LEGGE 119/2013: L'AGGRAVANTE PER LA FRODE INFORMATICA CON FURTO O INDEBITO UTILIZZO D'IDENTITÀ DIGITALE

di Roberto Cosa

Legge 15 ottobre 2013, n. 119

Il Decreto Legge 14 agosto 2013, n. 93, convertito in Legge 15 ottobre 2013, n. 119, noto anche come Decreto contro il femminicidio, ha di fatto apportato modifiche in settori eterogenei del diritto. In particolare, l'articolo 9 del Decreto ha modificato l'articolo 640-*ter* del Codice Penale in materia di frode informatica, introducendo la nozione di "identità digitale".

Uno dei problemi sui quali da tempo si è appuntata l'attenzione dei *media* e dei cittadini è quello del furto di identità. Reato dai toni (e dagli effetti) preoccupanti, che di fatto è sempre esistito sia pure con modalità differenti, sicuramente più pubblicizzato oggi rispetto al passato anche per la stretta connessione con l'esigenza più sentita da parte della collettività di essere tutelata nella propria *privacy*.
Il furto di identità, da un punto di vista giuridico, fino a poco tempo fa era previsto dall'art. 494 del Codice penale che puniva, a dir la verità con una pena minima (fino ad 1 anno di reclusione), la sostituzione di persona, cioè l'azione di colui che in vario modo rubava o utilizzava l'identità di una persona per procurare, generalmente a se, un vantaggio e/o arrecare un danno. In realtà la norma non era per nulla specifica in quanto puniva la sostituzione di persona e non il furto di identità in quanto tale: la carenza normativa doveva essere necessariamente colmata. Esigenza sicuramente sentita e surrogata, nelle more di una definizione compiuta di un nuovo assetto giuridico, da altre norme a supporto, in particolare il Decreto legislativo 231/2007 che recepisce la Direttiva europea 2005/607CE, il Codice in materia di protezione dei dati personali e la Legge 12/2012 in materia di contrasto alla criminalità informatica.

Ora, con l'emanazione del Decreto legge 93/2013 convertito nella Legge n. 119 del 15 ottobre 2013 è stato colmato un gap notevole. In sostanza all'art. 640 ter del Codice Penale, titolato Truffa informatica, è stato aggiunto il comma 2, un passaggio fondamentale dove si sanziona con la pena della reclusione da 2 a 6 anni la frode informatica "*…se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti*". Nota da sottolineare, nel Decreto convertito la modifica era presente nel Capo II, titolato "*…prevenzione e contrasto a fenomeni di particolare allarme sociale*"!
Esaminando più da vicino la fattispecie, se ne percepiscono con immediatezza alcuni aspetti caratterizzanti. Il primo, e più importante, è che **la vittima non è assolutamente a conoscenza del furto di identità a suo danno finché non ne subisce le conseguenze**. Il secondo è che la sottrazione deve necessariamente riguardare una identità reale, di una persona fisica o di una persona giuridica, e non una di fantasia, quale presupposto del reato stesso. In questo, una considerazione deve essere fatta in ordine all'utilizzo sempre più diffuso specie sui *social network*, di *nickname* o di *alias* che sono riconducibili pubblicamente a una persona fisica certa. **Applicando la norma in modo letterale, manca il presupposto di procedibilità stessa**, ma il *gap* deve andare colmato altrimenti avremo una violazione di identità "indiretta" nel senso sopra riportato, senza conseguenze per il responsabile.
Il terzo elemento è costituito dalla pluralità dei modi con i quali è possibile acquisire i dati personali, che spazia dai metodi tradizionali tipici alle possibilità offerte dalla tecnologia, dall'uso dei *social network* e decisamente non da ultimo alle attività fraudolente. È quindi da sfatare la percezione che solo chi "frequenta" i *social* o naviga in rete può incappare in questi problemi. Basti pensare all'invisa abitudine di alcuni negozi che a fronte del pagamento di prodotti con assegno bancario, richiedevano e richiedono tuttora un documento di identità di cui spesso facevano la fotocopia.
Vediamo quindi che lo spettro di possibilità di "diventare" un altro è decisamente elevato e, a parte gli accorgimenti usuali e tipici del buon senso, ben poche sono le possibilità di difendersi o meglio, di prevenire in maniera efficace.

Proviamo solo ad immaginare in una nostra giornata-tipo quante volte esiste la concreta possibilità che qualcuno acquisisca i nostri dati e si trasformi in noi! Sembra di essere quasi in un *film* di fantascienza, con la differenza che è reale e, come dicevamo prima, probabilmente non lo sappiamo. Fastidioso, ma non solo: pensiamo un attimo alle conseguenze, che non sono solamente di ordine economico, ma investono l'aspetto emozionale, impattano psicologicamente sulla persona derubata della sua identità, vanno ad incidere sulla stessa reputazione e mettono anche in condizione di doversi "difendere" da un qualcosa che non si è mai commesso. E in questo, spesso, ci si trova due volte vittima: la prima dei ladri di identità, la seconda della burocrazia talvolta incomprensibile con la quale ci confrontiamo. A tal proposito possiamo ricordare le sanzioni al Codice della Strada erogate a carico di proprietari di autovetture che nella località e nella data contestate erano – con prove provate – da tutt'altra parte: c'è gente che dopo averle provate tutte, compreso il

ricorso al Giudice di Pace, ha deciso di pagare e non perdere ulteriore tempo. Qualcuno può obiettare che più che di furto di identità si tratta di altro. Pensiamo però alla lungimiranza con la quale il Garante per la protezione dei dati personali ha definito a suo tempo, nel 1996, il dato personale, che può essere anche un codice alfanumerico – come una targa – dal quale si arriva all'identità del soggetto, e vediamo che siamo nello stesso campo di applicazione!

Dopo anni di immobilismo su questo fronte, se qualcosa si è mosso lo si deve anche all'azione dell'Unione Europea, che a fronte del dilagare del fenomeno delle frodi ha messo in campo soluzioni di prevenzione e contrasto ai furti di identità. L'Italia in questo ha fatto importanti passi avanti con l'approvazione della citata 119/2013, che segue il Decreto 30 aprile 2007 del Ministero dell'Economia, emesso in attuazione della Legge 17 agosto 2005 n. 166 in materia di prevenzione delle frodi nel settore del credito al consumo, dei pagamenti dilazionati o differiti e nel settore assicurativo, che sono le aree più colpite dal fenomeno.
Si tratta quest'ultimo di un provvedimento importante che prevede la possibilità per una serie di soggetti – banche, intermediari finanziari, assicurazioni, società di mediazione creditizia, gestori di informazioni sul credito, società di servizi di comunicazione elettronica, etc. – **di accedere a informazioni su quanti richiedono l'erogazione del credito al consumo o altre facilitazioni finanziarie. L'interlocutore istituzionale è l'Ufficio centrale antifrode dei mezzi di pagamento (Ucamp)**, costituito presso il Ministero dell'Economia, che oltre ai compiti istituzionali sul monitoraggio delle falsificazioni dell'euro, vaglia e autorizza le richieste di accesso alle banche dati integrate che verranno inoltrate dai soggetti abilitati a richiedere la verifica del credito. La particolarità del provvedimento è che prevede una sorta di cooperazione pubblico-privato, finalizzata a diminuire i costi sociali dei furti di identità e delle frodi che ne sono una delle conseguenze, e limitare per quanto possibile un effetto decisamente pericoloso in termini assoluti, che è quello che stanti le attuali condizioni, chi si appropria delle altrui identità ha la ragionevole certezza di non essere scoperto, se non per cause fortuite.

Legge o non legge, il fenomeno è decisamente notevole per le dimensioni, forse meno per la consapevolezza diffusa, nel senso che se ne parla tanto, ma di fatto a temerne le conseguenze sono soprattutto gli addetti ai lavori, valendo per gli altri, che sono la stragrande maggioranza, la legge per cui certe cose capitano agli altri! Resta così ancora una cosa da fare, che è quella della sensibilizzazione, e in questo lo stesso Ucamp ha già iniziato un programma di formazione/informazione attraverso seminari somministrati agli enti e società sopra citati per far conoscere lo stato dell'arte e le iniziative anche legislative atte a implementare i sistemi di sicurezza per i circuiti delle carte di pagamento e del credito al consumo.
Certo, il percorso è ancora lungo e sentiremo sempre più spesso parlare del fenomeno dei furti di identità, che trova terreno fertile nel processo di innovazione tecnologica che tutti, dallo Stato alle aziende, pongono come obiettivo strategico per elevare gli *standard* qualitativi e di efficienza di servizi erogati, ma che comporta inevitabilmente le vulnerabilità tipiche dei sistemi aperti.

A questo punto, vale fare una considerazione. Con la legge 241/90 viene normato il *"diritto degli interessati di prendere visione di estrarre copia di documenti amministrativi"*, come previsto dall'art. 22, che rimanda al successivo art. 25 per le modalità di accesso, che si sostanziano in visione ed estrazione in copia dei documenti stessi.

L'evoluzione tecnologica, l'avvento delle politiche di *e-government* e soprattutto l'emanazione del Codice dell'amministrazione digitale con il decreto legislativo 7 marzo 2005 n.82 hanno sostanzialmente configurato il diritto a colloquiare con la Pubblica Amministrazione attraverso l'uso di tecnologia telematica, quindi riconoscendo al cittadino il diritto a interfacciarsi con la PA nelle sue varie configurazioni attraverso modalità di accesso digitale. Siamo di fronte ad una nuova frontiera, con un nuovo ruolo dello Stato, che accorcia la distanza tra sé ed i suoi cittadini in un'ottica di efficienza, democrazia e abbattimento delle barriere.
Ultimo atto normativo di gran significato è il cd. Decreto Fare 69/2013 convertito con legge 9 agosto 2013 n. 98 dove, oltre all'istituzione del tavolo di lavoro per l'attuazione dell'Agenda digitale italiana, **viene riconosciuta la liberalizzazione dell'accesso ad internet**.

Come spunto di riflessione, è da notare come si stia iniziando a parlare della nascita di un nuovo diritto, che è quello da più parti ipotizzato come diritto di accesso alla Rete, che verosimilmente troverà la sua legittimazione normativa. Senza entrare in argomento ora, è un argomento di grande interesse e di grandi speculazioni, sul quale sarebbe interessante approfondire, anche in relazione ai prevedibili mutamenti di scenario.
Tutto questa evoluzione riconduce poi all'argomento iniziale: aumenta la libertà di circolazione digitale, aumentano i rischi connessi ed è necessario trovare una conciliazione tra l'esigenza, irrinunciabile, del diritto di accesso ora e domani del diritto di accesso alla Rete, e l'esigenza di sicurezza, che riguarda tanto il singolo quanto l'organizzazione, pubblica quanto privata, cioè Stato e Aziende.
Non vorrei in questo che l'onere maggiore di sicurezza in termini di costi di implementazioni ricada proprio su queste ultime, ma il mio pensiero è forse condizionato dal **recente tentativo** di introdurre nella 231/2001 i reati di frode informatica con sostituzione di persona, indebito utilizzo di carte di credito o di pagamento illeciti penali in tema di trattamento dei dati personali. Norma importante, che ha come obiettivo da un lato la tutela dell'identità digitale al fine di arginare il fenomeno delle frodi, dall'altro però pone in capo alle (sole!) Aziende la responsabilità di porre in essere predisposizioni logiche e organizzative per evitare la commissione di questi reati. Facile a dirsi, molto più complesso a farsi per la natura stessa della tecnologia, che si evolve in maniera talmente rapida da rendere sostanzialmente non adeguate le misure di sicurezza, che costituiscono di fatto l'unica esimente per evitare la responsabilità amministrativa prevista dalla 231.

In chiusura, una nota: **è un problema globale e come tale deve essere affrontato, sinergicamente, tra tutte le componenti del Sistema Paese, pubbliche e private**, che in questa lotta dovrebbero essere poste sullo stesso piano. ©