LA RISERVATEZZA CORRE SUL FILO

Le principali novità in arrivo. Terrorismo, cyberwarfare e intercettazioni.

Alla luce della recente riforma del codice penale e di procedura penale entrata in vigore con la Legge n. 103 del 23/6/2017, si sono viste modificate anche le regole che normano le intercettazioni e il loro uso o abuso ai fini processuali. Si tratta del labile confine tra il diritto (sancito insieme a quelli fondamentali nella nostra stessa Costituzione) alla Privacy e quello processuale di giustizia. **Con la stretta all'utilizzo delle intercettazioni ai fini processuali si vede sì riconosciuto il diritto alla secretazione di notizie considerate non rilevanti ai fini processuali ma è vero anche che questo comporti delle serie limitazioni ai fini delle indagini** (si pensi, ad esempio, ai processi per mafia, per i quali l'utilizzo di tale strumento gioca una posizione rilevante e di fondamentale importanza nel corso delle indagini utili a reperire fonti probatorie e notizie di reato).

Questo, se da un lato giustamente tutela tutte le parti che, anche solo per incidenza, possano essere inserite in una conversazione captata, dall'altro limita la strumentazione necessaria in sede processuale.

Tutte le notizie e le conversazioni captate che non si ritengano rilevanti ai fini del processo penale dovranno quindi essere secretate e riversate in appositi server a cura della Procura. Con la riforma è stato inoltre previsto un nuovo reato inerente la diffusione di immagini o registrazioni fraudolentemente acquisite con l'obiettivo di danneggiare l'altrui reputazione, salvo che tale utilizzo non sia fatto in sede di difesa giudiziaria.

Quel che è importante qui rilevare è l'utilizzo di tali strumenti anche ai fini giornalistici. **Secondo il codice deontologico dei giornalisti**, infatti, **è previsto che si debbano fornire notizie rispondenti a verità e si debbano correggere eventuali errori** di notizie precedentemente fornite non correttamente. **Il giornalista deve difendere i diritti all'informazione e alla libertà di opinione ma deve rispettare i principi fondamentali delle persone** (e con esso è inteso anche quello alla riservatezza degli individui coinvolti). Deve altresì rispettare il diritto all'identità personale senza far riferimento a eventi passati e, nel diffondere a distanza di tempo dati identificativi dei condannati, deve valutarne l'incidenza ai fini del reinserimento sociale. Non deve pubblicare nomi o immagini di coloro i quali abbiano subito violenze sessuali, né fornire particolari che possano portare alla loro identificazione. Il codice deontologico dei giornalisti, infatti, tiene in stretta considerazione, e a esso è legato a doppia mandata, il vecchio (quasi al traguardo pensionistico, almeno lui) codice Privacy Dlgs 196/2003 che sarà a breve sostituito dal novello 679/2016, il cui debutto è previsto in data 25/5/2018.

In merito ai doveri di informazione dei giornalisti inerenti notizie di cronaca giudiziaria, essi devono sempre rispettare il diritto alla presunzione di non colpevolezza. Si deve osservare la massima cautela nel diffondere immagini di persone incriminate per reati minori e, con l'entrata in vigore della riforma del codice penale, occorrerà una cautela ulteriore. Gli atti dovranno essere custoditi in archivio riservato, così come poc'anzi menzionato.

Si deve osservare la massima cautela nel diffondere immagini di persone incriminate per reati minori e, con l'entrata in vigore della riforma del codice penale, occorrerà una cautela ulteriore.

La riforma tende a garantire la riservatezza delle comunicazioni e delle conversazioni telefoniche e telematiche oggetto di intercettazione e viene disciplinato altresì l'utilizzo dei cosiddetti "Trojan Horses".

Con tale riforma, infatti, si tende a garantire la riservatezza delle comunicazioni e delle conversazioni telefoniche e telematiche oggetto di intercettazione e viene disciplinato altresì l'utilizzo dei cosiddetti "Trojan Horses".

A tal proposito, ad esempio, i captatori informatici in dispositivi elettronici portatili potranno essere attivati (nel caso del microfono, ad esempio) solo su comando remoto e dietro autorizzazione del giudice; le registrazioni audio potranno essere avviate solo da parte della polizia giudiziaria e sarà ammessa solo per reati afferenti il 614 cp; come poc'anzi anticipato, le intercettazioni che abbiano coinvolto soggetti estranei ai fatti non potranno essere conoscibili, divulgabili, pubblicabili.

D'altro canto occorre rimarcare come la stretta all'utilizzo delle intercettazioni possa porre anche un freno alla lotta alla criminalità. Ricollegandosi ai Trojan Horses e alle intercettazioni, non si può fare a meno di soffermarsi sul fenomeno dilagante quale il terrorismo. Già, perché se, da un lato, i famosi "cavalli di Troia" possono essere utilizzati dalla Procura nei processi penalmente rilevanti al fine di acquisire fonti probatorie, allo stesso modo **tali strumenti possono essere utilizzati da cybercriminali dediti a quella che ai giorni nostri viene definita "cyberwarfare", ossia "guerra cibernetica"**, combattuta non più "boots on the ground" ma bensì "fingers on PC".

E quel che è peggio, è che **questa guerra è di difficile anticipazione, poiché non è così semplice e scontato rilevare posizioni, intenzioni e mosse nemiche**, soprattutto perché il cyberworld è talmente vasto e pieno di "facili nascondigli" quali TOR e dark net che Bin Laden, in confronto, giocava a nascondino.

Le maggiori minacce cibernetiche, considerate un vero e proprio buco nero e problema di rilevanza strategica nazionale e internazionale sono oggetto di attenzione da parte del nostro comparto dedito alla sicurezza nazionale, come più volte ribadito anche nel Libro Bianco.

Le principali *technicalities* di attacco nella cyber war, o guerra cibernetica, sono costituite da attacchi a infrastrutture critiche, mezzi di comunicazione, attacchi a pagine web, attacchi DDOS, intralcio ad apparecchiature e così via, passando poi allo spionaggio per finire alla guerra psicologica, per sottomettere le masse.

Insomma, il legislatore che ha messo mano al codice Privacy non si è fatto mancare nulla per essere arrivato a produrre un nuovo codice, pronto a debuttare il prossimo 25/5/2018, ossia il 679/2016.

Considerati tutti i rischi legati agli attacchi alle informazioni riservate che riguardano i nostri dati personali, visti tutti i tipi di mezzi (leciti e non) in possesso ai vari soggetti (nemici o meno) che possano ledere tali dati in qualsiasi maniera e, con essi, i diritti a essi connessi, **occorre analizzare nel dettaglio quali siano le incombenze in capo a coloro i quali debbano, in qualsivoglia maniera e per qualsiasi finalità, trattarli**.

La normativa europea 679/2016, come ribadito, entrerà in società in data 25 maggio 2018, momento in cui inizierà a produrre i suoi effetti nel nostro ordinamento, mandando in pensione il nostro caro codice Privacy Dlgs 196/2003.

Passiamo quindi ad analizzare quali saranno le principali novità e le misure che, anche i professionisti che risultino incaricati esterni dai clienti, dovranno attivare.

- Anzitutto occorre ricordare che, per quel che attiene i dati sensibili, **il consenso deve essere sempre esplicito**; non deve essere necessariamente fornito in forma scritta, ma occorre poterlo dimostrare. In tal caso una prima domanda sorge spontanea: se non viene fornito in forma scritta occorrerà pensare a una forma probatoria idonea per poterlo dimostrare?
- Per i **minori**, considerati tali al di sotto dei 16 anni, **il consenso dei genitori si rende sempre necessario**. Si rammenta che **il consenso deve essere libero, specifico e informato e che non sono ammesse spunte precompilate**. I dipendenti pubblici sono, allo stato attuale, esonerati da tale incombenza.
- Verrà poi istituita **una nuova figura, il RPD**, acronimo che sta a indicare "**Responsabile della protezione dei dati**" o DPO "Data Protecion Officer" che avrà funzione di formazione del personale e sorveglianza.

- **Il titolare dovrà specificare l'interesse legittimo dei dati e se gli stessi verranno trasferiti all'estero**. In quest'ultima ipotesi, non sarà più necessario attendere l'autorizzazione dal nazionale per poter trasferire i dati all'estero, purché lo si faccia verso Paesi adeguati stabiliti.
- Nel caso di dati raccolti non direttamente presso l'interessato, l'informativa deve essere fornita entro un termine ragionevole che non può eccedere il mese. L'informativa, inoltre, dovrà essere trasmessa in termini chiari e trasparenti e preferibilmente in formato elettronico.
- I **termini per le risposte all'interessato** passano da un mese dalla richiesta e fino a un massimo di tre.
- Il **diritto all'oblio**, ossia il diritto alla cancellazione dei propri dati personali in forma rafforzata viene altresì contemplato.
- È stato previsto il blocco, diretto alla limitazione del trattamento non solo in caso di violazione dei dati. Una importante novità è afferente alla cosiddetta **portabilità dei dati**, così come la MNP telefonica: in sostanza sarà possibile trasferire i propri dati da un titolare a un altro avverso consenso dell'interessato.
- In merito alle "figure incaricate" è fatto obbligo ai titolari di definire con un atto l'ambito di responsabilità di ciascuno riguardo ai diritti degli interessati.
- Cambierà anche l'approccio delle valutazioni: si passerà infatti a un approccio basato sulla "responsabilizzazione dei responsabili" (si passi il gioco di parole). Dovranno, infatti, provvedere a effettuare le comunicazioni all'Autorità entro le 72 ore successive alla conoscenza della violazione, sulla base della loro percezione del rischio che i dati possano esser considerati "in pericolo". La novità sta nel fatto che, con la nuova normativa, **la notizia della violazione va trasmessa da parte di tutti i titolari e non solo dai fornitori di servizi di comunicazione**. Qualora la percezione del rischio sia elevata, si dovrà dare notizia della violazione anche all'interessato.
- Occorrerà poi **istituire un registro**, ma solo per entità con personale dipendente superiore a 250 unità, che sarà utilizzato al fine di valutare e analizzare il rischio. Deve avere forma scritta o elettronica e deve poter esser fornito in caso di ispezione del Garante.

Con l'adozione del nuovo codice verranno sì snellite alcune procedure e rafforzati i diritti degli interessati, ma verranno altresì implementate le incombenze in capo ai titolari.

Buon lavoro.

Valeria Rosa