabili e dell'uguaglianza di condizioni per tutti.

Ogni libertà deve quindi incontrare dei limiti, altrimenti ci sarebbe la prevaricazione di una sulle altre. I diritti esistono, sono le fondamenta della costruzione sociale, ma sono tutti sempre limitati, anche quelli che chiamiamo diritti assoluti.

Violazione dei diritti e sicurezza

Se gli altri possono impunemente violare i miei diritti, sono libero? Quale sarà la mia sensazione se sono consapevole che chi mi aggredisce non potrà essere individuato, mi sentirò sicuro? La sicurezza ha un ruolo centrale:

“La sicurezza è uno dei diritti naturali ed imprescrittibili dell'uomo” art. 2 Dichiarazione dei diritti dell'uomo e del cittadino - 1789

“Ogni persona ha diritto alla libertà e alla sicurezza” art. 5, Diritto alla libertà e alla sicurezza - Convenzione Europea dei Diritti dell'Uomo

L'insicurezza e la paura possono essere ricompresi tra gli ostacoli di ordine sociale che impediscono il pieno sviluppo della persona umana: è compito della Repubblica rimuoverli (art.3 co 2 cost). Più che un diritto autonomo, tuttavia, credo che la sicurezza possa considerarsi la sfera esterna protettiva dei diritti, relativa alla loro fase dinamica.

Non è una deminutio: si tratta, infatti, di un elemento imprescindibile di ogni diritto civile, una condizione o una preconditione per il suo esercizio.

C'è uno stretto legame tra la sicurezza, il rispetto delle regole e la concreta possibilità di sanzionare chi le viola.

Il compito di far rispettare le regole deve essere affidato allo Stato, che deve far sì, impiegando uno sforzo ragionevole, che sia individuabile il responsabile di una violazione: è centrale in questo contesto l'art. 111 co. 3 Cost., che attribuisce alle parti il potere di ricercare le fonti e di chiedere al giudice l'ammissione del relativo mezzo di prova.

Il mezzo adottato dallo Stato per raggiungere lo scopo deve essere il meno invasivo per le libertà personali e sociali: le libertà, infatti, non devono essere compresse in modo ingiustificato. Ciò vale naturalmente anche per la libertà di comunicazione e per i dati personali ad essa associati: la conoscenza e il trattamento di questi dati da parte di soggetti diversi da quelli cui si riferiscono e da chi li elabora per fornire il servizio di comunicazione è possibile solo a determinate condizioni. La possibilità per gli investigatori di acquisire i dati esterni delle comunicazioni, invadendo la sfera di libertà di coloro che hanno commesso una violazione, è tuttavia un passaggio quasi sempre essenziale per individuare il responsabile dell'illecito e rendere effettivo il principio di legalità.

Con l'avvento della rete ed il moltiplicarsi delle comunicazioni digitali la questione della conservazione dei dati personali esterni alle comunicazioni costituisce un punto cruciale per l'accertamento non solo dei reati ma, in generale, dei responsabili delle violazioni dei diritti. È indubitabile che la data retention sia il punto di frizione principale tra la privacy e la sicurezza e che sia particolarmente complesso trovare un punto di equilibrio, tuttavia sia la CGUE che il Garante privacy non sembrano aver seguito un percorso logico coerente, spesso trascurando gli eventuali riflessi negativi sul principio di legalità.

Data retention nelle pronunce della Corte di Giustizia dell'Unione europea

La normativa dell'Unione europea è declinata in numerose e incisive sentenze della Corte di giustizia dell'Unione, la più recente delle quali ha esaminato la modifica avvenuta nel 2021 dell'art 132 del codice privacy

La decisione più importante della Corte è sicuramente l'invalidazione nel 2014 di tutta la Direttiva 2006/24/CE - direttiva Frattini -, perché imponeva una conservazione dei metadati indiscriminata e sproporzionata rispetto alla tutela della vita privata. A questo punto, il riferimento in materia tornava ad essere la precedente Direttiva 2002/58, in particolare le seguenti prescrizioni:

art 5 - prevede l'obbligo per gli Stati membri di assicurare la riservatezza delle comunicazioni, nonché dei relativi dati sul traffico;

art.6 - prevede in linea generale la loro cancellazione o anonimizzazione quando non più necessari ai fini della trasmissione di una comunicazione, facendo salvi:

- i trattamenti ai fini della fatturazione per l'abbonato e dei pagamenti di interconnessione (per un periodo limitato)
- i trattamenti fatti per la commercializzazione dei servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto per cui sia stato prestato un consenso informato

art 15, paragrafo 1: «**Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva [95/46], una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica.** A tal fine gli Stati membri possono tra l'altro adottare misure legislative, le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo....»

L'interpretazione dell'art 15 dell Direttiva 2002/5 è un punto cruciale, perché la Corte è arrivata a modificare il dettato letterale della norma attraverso la sua lettura alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, cosicché solo la finalità di lotta alla criminalità **grave** e di prevenzione delle minacce **gravi** alla sicurezza pubblica, consentono la conservazione preventiva generalizzata e indifferenziata dei dati relativi al traffico e all'ubicazione. In poche righe, inserendo l'aggettivo grave, si escludeva l'utilizzo di uno strumento per contrastare le minacce alla sicurezza e i crimini di media e bassa pericolosità

Qui va sottolineata una palese incongruenza: la delimitazione alla sola criminalità "grave" delle ipotesi in cui è possibile acquisire i dati esterni alle comunicazioni non riduce affatto il numero di dati conservati e gli

interessati a cui si riferiscono (non possono prevedersi in anticipo i legami reato - comunicazione e i soggetti coinvolti: dovranno conseguentemente essere conservati i metadati di tutte le comunicazioni) e, quindi, non ci sono minori rischi di perdita o trattamento illecito; la capacità di ricerca della prova, invece, viene considerevolmente ridotta per molti reati e, con essa, la possibilità di individuazione del responsabile della violazione.

Nel nostro ordinamento, l'interpretazione restrittiva della Corte di Giustizia Europea è stata recepita nel 2021 con una modifica al comma 3 dell'articolo 132 del codice privacy, facendo sì che - con la sola eccezione di due ipotesi (minaccia e di molestia o disturbo alle persone) - solo le fattispecie sanzionate con la reclusione non inferiore nel massimo a tre anni è possibile acquisire i dati relativi al traffico.

Paradossalmente, uno dei reati per i quali non è possibile acquisire i metadati è la sostituzione di persona, una delle principali ipotesi di trattamento illecito e una vera e propria fattispecie "spia", in Internet, di ulteriori reati in corso di preparazione; in buona sostanza, la privacy dell'aggressore è tutelata a scapito di quella della vittima, con un considerevole vulnus del principio di legalità.

LA CGUE ritiene tuttavia ammissibile la conservazione "mirata" di metadati prodotti da comunicazioni telefoniche, limitata nel tempo e basata su minacce gravi e reali alla sicurezza pubblica, purché soggetta a revisione giudiziaria o amministrativa indipendente. In merito a tale conservazione mirata, lascia tuttavia interdetti quanto riportato nella sentenza del 5 aprile 2022 dalla Grande Sezione, punto 79, per sostenere una sua valida modalità di attuazione: «Dall'altro lato, una misura di conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione può, a seconda della scelta del legislatore nazionale e nel rigoroso rispetto del principio di proporzionalità, essere fondata anche su un criterio geografico qualora le autorità nazionali competenti ritengano, sulla base di elementi oggettivi e non discriminatori, che sussista, in una o più zone geografiche, una situazione caratterizzata da un rischio elevato di preparazione o di commissione di atti di criminalità grave. Tali zone possono essere, in particolare, luoghi caratterizzati da un numero elevato di atti di criminalità grave, luoghi particolarmente esposti alla commissione di atti di criminalità grave, quali luoghi o infrastrutture frequentati regolarmente da un numero molto elevato di persone, o ancora luoghi strategici, quali aeroporti, stazioni o aree di pedaggio».

In verità, una simile conservazione mirata sembra integrare, di per sé, una misura discriminatoria basata su un pregiudizio, che ghettonizza i soggetti che frequentano le aree selezionate e può creare sacche di impunità al loro esterno.

Certezza del diritto e definizioni stabilite dal Garante privacy

Il Garante privacy italiano ha seguito una linea interpretativa conforme alle pronunce della Corte di giustizia europea, ma in un caso è andato ben oltre: un provvedimento datato 17 gennaio 2008 ha prodotto notevoli difficoltà alla lotta alla criminalità organizzata, in quanto prevedeva l'esclusione degli indirizzi Ip di destinazione dai dati oggetto di conservazione, prima pacificamente considerati dagli operatori come esterni alla comunicazione e, quindi, da conservare obbligatoriamente.

Per le comunicazioni telematiche, il Garante ravvisa, in sostanza, specifiche criticità, «in quanto il dato apparentemente "esterno" a una comunicazione (ad es., una pagina web visitata o un indirizzo Ip di destinazione) spesso identifica o rivela nella sostanza anche il suo contenuto: può permettere, quindi, non solo di ricostruire relazioni personali e sociali, ma anche di desumere particolari orientamenti, convincimenti e abitudini degli interessati»

Ne consegue che il dato deve essere assimilato al contenuto della comunicazione, che è escluso dalla conservazione per finalità di giustizia.

Secondo questo ragionamento, accanto ai dati propriamente esterni ed a quelli costituenti il nucleo della comunicazione, si potrebbe ipotizzare un *tertium genus* creato dal Garante, formato da dati, definiti apparentemente esterni, da cui si può desumere il contenuto e, pertanto, a questo assimilabili in quanto a regole di conservazione.

Si realizza, così, un paradosso: una parte della comunicazione, formata da informazioni prodotte automaticamente dalle apparecchiature del circuito telematico, pur essendo considerata contenuto, è del tutto sconosciuta a chi la invia o la riceve.

Da un punto di vista sostanziale, va sottolineato che il contenuto di una pagina web consultato ad una determinata ora della giornata non dà alcuna sicurezza su quanto contenuto il giorno od il mese precedente, perché, come è stato giustamente osservato, una cosa sono le informazioni consultate - che sono effettivamente equiparate al contenuto ai sensi della direttiva 2006/24/CE e del d. lgs. n. 109 /2008 - e un'altra è il sito visitato dall'utente: la «volatilità e la modificabilità dei contenuti amministrati dai siti o dai gestori che diffondono contenuti sulla rete (cd. content provider) escludono che si abbia conservazione di informazioni nel caso in cui si custodisca memoria dell'indicazione del solo URL di destinazione o dell'IP address nella navigazione" (v. S. Aterno).

In definitiva il provvedimento, attraverso una qualificazione dei dati che sembra andare al di là delle proprie competenze, ha provocato la modifica del quadro normativo di procedura penale applicabile.

È frutto anche dell'accostamento, operato talvolta dal Garante privacy italiano e dalla Corte di giustizia dell'Unione europea, tra monitoraggio e profilazione, da una parte, e conservazione dei metadati dall'altra, perché lascia indurre la concreta possibilità che sulle informazioni memorizzate a fini di giustizia si possa operare un'attività di controllo a fini politici o commerciali a discapito della collettività o di gruppi selezionati di persone.

Anche i rischi connessi all'attività di mera conservazione dei dati esterni sono troppo spesso sopravvalutati; in realtà, tra tutti i trattamenti, la conservazione si caratterizza per essere un'attività statica, non soggetta ai pericoli ben più elevati connessi al passaggio delle informazioni tra due apparati.

Non è un caso se per questa specifica attività di conservazione non si sono registrati presso i provider casi massivi di data breach, compromissione o perdita di informazioni digitali nel contesto italiano ed europeo; ben diversa si presenta la situazione dei dati (e dei contenuti) gestiti da società private a fini commerciali, coinvolte massicciamente in scandali quali il Datagate/Wikileaks o Cambridge Analytica.

Decisioni del Garante privacy sulla conservazione a fini commerciali

In alcuni provvedimenti del Garante privacy italiano sembra emergere un'attenzione per il periodo di conservazione dei dati a fini commerciali tendenzialmente benevola, comunque lontana dal rigore mostrato nei confronti delle scelte del legislatore in materia di durata della conservazione dei dati esterni alle comunicazioni per finalità di giustizia.

Alcune importanti società commerciali si sono rivolte, tra il 2013 ed il 2016 all'autorità indipendente per presentare un'istanza di verifica preliminare ai sensi dell'art. 17 del codice privacy (ora abrogato a seguito dell'introduzione del Nuovo Regolamento Generale Europeo) concernente il trattamento di dati della

propria clientela per finalità di profilazione e marketing per un periodo superiore, rispettivamente, a dodici e ventiquattro mesi; pur trattandosi di dati ottenuti con il consenso informato degli interessati, è chiaro che esiste un limite temporale per il loro utilizzo a fini commerciali.

La richiesta più significativa, tesa a conservare e trattare i dati riferiti alla clientela propria e a quella dei propri "affiliati" per un periodo pari a venti anni, è stata avanzata nel 2016 da una primaria società presente in Italia nel settore dell'intermediazione immobiliare, attraverso circa 1700 soggetti operanti in franchising (definiti "affiliati") sotto la direzione ed il coordinamento da parte di una holding s.p.a.; alla stessa holding fa capo una ulteriore società operante nello stesso settore, attraverso circa 350 affiliati.

Molto ampia la mole di dati coinvolti: anagrafici, categorizzazione (secondo le tipologie: famiglia, studi, lavoro), dati di contatto (numero di telefono e indirizzo email), residenza e domicilio, informazioni sulla composizione del nucleo familiare, provenienza dei dati, informazioni qualitative e quantitative in merito alle proprietà immobiliari (caratteristiche, indirizzo, coordinate geografiche), dati su interessi del proprietario a vendere o affittare.

Il Garante, esaminata la richiesta ed in particolare le misure di sicurezza predisposte, ha ritenuto che i dati in questione potessero essere conservati per un periodo massimo pari a 15 anni, decorrente dalla registrazione degli stessi, ritenendo tale arco temporale congruo e proporzionato alle finalità che si intendono realizzare con il trattamento. Un arco temporale così lungo, considerando la considerevole quantità di dati immagazzinati raccolti anche solo per generiche richieste di clienti non sfociate in contratti di acquisto o affitto, sembra sproporzionato in relazione alle esigenze di minimizzazione dei trattamenti.

Una sorta di ravvedimento operoso delineato nella motivazione di un provvedimento sanzionatorio

Anche in casi più recenti, con il GDPR applicato in modo consolidato, il Garante è sembrato eccessivamente indulgente nell'intervento sanzionatorio susseguente ad un data breach che ha riguardato dati particolari di natura sanitaria.

Il problema ha coinvolto ASL 1 di Avezzano, Sulmona, L'Aquila, vittima nel 2023 di un attacco ransomware che ha reso indisponibili i sistemi informatici, con esfiltrazione di dati personali contenuti nei database violati e, richiesta di riscatto. Allo scadere del termine, stante l'avvenuto mancato pagamento da parte dell'ASL, gli attaccanti hanno rilasciato sul dark web l'intero contenuto dell'esfiltrazione: ci sarebbero cartelle cliniche, referti di analisi genetiche, valutazioni psicologiche di minori documenti di inventario e modelli e schemi documentali che gli ambulatori e gli uffici dell'ASL utilizzavano per rilasciare certificazioni, referti, e documentazione inerente prestazioni mediche. A fronte di circa 300mila cittadini interessati coinvolti e della sensibilità dei dati sottratti, era plausibile aspettarsi una sanzione severa per le carenti misure di protezione adottate dalla struttura sanitaria e per la ritardata comunicazione individuale dei fatti: il Garante Privacy nel febbraio del 2025 si è invece limitato solo ad ammonire "tale titolare del trattamento per aver violato le disposizioni" in ragione della sua cooperazione con l'Autorità "ben oltre l'obbligo previsto dall'art. 31 del Regolamento", un parametro attenuante talmente inconsueto da suscitare sospetti nell'ambito di un'inchiesta giornalistica che ha suscitato grande clamore.

Indeterminatezza degli obblighi cui sono tenuti i titolari dei trattamenti

Si deve infine far riferimento a due controversi documenti di indirizzo del Garante relativi ai programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e nel trattamento dei metadati, che hanno indicato un termine relativamente breve per la loro conservazione, senza motivare il metodo usato per determinare tale durata massima.

Nel primo, datato 21 dicembre 2023, si stabiliva che i metadati delle comunicazioni di posta elettronica dei dipendenti possono essere conservati dai datori di lavoro, al massimo, per 7 giorni, prorogabili con motivate ragioni per ulteriori 48 ore. Alcune incertezze riguardavano l'ampiezza dei dati coinvolti, in quanto erano ricompresi i "metadati generati e raccolti automaticamente dai protocolli di trasmissione e smistamento della posta elettronica e relativi alle operazioni di invio, ricezione e smistamento dei messaggi di posta elettronica."

La questione principale è se il Garante può introdurre liberamente termini di conservazione dei dati personali di portata generale e preventiva in assenza di un'indicazione normativa che assegni tale potere: ne consegue che in questo caso non sono circoscritte le prescrizioni che si è tenuti ad osservare. In realtà, secondo il GDPR, compete al titolare del trattamento/datore di lavoro stabilire i termini di conservazione dei dati personali, non all'autorità di controllo. Ogni titolare del trattamento li potrà stabilire in maniera diversa, motivando il termine scelto in base alla finalità. Va sottolineato che la norma base del provvedimento di indirizzo, ossia il comma 1, lett. a) dell'art. 154-bis cod. priv. non consente contenuti prescrittivi: il legislatore parla chiaramente di "linee guida", è possibile quindi solo il chiarimento della disciplina in vigore.

I dubbi e le reazioni negative seguite al documento di indirizzo indussero ben presto lo stesso Garante a sottoporre la questione a consultazione pubblica, a seguito della quale è stato emanato il 6 giugno 2024 un ulteriore documento di indirizzo, che delinea meglio tempi di conservazione e campo di applicazione.

Il limite è stato fissato ora in 21 giorni, la conservazione per un periodo più lungo è possibile, ma richiede una giustificazione specifica, la redazione di una Valutazione d'Impatto (DPIA) e la dimostrazione della necessità e della proporzionalità. Ancora una volta, non viene però data una motivazione specifica per l'indicazione di questo preciso periodo temporale, con cui il Garante si sostituisce al titolare del trattamento nella determinazione dei tempi di conservazione. Anche se l'indicazione del termine è "a titolo orientativo" e si precisa che il documento "non reca prescrizioni né introduce nuovi adempimenti a carico dei titolari del trattamento" sembra difficile pensare che un datore di lavoro e i lavoratori interessati non la considerino una regola vincolante a tutti gli effetti.

Come anticipato, in questo suo secondo documento il Garante perimetra il campo di applicazione ai metadati delle email "corrispondono tecnicamente alle informazioni registrate nei log generati dai sistemi server di gestione e smistamento della posta elettronica (MTA = Mail Transport Agent) e dalle postazioni nell'interazione che avviene tra i diversi server interagenti e, se del caso, tra questi e i client", specificando che non si applica alle comunicazioni di posta elettronica presenti nella casella dei dipendenti.

In definitiva, il fatto che il termine di 21 giorni non fosse previsto da alcuna norma crea una situazione di incertezza sugli obblighi cui sono tenuti i titolari coinvolti, con una sorta di determinazione della fattispecie comportamentale ex post: in precedenza il titolare del trattamento sapeva che in osservanza del GDPR, doveva stabilire i termini di conservazione di questi dati personali in base a finalità, tipologia e contesto. Non c'è dubbio poi che, ai fini della certezza del diritto, la determinazione di un termine temporale preciso attraverso un documento la cui finalità deve essere solo quella di rendere chiaro un quadro normativo sia la modalità meno appropriata; sembra quanto mai opportuno un intervento legislativo che definisca meglio il perimetro delle competenze del Garante privacy.

