ARTICOLO SOTTOPOSTO A PEER REVIEW

LA NUOVA FATTISPECIE DI "INDEBITO UTILIZZO D'IDENTITÀ DIGITALE"

Un problema interpretativo

Gianclaudio Malgieri

Abstract

La recente introduzione nel nostro codice penale della frode informatica aggravata dall'indebito utilizzo d'identità digitale pone una rilevante questione interpretativa. Nel presente contributo si analizza il rapporto tra la suddetta aggravante e quella di "furto d'identità digitale", nonché le intersezioni con le fattispecie previste dal codice della privacy: mezzi diversi (e in cerca di autonomia) a tutela della "identità digitale".

Sommario

1. Introduzione.

È di recente introduzione, nel nostro ordinamento, l'ipotesi di indebito utilizzo d'identità digitale[1]. Si tratta di un'aggravante della frode informatica, contemplata assieme al furto d'identità al terzo comma dell'art. 640 *ter* c.p.: "la pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti".

Sorvolando sul non banale problema di definizione del concetto di identità digitale[2], ancor più problematica appare la collocazione e l'applicazione della fattispecie dell'"indebito utilizzo" della stessa.

Tre sono le maggiori questioni che si presentano all'interprete: a) la definizione di "utilizzo" indebito di una identità digitale altrui; b) il rapporto e la differenza tra il "furto" e l'"indebito utilizzo" di identità digitale; c) il rapporto tra l'indebito utilizzo e l'ipotesi base di frode informatica. Non da ultimo, occorre poi indagare sulla possibile intersezione/sovrapposizione della fattispecie in esame con quella di trattamento illecito di dati personali, ai sensi del c.d. codice della privacy.

2. La materializzazione dell'identità digitale.

Innanzitutto, non si può nascondere una certa perplessità riguardo all'ipotesi di "utilizzare" l'identità umana altrui, parallelamente alla possibilità di "rubarla"[3].

Del resto, ciò che appare in modo univoco è il tentativo legislativo di una "materializzazione" dell'identità personale in rete[4] e dunque la necessità per l'interprete di tradurre l'identità in qualche entità definita, come ad esempio i dati personali, intesi come le forme privilegiate con cui il soggetto proietta se stesso (più o meno volontariamente) nel mondo digitale[5].

Inoltre, la fattispecie dell'indebito utilizzo di identità digitale appare quanto mai problematica, per diversi motivi[6]: innanzitutto, essa non richiama in alcun modo il *nomen iuris* dell'aggravante (ossia la rubrica dell'art. 9 del d.l. del 2013) che si riferisce alla "frode commessa con sostituzione d'identità digitale" e dunque non ha alcun legame apparente con l'incriminazione prevista in sede di decreto legge ("sostituzione di identità digitale" appunto), essendo essa il frutto di una modifica in sede di conversione parlamentare del decreto[7].

Inoltre, ci si domanda come coniugare tale fattispecie con quella di "furto di identità": due condotte apparentemente eterogenee eppur legate da un medesimo giudizio di disvalore nell'aggravante in esame[8].

In mancanza di una precisa definizione dell'"indebito utilizzo" di identità digitale, non si potrà che ricercare un riferimento normativo nel nostro ordinamento all'"indebito utilizzo" di dati riguardanti l'identità.

[1] Art. 9 del d.l. 14 agosto 2013 n. 93, convertito con modifiche dalla legge 15 ottobre 2013 n. 119.

[2] Che è stato anche oggetto di discussione parlamentare: cfr. emendamento 9.100 Quintarelli pubblicato nell'Allegato A degli atti della seduta dell'Aula del 9/10/2013, Camera dei Deputati, ma cfr. anche gli interventi in aula degli onn. Coppola, Schirò Planeta, Palmieri, Boccadutri, De Lorenzis, Resoconto Stenografico dell'Assemblea, Seduta n. 93 di mercoledì 9 ottobre 2013, Camera dei Deputati, XVII Legislatura, pp. 21 e 22. Cfr. in dottrina A. Di Tullio D'elisiis, *Frode informatica commessa con sostituzione d'identità digitale: profili applicativi,* in *Altalex*, 14 gennaio 2014; L. Pistorelli, *Prime note sulla legge di conversione, con modificazioni, del d.l. n. 93 del 2013, in materia tra l'altro di «violenza di genere» e di reati che coinvolgano minori,* in *Dir. pen. cont.*, 18 ottobre 2013, pp. 6 e 7.

[3] G. Ziccardi, *voce* "*Furto d'identità*", in *Digesto delle Discipline Penalistiche* a cura di A. Gaito, Torino, 2011, pp. 253 ss.

[4] Cfr. L.C. Ubertazzi, *Riservatezza informatica ed industria culturale*, in *AIDA*, Milano, 1997, pp. 530 ss; Id., *I diritti d'autore e connessi. Scritti*, Milano, 2000, 185; R.S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, in 84 Geo. L.J., 1996, 2381; P. Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, in 11 Berkeley Tech. L.J., 1996, 1.

[5] Per una panoramica sul concetto di "identità digitale" e di materializzazione dei dati identitari cfr. G. Resta, *Identità personale e identità digitale*, in *Dir. Informatica*, fasc. 3, 2007, pp. 511 ss.; J.D. Lassica, *Identity in the Age of Cloud Computing: The Next-Generation Internet's Impact on Business, Governance and Social Interaction*, Washington (DC), 2009, 1.

[6] Cfr. rilievi critici di A. Di Tullio D'elisiis, *op. cit.*

[7] Emendamento 9.5 Colletti, Turco, Businarolo, Ferraresi, Bonafede, Agostinelli, Micillo, Sarti, Mucci approvato dalle Commissioni riunite I e II della Camera dei Deputati (XVII legislatura) nella seduta di venerdì 6 settembre 2013.

[8] Cfr. al riguardo i rilievi di L. Pistorelli, *op.cit.*, pp. 6 e 7.

3. Il rapporto tra l'indebito utilizzo e la condotta base di frode informatica.

In primis, occorre menzionare che l'ipotesi generale di frode informatica *ex* art. 640 *ter*, 1° comma, c.p. sanziona esplicitamente l'intervento "senza diritto con qualsiasi modalità su dati, informazioni, (...)". Nell'interpretare tale fattispecie la dottrina si è chiesta se vi rientrasse anche l'ipotesi di un "uso non autorizzato di dati", ossia una "introduzione indebita di dati altrui in un sistema informatico[9]", che è poi la struttura portante della condotta di sostituzione d'identità digitale in commento.

Molti ordinamenti già prevedono esplicitamente tale ipotesi nei casi di frode informatica: il codice penale tedesco, ad esempio, al § 263a prevede che "chiunque con l'intenzione di procurare a sé o ad altri un ingiusto vantaggio patrimoniale, danneggia il patrimonio altrui (...) attraverso (...) un'utilizzazione di dati inesatti o incompleti o un uso non autorizzato di dati (...) è punito (…)[10]". Del tutto speculare è il codice penale portoghese (art. 221[11]).

Nel nostro art. 640 *ter* c.p., invece, non c'è un riferimento esplicito all'uso indebito di dati, ma solo ad un "intervento senza diritto sui dati". Ora, posto che l'intervento è inteso nel senso di una modificazione del contenuto o della destinazione dei dati[12] non sembra possibile considerare tra le condotte punite dalla fattispecie generale *ex* art. 640 *ter* c.p. anche il mero uso indebito di dati (che si esplica ad esempio nell'utilizzo di una password altrui per l'accesso ad un profilo digitale[13]).

Tuttavia, tali considerazioni, se da una parte sembrano smentite dalla novella in commento poiché essa considera esplicitamente l'"utilizzo indebito" di dati (identitari) altrui tra le modalità di commissione della frode informatica ("se il fatto è commesso con (...) indebito utilizzo"), dall'altra non chiariscono il significato di quell'"indebito utilizzo di identità digitale".

Per rispondere alla prima questione occorre notare che la condotta in commento non integra da sola il fatto tipico, essendo soltanto un elemento strumentale alla realizzazione della condotta offensiva[14]: in effetti la novella si esprime con un generico "se il fatto è commesso con" e non con un "se il fatto consiste in", pertanto specifica soltanto una delle modalità che possono portare alla perfezione del fatto tipico.

Per rispondere, invece, alla seconda questione occorre ricercare se nel nostro ordinamento esistano spunti rilevanti in merito.

4. Spunti normativi per definire l'"indebito utilizzo d'identità digitale" e il rapporto col furto d'identità.

Un primo riferimento può trovarsi all'art. 55, comma 9 del d.lgs. del 21 novembre 2007 n. 231[15] che punisce chi "al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, in altre parole qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi" (disposizione che richiama quasi integralmente l'abrogato art. 12, d.l. 3 maggio 1991, n. 143, convertito, con modificazioni, nella l. 5 luglio 1991, n. 197).

Tale norma può giovare ai fini di una previsione dei profili applicativi concreti della fattispecie in commento[16], tuttavia nonostante anche tale fattispecie colpisca violazioni del

[9] C. Pecorella, *Diritto penale dell'informatica,* II ed., Padova, 2006, p. 102.
[10] Cfr. K. Tiedmann, *Strafgesetzbuch. Leipziger Kommentar,* XI ed., Berlin, 1998, *sub § 263a*.
[11] Cfr. J. Figueiredo Dias, *Introduzione al codice penale portoghese* (trad. it. a cura di G. Torre), Padova, 1997; si segnala che anche il codice penale giapponese, parla al § 246-2 di un utilizzo illegittimo di dati elettronico-magnetici.
[12] C. Pecorella, *op.cit.*, 90.
[13] *Idem*, 103; che riguardo alle condotte di abuso del sistema di *home banking* altrui, ravvede l'integrazione del reato di frode informatica nel momento del trasferimento illecito di denaro (in quanto "intervento senza diritto" su dati informatico-bancari) e non già nel mero accesso al profilo, che può semmai integrare gli estremi dell'art. 615 *ter* c.p.
[14] *Idem, 90.*
[15] "Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione". Per un commento della norma si rimanda a U. Pioletti, *Possesso o utilizzo abusivo di carte di credito*, in *Giur. Merito*, 2012, 9, 1936.
[16] Ad esempio riguardo ai profili sostanziali del tentativo, del concorso di reati, ecc. cfr. A. Di Tullio D'elisiis, *op. cit.*

patrimonio in ambito informatico e inglobi parzialmente la condotta di sostituzione di persona[17], non si può trascurare che in questo caso l'"indebito utilizzo" si riferisce ad oggetti concreti (carte di credito o altri documenti analoghi) e per questo mal può prestare ausilio ad una definizione corretta dell'indebito utilizzo di identità digitale.

Spunto forse più significativo ci è fornito dall'art. 30 *bis* del d.lgs. 141 del 2010[18]: nel definire il furto d'identità, esso parla di "impersonificazione" in termini di occultamento totale o parziale della propria identità mediante l'utilizzo indebito di dati relativi all'identità e al reddito di un altro soggetto.

Si noti, dunque, come alla luce di tale riferimento l'indebito utilizzo di dati personali è condotta strumentale al furto d'identità e non è dunque una condotta alternativa come sembrerebbe dalla formulazione dell'attuale art. 9 del d.l. del 2013 così come modificato in sede di conversione.

A suffragare tale punto di vista, occorre menzionare la definizione del furto d'identità proposta dall'OCSE, secondo cui esso consiste, tra l'altro, in un "uso di informazioni personali in modo non autorizzato[19]". Anche tale definizione, infatti, sembra considerare l'"indebito utilizzo" come una sottocategoria del furto d'identità.

Spunti opposti, invece, ci sono forniti dalle definizioni della dottrina di *common law*[20] e del centro studi delle Nazioni Unite[21]: per entrambe le definizioni, infatti, il furto d'identità digitale è visto come mera apprensione di dati, mentre l'"utilizzo" illecito di tali dati rientra tra gli elementi strutturali della "frode d'identità" (peraltro molto più affine al ruolo che il nuovo furto d'identità digitale assume nel nostro ordinamento[22]).

In altri termini, in base a questo paradigma, l'indebito utilizzo dell'identità digitale può ben sussistere come condotta alternativa al furto, in quanto "frode" all'identità.

Dal momento che in questo paradigma la frode non comporta un'apprensione dei dati contro la volontà, ma solo un utilizzo degli stessi contro la volontà del titolare di quei dati, se accettassimo questa struttura, si potrebbe comprendere la differenza strutturale tra "furto d'identità" e "indebito utilizzo": nel primo caso è indebita già l'acquisizione dei dati; nel secondo invece l'offensività rileva non nel momento acquisitivo, ma nel successivo utilizzo dei dati acquisiti.

Parrebbe conveniente sposare questo secondo paradigma poiché la norma in commento collega le due ipotesi (furto e indebito utilizzo) tramite una "o" disgiuntiva: è quindi necessario dimostrare l'alternatività della condotta di furto e di quella di indebito utilizzo[23].

In effetti, se sposassimo il concetto secondo cui l'"indebito utilizzo" d'identità digitale sia solo un elemento strutturale del più ampio furto d'identità digitale, non si comprenderebbe come mai il legislatore abbia voluto punire con la stessa severità sia una condotta complessa (il furto) sia una sua sotto-condotta semplice (l'uso indebito).

L'unica soluzione sarebbe quella di considerare la congiunzione "o" non come elemento di alternatività esclusiva tra le due condotte, ma come mezzo (abbreviativo di "ossia", "ovvero") per definire il furto d'identità digitale, per introdurre una diversa denominazione per una condotta similare. Si supererebbe così il limite per cui i dati identitari non si possono

[17] Cfr. Cass. pen., Sez. V, 6 giugno 2003, n. 24816, Ferruti, Rv. 225945, secondo cui «il reato di indebita utilizzazione di carta di credito e di pagamento, di cui all'art. 12 d.l. 3 maggio 1991, n. 143, assorbe il reato di sostituzione di persona, di cui all'art. 494 c.p., ogni qual volta la sostituzione contestata sia posta in essere con la stessa condotta materiale integrante il primo reato. Ed infatti, l'ipotesi delittuosa dell'indebito utilizzo del mezzo di pagamento lede, oltre il patrimonio, anche la pubblica fede, mentre l'art. 494 c.p. contiene una clausola di riserva destinata ad operare anche al di là del principio di specialità ("se il fatto non costituisce un altro delitto contro la fede pubblica"). Sussiste, invece, concorso materiale fra gli stessi reati nel caso in cui la sostituzione sia stata realizzata con un'ulteriore e diversa condotta rispetto a quella che ha integrato l'altra fattispecie delittuosa (nel caso di specie, la S.C. ha annullato senza rinvio l'impugnata sentenza in quanto non risultava la sostituzione di persona fosse stata realizzata con ulteriore comportamento rispetto a quello consistente nella mera utilizzazione indebita della carta)». Cfr. U. Pioletti, *op. cit.*, § 5.

[18] D.lgs. 13 agosto 2010, n. 141, *Attuazione della direttiva 2008/48/CE*.

[19] OECD, *Scoping Paper on Online Identity Theft,* 18 giugno 2008, Section I.

[20] Australasian Centre for Policing Research and the Australian Transaction Reports and Analysis Centre, *Standardisation of Definition of Identity Crime Terms: A Step towards consistency,* Report Series no. 145.3, 2006, 7.

[21] Un Ieg, *Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity,* Australasian Centre for Policing Research and the Australian Transaction Reports and Analysis Centre, *op.cit.*, 5-20.

[22] Cfr. B. Acoca, *Online identity theft: a growing threat to consumer confidence in the Digital Economy*, in D. Chryssikos, N. Passas, C.D. Ram (a cura di), *The evolving challenge of identity-related crime: addressing fraud and the criminal misuse and falsification of identity*, Milano, 2008, 75.

[23] A. Di Tullio D'Elisiis, *op. cit.*

propriamente rubare con spossessamento quanto piuttosto utilizzare indebitamente[24] e la aggiunta dell'ipotesi di "indebito utilizzo" gioverebbe ad aumentare il raggio applicativo in un campo che rischia di peccare di indefinitezza[25] come del resto avviene spesso in ambito di sostituzione di persona[26] o in generale nei reati informatici[27].

Tuttavia, per evitare la ridondanza delle disposizioni penali, ossia per garantire pieno valore ad ogni tratto grafico del legislatore, occorrerebbe, in ossequio ad una interpretazione conservativa della legge, dare valore disgiuntivo alla parola "o[28]".

Ed è così che risulta preferibile il primo paradigma: il furto d'identità si palesa nell'illecita apprensione dei dati identitari, mentre l'indebito utilizzo si concretizza in un utilizzo abusivo di quei dati, a prescindere dalle modalità con cui essi siano stati ricavati. E il dualismo tra furto e indebito utilizzo ricalcherebbe la storica separazione, postulata dalla dottrina più avveduta in campo criminalità informatica, tra *unauthorized access* (accesso non autorizzato a sistemi altrui / possesso non autorizzato di dati altrui) e *unauthorized use* (uso non autorizzato di dati altrui lecitamente posseduti[29]).

Si può però obiettare che un furto di identità digitale non può consistere certo nel mero possesso di dati altrui (o nel compiere un *unauthorized access*), ma in una concreta sostituzione di persona, come del resto richiede la stessa rubrica della novella. Dunque, anche per conciliare la disposizione col suo *nomen iuris*, si potrebbe concludere che la nuova circostanza aggravante consiste sempre in una sostituzione di persona (quanto agli effetti), ma nel caso del "furto d'identità digitale" ciò è reso possibile da un'apprensione illecita dei dati personali; nel caso dell'"indebito utilizzo", invece, ciò è compiuto con un uso "deviato" o "non autorizzato" di dati lecitamente raccolti (perché liberamente disponibili sul *web*, noti, "abbandonati" da altri[30] oppure raccolti consensualmente per scopi diversi e poi traditi[31]).

Solo così le due condotte sono pienamente alternative, poiché il disvalore del fatto consiste nella violazione del consenso del titolare dei dati, che si può realizzare una sola volta: o al momento dell'apprensione dei dati o al momento di un uso deviato di dati lecitamente appresi.

Dunque, con questa definizione di indebito utilizzo trova punizione anche la creazione di un *account* o di un profilo digitale falso che richiama il nome o le caratteristiche personali di un'altra persona (dati non rubati, ma semplicemente "noti" e indebitamente utilizzati col fine di sostituirsi alla persona della vittima).

Tale soluzione trova fondamento analogico anche nelle soluzioni adottate dalla giurisprudenza nell'applicazione del già menzionato reato di cui all'art. 55, comma 9 del d.lgs. 231/2007 (e del precedente e identico art. 12 d.l. 3 maggio 1991, n. 143, convertito, con

[24] Cfr. al riguardo il fatto che art. 30 *bis* del d.lgs. 13 agosto del 2010 n. 141, definisca il furto d'identità con "utilizzo indebito", proprio perché un furto immateriale si appalesa perlopiù in "utilizzo". Cfr. anche P. Catala, *Ebauche d'une Théorie Juridique de l'Information*, in *Inf. e dir.*, 1983, 97, che pur dando fondamento al furto immateriale, ne costruisce tutela sulla segretezza e sul risarcimento in caso di "uso abusivo", definendo di fatto il "furto" con "uso abusivo".

[25] Cfr. G. Marinucci, E. Dolcini, *Manuale di diritto penale. Parte generale*, Milano, 2012, 58, secondo cui una precisa elencazione di figure o condotte, in ossequio ad una tecnica casistica di formulazione della legge penale, assicura il più elevato grado di precisione tra le tecniche di redazione legislativa criminale, col solo rischio di una possibile elefantiasi della legislazione penale.

[26] Un esempio è costituito proprio dall'art. 494 c.p. (sostituzione di persona) che punisce chi "sostituisce illegittimamente la propria all'altrui persona" *oppure* "attribuisce a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici". Anche in questo caso si è di fronte a due condotte in cui l'una (attribuirsi nome o condizione personale altrui) è sostanzialmente un sottoinsieme della seconda (sostituirsi ad altra persona).

[27] Si confronti la ricorrente formulazione "sistemi informatici o telematici" di cui agli articoli dal 615 *ter* al 615 *quinquies*, dal 617 *quater* al 617 *septies* e 640 *ter* c.p. nonostante i secondi siano comunque compresi nei "sistemi informatici". Così come la menzione di "comunicazione o conversazione" di cui agli art. 617, 617 *bis*, 617 *ter* c.p. (nonostante la conversazione sia un elemento del macro insieme "comunicazioni"), o ancora la menzione di "dati o informazioni" (nonostante la differenza tra dati e informazioni da taluno fortemente problematizzata, è indubbio comunque l'interscambiabilità tra i due termini, cfr. C. PECORELLA, *op. cit.*, pp. 75 ss.) di cui all'art. 615 *quinquies* e 640 *ter* c.p. Riguardo alle tecniche di formulazione dei reati informatici cfr. L. Picotti, *Tutela penale della persona e nuove tecnologie,* Padova, 2013, pp. 53 ss. e Id., *Biens juridiques protégés et techniques de formulation des incrimination en droit pénal de l'informatique,* in *Rev. Int. Droit pénal,* 2006, 3/4, pp. 525 ss.

[28] Cfr. ad esempio Cass., Sez. II, 30 gennaio 2006, Jolly Mediterraneo, in *Foro it.*, II, 2006, pp. 329 ss. che, seppur su altro tema, dà valore di disgiunzione alla "o" all'art. 5, comma 1, d.lgs. 231/2001, anche considerando la possibilità di attribuire un significato diverso ai due elementi disgiunti (*interesse* e *vantaggio*).

[29] Cfr. M. Wasik, *Crime and the computer*, Oxford, 1991, pp. 69 ss.

[30] Cfr. Un Ieg, *Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity,* Report of the Secretary-General, E/CN.15/2007/8, 2 April 2007, 5-20, quando si riferisce alle informazioni personali "abbandonate", si noti inoltre che la pratica del "*bin raiding*" (ovvero ottenimento dei dati attraverso estratti conto, bollette, vecchi contratti assicurativi, lettere personali, involucri di giornali spediti a casa, informazioni fiscali ecc. che sono stati buttati nel cestino della spazzatura). Cfr. Adiconsum, Osservatorio Permanente sul furto d'identità, *Report 2010*, 3.

[31] Cfr. *infra* par. 5, il concetto di "trattamento illecito di dati personali" del cod. privacy e dell'abuso delle finalità specifiche per cui è concordato un trattamento (inizialmente lecito) di dati (artt. 3, 13, comma 1, lett. a); art. 23, comma 3 cod. privacy).

modificazioni, nella l. 5 luglio 1991, n. 197) in cui si è specificato che l'"indebito utilizzo ricorre anche quando il consenso è prestato da parte del titolare dell'identità digitale violata sempre che l'uso avvenga in modo difforme all'accordo convenuto col titolare stesso" (dunque non "furto di dati", ma "indebito utilizzo" di dati lecitamente posseduti[32]).

Posta dunque l'alternatività tra le condotte di furto e di indebito utilizzo dell'identità digitale, viene da chiedersi in quali condotte concrete si esplichi un "utilizzo indebito" di dati identitari.

Per rispondere a tale quesito si può considerare la condotta di "trattamento illecito di dati personali" sanzionata dal d.lgs. 196/2003, codice in materia di protezione dei dati personali (di qui in avanti cod. privacy)[33].

5. Il trattamento illecito per il codice della privacy.

Dal combinato disposto degli artt. 167 e 23 cod. privacy[34], risulta che i privati o gli enti pubblici economici[35] che, al fine di trarne per sé o per altri profitto o di recare ad altri un danno[36], procedano al trattamento di dati personali senza il consenso dell'interessato espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, documentato per iscritto, di cui sono state rese all'interessato le informazioni di cui all'articolo 13[37], e sia un consenso scritto accompagnato da autorizzazione del garante in caso di dati sensibili[38] sono puniti, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi, ma se il fatto consiste in diffusione o comunicazione da sei a ventiquattro mesi, sempre che tutto ciò non costituisca un più grave reato[39].

Per i soggetti pubblici (non economici) si applica la stessa fattispecie, con la differenza che il trattamento è reso illecito non dalla mancanza del consenso, ma dall'abuso o dalla mancanza di funzioni istituzionali a fondamento della condotta[40].

La definizione di trattamento fornita dal codice, peraltro, è molto ampia e in grado di comprendere qualsiasi attività che abbia ad oggetto dati personali[41].

La suddetta norma, dunque, punisce qualsiasi attività privata su dati altrui contraria ad un consenso pieno e circostanziato dell'interessato e qualsiasi attività pubblica su dati personali che abusi delle funzioni istituzionali, se queste attività sono commesse col dolo (specifico) di trarne profitto o arrecare danno e se il danno si verifica.

Peraltro, risulta molto interessante, ai nostri fini, il riferimento alle finalità specifiche e chiaramente delimitate[42] per cui un trattamento deve compiersi: è proprio l'abuso delle finalità

[32] Trib. Milano, 8 novembre 2006, in *Giur. merito*, 2012, 9, 1936, con nota di U. Pioletti.

[33] Il collegamento tra tale novella e il cod. privacy è rafforzato tra l'altro dal comma 2 dell'art. 9 del d.l. 93/2013 che estende i reati presupposto per la responsabilità amministrativa degli enti collettivi (*ex* art. 24 *bis* d.lgs. 231/2001) anche alle ipotesi delittuose previste dal codice del trattamento dei dati personali.

[34] In realtà l'art. 167 richiama anche altri articoli la cui violazione, ai termini da esso stabiliti, costituisce reato, ma nello specifico si è preferito indicare solo il riferimento all'art. 23, essendo il più ampio e generico, mentre gli altri riguardano campi più specifici che non giovano ad un approccio astratto: art. 18 (che riguarda i trattamenti effettuati da soggetti pubblici), art. 19 (che riguarda il trattamento e la comunicazione da parte di soggetti pubblici di dati diversi da quelli sensibili e giudiziari), artt. 123, 126 e 130 (che riguardano i dati relativi al traffico o all'ubicazione ovvero le comunicazioni indesiderate nell'ambito delle comunicazioni elettroniche), art. 129 (che riguarda la formazione degli elenchi di abbonati), art. 17 (che riguarda il trattamento di dati che presentano rischi specifici per i diritti e le libertà fondamentali e per la dignità dell'interessato), art. 20 (che riguarda il trattamento di dati sensibili), art. 21 (che riguarda il trattamento di dati giudiziari), art. 22 (che riguarda i dati idonei a rivelare lo stato di salute), artt. 26 e 27 (che riguardano rispettivamente i dati sensibili ed i dati giudiziari) art. 45 (che riguarda il trasferimento di dati fuori dal territorio dello Stato).

[35] Art. 23, comma 1, cod. privacy.

[36] Art. 167, comma 1, cod. privacy.

[37] Art. 23, comma 3. Ossia (art. 13, comma 1): lett. *a) le finalità e le modalità del trattamento, b) la natura obbligatoria o facoltativa del conferimento dei dati, c) le conseguenze di un eventuale rifiuto di rispondere, d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi; e) i diritti di cui all'articolo 7* (accesso, aggiornamento, cancellazione, ecc.) *f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.*

[38] Art. 23, comma 4, cod. privacy.

[39] Art. 167, comma 1, cod. privacy.

[40] Art. 18, comma 2, cod. privacy.

[41] Art. 4, comma 1, lett. a). Cfr. F. Buffa, *Profili penali del commercio elettronico*, Milano, 2006, 166.

[42] Art. 13, comma 1, lett. a); art. 23, comma 3, cod.privacy. Cfr. più in generale il "principio di necessità" art. 3 cod. privacy.

concordate a determinare l'indebito utilizzo di dati (non già "rubati", ma ottenuti col pieno consenso dell'interessato).

6. Differenze e intersezioni tra la condotta di trattamento illecito di dati e l'indebito utilizzo d'identità digitale.

Ci si può chiedere dunque se tale norma possa costituire un solido riferimento normativo alla definizione di "indebito utilizzo" ovvero se si possa sostanzialmente leggere l'aggravante di cui al comma 3 del nuovo art. 640 *ter* c.p. in un modo analogo al seguente: "(...) se il fatto è commesso con furto d'identità digitale o in concorso col reato di cui all'art. 167 del codice della privacy".

In realtà, il concetto di "trattamento illecito" sembra più ristretto rispetto al concetto di "indebito utilizzo", proprio perché il primo è delimitato nel campo applicativo da concetti normativamente delimitati e definiti[43].

Occorre allora domandarsi se ci sono ipotesi di condotta che pur riguardando l'"indebito utilizzo d'identità digitale" non siano ascrivibili al trattamento illecito di dati personali.

Al riguardo, si può riflettere sul caso della creazione di un profilo digitale falso a nome altrui. In questo caso, peraltro già riscontrato in giurisprudenza[44], ci si può domandare se il solo utilizzo del nome altrui senza consenso (e con lo scopo di creare un danno, che poi si verifica concretamente) nella sfera digitale possa configurare un'ipotesi di "trattamento illecito" punibile penalmente ai sensi dell'art. 167 cod. privacy.

Due elementi potrebbero condurre ad una risposta negativa: la non applicabilità delle norme del codice della privacy quando il trattamento è compiuto per "fini esclusivamente personali" (e dunque non nell'ambito di un'attività commerciale o professionale) in base all'art. 5, 3° comma del codice (la c.d. "eccezione domestica[45]") e la non necessità del consenso (*ex* art. 24, lett. c)) quando il trattamento riguardi dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, come è appunto il caso del nome e cognome.

Tuttavia, per quanto riguarda l'"eccezione domestica" non si può fare a meno di notare che si tratta comunque di un'attività che, per quanto non professionale, è svolta su una piattaforma internet accessibile da un numero elevato di persone. Infatti, l'Article 29 Working Party[46], ha chiarito che tale eccezione non può esonerare dagli obblighi (e dalle sanzioni) previsti dalla disciplina gli utenti che utilizzino la piattaforma principalmente per finalità politiche o sociali diffuse (poiché mancherebbe il requisito dell'uso domestico o personale dei dati) o qualora i contatti auto-selezionati con cui è in relazione l'utente siano numericamente elevati (con la conseguenza che molti contatti-utenti siano potenzialmente sconosciuti all'utente che tratta i dati), o costituiscano addirittura la totalità degli utenti *web*[47]. Tutto ciò, del resto, è stato confermato anche dalla Corte di giustizia europea[48] e dal Garante europeo sulla protezione dei

[43] Si noti, infatti, che l'art. 4, che definisce il significato di "trattamento" specifica che esso (per quanto ampio) vale solo "ai fini del presente codice" e che il trattamento si definisce "illecito" (art. 167) solo in quanto in violazione di altre norme tipiche dello stesso codice della privacy (artt. 17-23, 25-27, 45, 123, 126, 130).

[44] Si noti l'importante caso di sostituzione di identità digitale tramite un *account* su un social network: Cass. pen., Sez. V, 8 novembre 2007, n. 46674, in *Dir. informatica*, fasc. 4-5, 2008, 526, con nota di C. Flick, *Falsa identità su internet e tutela penale della fede pubblica degli utenti e della persona,* in cui la creazione di un profilo utente utilizzando il nome di un'altra persona è sanzionato ai sensi di un'interpretazione estensiva dell'art. 494 c.p. (sostituzione di persona).

[45] Cfr. M. Gorgoni, *Commento all'art. 5, 3° comma*, in C.M. Bianca, F.D. Busnelli (a cura di), *La protezione dei dati personali, Commentario al D.lgs. 30 giugno 2003, n. 196*, tomo I, Padova, 2007, 97-123.

[46] L'organo in seno alla Commissione europea preposto all'interpretazione della disciplina sul trattamento dei dati personali *ex* art. 29, direttiva 95/46/CE.

[47] *Ibidem*; inoltre con riferimento alla pubblicazione su internet di dati provenienti da elenchi pubblici e sulle conseguenze connesse al fatto che su internet c'è una fortissima contrazione (se non annullamento) della dimensione spaziale e temporale, cfr. R. Clarizia, *La pubblicazione on-line delle dichiarazioni dei redditi*, in *Dir. Int.*, 4/2008, 333, e G. Cassano, *Redditi on-line*, in *Dir. Int.*, 4/2008, 329.

[48] CGE, C-73/07, 12 settembre 2007, Satamedia, Racc. pag. I-9831, punto 47 che riprende CGE, C-101/01, 6 novembre 2003, Lindqvist, Racc. pag. I-12971, punti 43 e 44; ma si rileva già CGE, C-101/01, 6 novembre 2001, in *Foro it.*, 2004, IV, 57, con nota di A. Palmieri, R. Pardolesi.

dati[49], nonostante alcune specificazioni della nostra giurisprudenza di legittimità[50].

Per quanto riguarda invece il secondo elemento, ovvero la non necessità del consenso in caso di dati "pubblici" si è argomentato che comunque un uso di tali dati al fine di sostituirsi ad altra persona contrasta col principio generale che permea la normativa a tutela della privacy *ex* art. 2 cod. privacy, ovvero che il trattamento dei dati personali avvenga nel rispetto dei diritti e delle libertà fondamentali nonché della dignità dell'interessato. E contrasterebbe anche con l'articolo 11 cod. privacy, per cui i dati debbono essere trattati secondo principi di liceità e correttezza[51] come del resto emerge da alcuni atti del Garante per la protezione dei dati personali[52].

In realtà la Suprema corte[53] ha ritenuto pienamente applicabile l'eccezione dell'art. 24, lett. c) cod. privacy riguardo ai dati già presenti in "pubblici" registri[54], utilizzati nell'ambito di una sostituzione digitale di persona, ritenendo pertanto che non possa parlarsi di "trattamento illecito" *ex* art. 167 cod. privacy.

Del resto, appare impervio affidarsi ad un'interpretazione *in malam partem* dei principi generali di cui all'art. 2 cod. privacy (dal momento che enuncia delle mere "finalità" che il legislatore si è posto, non dei criteri per l'interprete) e delle clausole generali di cui all'art. 11 cod. privacy (che comunque costituisce un regola specifica, non richiamata dalle fattispecie incriminatrici di cui agli artt. 167 e 23) al fine di ostacolare l'applicazione dell'art. 24, lett. c), norma chiara e univoca che esclude il fatto tipico di reato (*ex* art. 167[55]).

Comunque, quandanche si ritenesse l'indebito utilizzo sostanzialmente assimilabile al trattamento illecito *ex* art. 167 cod. privacy, bisognerebbe rilevare che non solo l'indebito utilizzo, ma anche il furto d'identità digitale integrerebbe la detta fattispecie dato che anche la "raccolta" di dati (che se non consensuale può ben dirsi "furto di dati") costituisce un "trattamento" ai sensi dell'art. 4, lett. a). Ciononostante non ci sarebbe corrispondenza biunivoca tra l'ipotesi speciale *extra* codicistica e le nuove aggravanti introdotte all'art. 640 *ter* c.p. Infatti, non tutti i "trattamenti illeciti" coinciderebbero con un abuso dell'identità digitale altrui, dal momento che solo la sostituzione digitale di persona costituisce circostanza aggravante[56].

C'è ora da chiedersi se, a valle di quanto detto, può prospettarsi un'ipotesi di concorso di reati tra la frode informatica aggravata e il trattamento illecito di dati.

7. Concorso di reati tra frode informatica e violazione del codice della privacy.

Per quanto, come sopra detto, il trattamento illecito di dati (*ex* art. 167 cod. privacy) è totalmente incluso nell'ipotesi di "sostituzione d'identità digitale commesso con furto

[49] European Data Protection Supervisor (P. Hustinx), *Opinion on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"*, 16 novembre 2012, par. 41.

[50] Cass. pen., Sez. III, 15 febbraio 2005, n. 5728, in *Dir. informatica*, 2005, 499, con nota di A. Di Ronzo, che chiarisce che la mera iscrizione a pagine internet a nome altrui, qualora non esponga i dati alla pubblica consultazione *online*, consiste nella mera comunicazione all'*internet service provider* (imprenditore privato) di dati altrui e dunque non trattandosi di diffusione o comunicazione sistematica si ritiene applicabile l'art. 5 e quindi il trattamento non è sottoposto agli obblighi del d.lgs. 196 del 2003.

[51] C. Flick, *op. cit.*, pp. 526 ss.

[52] Cfr. ad esempio Garante privacy, *Privacy e propaganda elettorale. Decalogo elettorale* - 12 febbraio 2004 *(G. U. n. 45 del 24 febbraio 2004)* da cui si evince che l'autodeterminazione della sfera privata non possa essere compromessa dalla pubblicazione di dati in pubblici elenchi, se non quando vi sia un interesse contrapposto, ugualmente meritevole di tutela.

[53] Cass. pen., Sez. III, 15 febbraio 2005, n. 5728, cit.

[54] Tuttavia cfr. S. Aterno, *Deregulation della Cassazione in materia di privacy?,* Cass. pen., fasc.11, 2005, p. 3514, che sottolinea la necessità di dimostrare che i dati si trovino in pubblici registri, elenchi, atti o documenti dove sono stati raccolti nel rispetto delle procedure previste, e che è impensabile un'equiparazione forzosa tra i dati presenti indistintamente nel *web* e i detti registri od elenchi.

[55] Sull'inopportunità di utilizzare clausole generali nelle fattispecie incriminatrici, Cfr. D. Castronovo, *Clausole generali e diritto penale*, in *Dir. pen. cont.*, 2010, che definisce "intollerabile" un ricorso a clausole generali in *malam partem* nel diritto penale; F. Bricola, *La discrezionalità nel diritto penale, I, Nozione e aspetti costituzionali*, Milano, 1965, 33 ss., 157 ss. (che si esprime in termini di "concetti giuridici indeterminati", ovvero *unbestimmte Rechtsbegriffe*); F. Palazzo, *Il principio di determinatezza nel diritto penale. La fattispecie*, Padova, 1979, pp. 421 ss. ("elementi valutativi"); C. Luzzati, *La vaghezza delle norme. Un'analisi del linguaggio giuridico*, Milano, 1990; G. Contento, *Clausole generali e regole di interpretazione come "principi di codificazione"*, in *Valore e principi della codificazione penale: le esperienze italiana, spagnola e francese a confronto*, Padova, 1995, pp. 109 ss.

[56] Mentre ad esempio tutto ciò che non riguarda sostituzione di persona, ma mero traffico non consentito di dati personali a fini commerciali, concorrenziali, ecc., non potrebbe considerarsi possibile circostanza aggravante dell'art. 640 *ter* c.p.

o indebito utilizzo di dati identitari", se si confronta la norma con la fattispecie di frode informatica nella sua completezza, non si può fare a meno di notare che i beni giuridici rimangono diversi (patrimonio nell'una e riservatezza dei dati personali nell'altra), e che ci si trova di fronte ad un rapporto di specialità bilaterale per aggiunta, dal momento che nella frode informatica l'ingiusto profitto con altrui danno è elemento costitutivo, mentre nel trattamento illecito è richiesto il dolo specifico di vantaggio o danno e il "nocumento" è solo una condizione obbiettiva di punibilità[57].

Ovviamente, qualora il trattamento illecito sia solo prodromico ad una frode informatica commessa con sostituzione d'identità digitale e distinto da questa, si tratterebbe di un concorso materiale, tuttavia si applicherà comunque il cumulo giuridico (con i regimi edittali sopra detti) trattandosi di un medesimo disegno criminoso *ex* art. 81 c.p.

È vero, tuttavia, che l'art. 167 cod. privacy presenta una clausola di riserva, ovvero "quando il fatto non costituisca più grave reato": la dottrina ha ritenuto che tale clausola escluda il concorso di reati ogniqualvolta la violazione della norma in oggetto costituisce esclusivamente una modalità di commissione di altro e più grave reato "cioè, ad esempio, quando costituisca il mezzo per la commissione di una truffa o di un abuso in atti d'ufficio[58]".

Al contrario, la giurisprudenza ha richiesto per l'assorbimento del reato di trattamento illecito di dati nella fattispecie "più grave" che i due reati siano a tutela dello stesso bene giuridico[59], escludendo dunque nell'ipotesi in commento tale assorbimento. In tal caso si tratterebbe di un concorso formale e dunque di un cumulo giuridico della pena.

8. Conclusioni.

Traendo le fila, la definizione dell'indebito utilizzo nonché il rapporto col furto d'identità digitale possono essere ricostruiti solo facendo leva sulla rubrica dell'articolo: "sostituzione d'identità digitale". L'indebito utilizzo e il furto d'identità, dunque, sono sì fattispecie produttive dello stesso effetto (la frode informatica commessa con sostituzione digitale di persona tramite un uso di dati senza il consenso della vittima), ma alternative quanto a modalità di esecuzione: nel furto di dati la violazione del consenso vi è già nel momento della ricezione dei dati; nell'indebito utilizzo, invece, il possesso dei dati è lecito, ed è solo un determinato utilizzo non concordato che va a integrare la violazione.

L'indebito utilizzo, pertanto, si integra ogniqualvolta la sostituzione di persona tramite tecnologie informatiche avvenga attraverso dati posseduti lecitamente per altri scopi (e solo in questo caso va ad intersecare il trattamento illecito di dati *ex* art. 167 cod. privacy, non assorbendolo, in quanto si tratta di norme in rapporto di specialità bilaterale e che tutelano un diverso bene giuridico) o dati noti o presenti in pubblici registri (ed in questo caso ipotesi totalmente nuova e indipendente rispetto all'art. 167 cod. privacy che invece prevede un'esimente nel caso di tali dati, *ex* art. 24 cod. privacy).

[57] Cfr. in tal senso Cass. pen., Sez. III, 9 luglio 2004, n. 30134, in *GDir,* 2004, n. 35, 67; Cass. pen., Sez. III, 17 febbraio 11, 1^, Rv. 249991; da ultimo Cass. pen., Sez. II, 24 maggio 2012, n. 23798, in *Diritto & Giustizia*, 2012, fasc. 0, 487, con nota di A. Ferretti; in dottrina Cfr. L. Manna, *Commento al d.lg. 196/03, DPP,* 2004, 17; V. Destito, *Dati personali (tutela penale dei),* (I agg.), *Digesto Online*, 2008, che hanno interpretato il nocumento come una condizione obiettiva di punibilità poiché non si spiegherebbe la presenza del dolo specifico di profitto "o" di danno se poi il danno stesso fosse parte costitutiva della fattispecie, del resto se così non fosse il nocumento dovrebbe rientrare nel rappresentazione soggettiva, quand'anche sia necessario anche il solo dolo specifico di "profitto" (e non anche di danno, data la presenza di una disgiuntiva). Di opinione contraria D. Ielo, V. Saponara, in AA.VV., *Codice della privacy,* II, Milano, 2004, 2148 e AA.VV., *Codice in materia di dati personali,* Milano, 2004, 710.

[58] V. Destito, *op. cit.*, per cui "il concorso, invece, andrà ammesso — in virtù della peculiarità del bene giuridico tutelato (che è quello al rispetto della riservatezza e, quindi, della persona) — ogni qual volta altra fattispecie penale si sovrapponga solo parzialmente, cioè quando vi sono elementi della fattispecie dell'art. 167, 1° co., che sono ultronei rispetto alla diversa norma presa in considerazione". Analogamente cfr. M.C. Bisacci, *Tutela penale dei dati personali*, in *Digesto Online*, 2005.

[59] Cass. pen., Sez. II, 7 maggio 2013, n. 36365 (Rv. 256877), *CED* Cassazione, 2013, per cui "la clausola di riserva '*salvo* che il *fatto costituisca* più *grave reato*' presuppone, perché operi in concreto il meccanismo dell'assorbimento, che il reato più grave sia posto a tutela del medesimo bene-interesse tutelato dal reato meno grave che deve essere assorbito. (Nella fattispecie è stato escluso che il delitto di trattamento illecito di dati personali potesse ritenersi assorbito nel più grave reato di ricettazione, dalla quale, peraltro, l'imputato era stato assolto)". Cfr. Anche Cass. pen., 11 aprile 1986, in *Resp. Civ. e Prev.*, 1987, 85 con nota di P. Zagnoni Bonilini per cui la clausola di riserva "*salvo* che il *fatto costituisca* più *grave reato*", non sempre è connessa con il problema del *concorso* apparente di norme e in particolare col principio di specialità o con quello di consunzione.