Barbara Pandolfino(*)

Quando l'intruso è il sistema antintrusione

Ormai da tempo stiamo assistendo ad una vertiginosa evoluzione del concetto di "sicurezza" inteso come l'insieme delle discipline che si riferiscono, in senso generico, alla sicurezza del territorio, dell'industria e del singolo (nella sua accezione di privato cittadino). In quest'ambito si inseriscono i più accurati e sofisticati sistemi di tecnologia hi-tech che dovrebbero rispondere ad esigenze di controllo e di sicurezza, senza mai dimenticare l'imprescindibile obbligo di coniugare la privacy dei soggetti coinvolti con la protezione dei dati, delle strutture e dei beni contenuti. Concetto di privacy che, si badi bene, accompagna tutti gli ambiti di applicazione che qui ci interessano. Parliamo dunque di sorvegliare e controllare tutti i diversi contesti: dall'attività industriale ai soggetti privati, passando dall'ambientazione delle mura domestiche fino ad arrivare all'esterno nei luoghi pubblici. Un obiettivo di protezione che si sviluppa in quella che possiamo definire "scienza della sicurezza".
Ma cosa accadrebbe se lo strumento (impianto di antintrusione, sistema di videsorveglianza, smartphone) rappresentasse, esso stesso, l'intruso? Sarebbe un semplice gioco di parole o un pericolo concreto?

(*) Avvocato in Torino **www.studiolegalepandolfino.it**
Studio Legale Feniva **www.feniva.it**

Se così fosse, scopriremmo che nel caso in cui, malauguratamente, venga dimenticata la password di amministrazione di un videoregistratore digitale, è possibile aggirare o sovrascrivere la password con un tool di generazione OTP (One Time Password) che, relazionato al clock di sistema di data e ora, cancella la password di amministrazione stessa. Una semplice OTP - o back door[1] - che da remoto può annientare qualsivoglia password a tutela del sistema! Come se un Grande Occhio, esterno, fosse in grado di violare la più granitica muraglia protettiva volta alla riservatezza (privacy) di un dato sistema. In questo catastrofico scenario il giurista si insinua, senza presunzione di completezza stanti le molteplici sfaccettature, ma col solo fine di comprendere quali possano essere i reali interessi da salvaguardare e le priorità da tutelare.

RESPONSABILITÀ CIVILE

A parere della scrivente, tutta l'annosa questione ruoterebbe intorno a diversi aspetti precipui sia alla nozione di responsabilità (sia civile che penale), sia di sicurezza in senso generale. Circa la nozione di responsabilità civile, da intendersi quale "mancata osservanza di un obbligo" ricordiamoci che l'esistenza dello strumento che genera l'OTP non è mai comunicata all'utente/consumatore, che resta quindi totalmente ignaro del potenziale lesivo dello strumento che invece dovrebbe proteggere la sua privacy (immaginiamo il caso in cui vi sia un accesso, da remoto, all'impianto di videosorveglianza posizionato all'interno delle mura domestiche). In questo senso l'obbligo a cui ci riferiamo è quello del venditore/installatore, che dovrebbe comunicare all'acquirente il potenziale rischio insito della natura stessa del prodotto. A livello codicistico, richiamiamo la "responsabilità per la vendita di un prodotto viziato che cagiona danni", in violazione degli obblighi di cui agli artt. 1476 e 1490 c.c. Ne discende che l'art. 1494 c.c esplicita una funzione di garanzia che tutela l'acquirente laddove prevede che il venditore sia tenuto in ogni caso al risarcimento del danno se non prova di aver ignorato senza colpa i vizi della cosa.

RESPONSABILITÀ PENALE

Mentre in ambito penalistico va evidenziato il portato codicistico di cui all'art. 614 c.p. nel quale il legislatore ha cristallizzato l'assunto secondo il quale "sono vietate le riprese visive o sonore all'interno del domicilio altrui quando queste vengono procurate dal soggetto che utilizza strumenti di ripresa visiva o sonora indebitamente". A questo punto è inevitabile domandarsi: "il cittadino/consumatore come può quindi tutelare il diritto alla riservatezza del proprio domicilio se il sistema di videosorveglianza installato nella propria abitazione potenzialmente può essere lesivo della sua stessa riservatezza?" Come proteggerci insomma dalle nostre telecamere, che seppur atte a riprendere l'eventuale intruso che si introduca in casa nostra, possono al contempo diventare lo strumento che viola, e costantemente, la nostra privacy mediante una neppur troppo complessa procedura di captazione? Una battuta d'arresto, che disarciona il timore del Grande Intruso che tutto vede e tutto sente, ci arriva da oltreoceano. E' dello scorso 2 dicembre il caso dell'attentato terroristico a San Bernardino (California) in cui Syad Rizwan Farook, insieme alla moglie, ha ucciso 14 persone all'Inland Center. Allo stato delle indagini era indispensabile accedere allo smartphone dell'attentatore al fine di ottenere preziosi indizi determinanti ai fini dell'indagine.

Un simile accesso era però ipotizzabile solo creando un nuovo iOS che aggirasse il sistema di sicurezza. A Cupertino, però, non sono sembrati dello stesso avviso, tant'è che secondo Cook (Ceo di Apple) ed i suoi, lavorare su un nuovo iOS sarebbe stato devastante per Apple. La posizione assunta, in perfetto equilibrio politico-tecnologico, ha posto comunque l'attenzione sul fatto che richiedere alle compagnia di rendere possibili azioni di hacking degli apparecchi e dei dati dei clienti, sarebbe infatti un precedente preoccupante. Date per certe tutte le garanzie processual-penalistiche del nostro sistema giudiziario, ciò non toglie che la questione porta con sé la necessità di imbastire un approfondito e aperto dibattito sul concetto di privacy, dovendo quindi fermarci a riflettere sulle possibili soluzioni. A parere della scrivente una soluzione immaginabile sarebbe quella di una corretta informazione sui prodotti, da parte dei produttori esteri, sulle potenzialità dei prodotti e l'eventuale difesa da attacchi di hacking, opera per la quale prestano supporto e valido aiuto figure specialistiche come Amministratori di Rete e Privacy Officer.

[1] Programma che permette di accedere in remoto a un computer evitando le consuete procedure di identificazione, creato per intervenire a distanza in caso di malfunzionamento oppure per effettuare accessi abusivi