DR Diritto del Risparmio

DISRUPTIVE DIGITALIZATION E TUTELA PENALE DEI DATI FINANZIARI

di Veronica Clara Talamo*

Technological evolution and branching of informatic processes have revolutionized social and business relationships with unavoidable consequences on the treatment of financial data that, in the lack of legal classification, are tacitly marked as species of the broader genus of personal data, by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 – on the protection of natural persons with regard to the processing of personal data and on the free movement of such data – and by the Legislative Decree of 30 June 2003, n. 196.
Furthermore, the dematerialization of financial services has granted unknown protection measures to consumers, who sometimes are victims of crimes against their digital identities, which refers also to their financial assets.
This paper aims to analyse the connections between the digitalization of banking and financial services and the criminal consumers' protection of virtual identity and personal data, according to the Criminal Code and Privacy Code.

fascicolo 2/2020

ISSN 2704-6184

* Abilitata all'esercizio della professione forense presso la Corte d'Appello di Lecce. Specializzata in diritto penale e privacy.

Rivista di Diritto del Risparmio

Disruptive digitalization e tutela penale dei dati finanziari[*]

di Veronica Clara Talamo[**]

Technological evolution and branching of informatic processes have revolutionized social and business relationships with unavoidable consequences on the treatment of financial data that, in the lack of legal classification, are tacitly marked as species of the broader genus of personal data, by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 – on the protection of natural persons with regard to the processing of personal data and on the free movement of such data – and by the Legislative Decree of 30 June 2003, n. 196.
Furthermore, the dematerialization of financial services has granted unknown protection measures to consumers, who sometimes are victims of crimes against their digital identities, which refers also to their financial assets.

This paper aims to analyse the connections between the digitalization of banking and financial services and the criminal consumers' protection of virtual identity and personal data, according to the Criminal Code and Privacy Code.

Maggio

Fascicolo 2/2020

---

[*] Contributo approvato dai referee

[**] Abilitata all'esercizio della professione forense presso la Corte d'Appello di Lecce. Specializzata in diritto penale e privacy

Abstract

L'evoluzione tecnologica e la ramificazione dei processi informatici hanno rivoluzionato le relazioni commerciali e sociali con inevitabili ricadute sul trattamento dei dati finanziari che, lungi dall'avere una qualificazione giuridica, sono tacitamente contrassegnati come *speciem* del più ampio *genus* dei dati personali dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 – relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati – e dal Decreto Legislativo 30 giugno 2003, n. 196. La smaterializzazione dei servizi finanziari ha, inoltre, introdotto inedite istanze di tutela in capo ai consumatori, i quali sono spesso vittime di condotte illecite in danno della propria identità digitale, dimensione che comprende anche lo *status* economico-patrimoniale.

Il presente contributo, pertanto, si pone di approfondire le interconnessioni tra la digitalizzazione dei servizi bancario-finanziari e la tutela penale dell'identità virtuale e dei dati personali degli utenti, rispettivamente alla luce del Codice Penale e del rinnovato Codice Privacy.

---

1. ***Free flow of data*** **nella morsa del** ***General Data Protection Regulation.***

La crisi finanziaria del 2009 e la riduzione dei margini di profitto delle imprese d'investimento e di prestito sono state terreno fertile per lo sviluppo del *Fintech*[1] (c.d. Finanza Tecnologica), settore caratterizzato dal concorso dei processi digitali alla creazione di servizi e di relazioni finanziarie connotate da una dimensione tecnologica (si pensi alle prestazioni *home banking* in luogo di quelle erogate presso gli sportelli degli istituti di credito oppure alla contrattazione telematica dei servizi assicurativi come forma alternativa alla trasmissione delle dichiarazioni negoziali).

Questa tecnologia ha garantito la circolazione delle risorse economiche mediante canali inaspettati, aprendo le porte del mercato finanziario anche a *players* diversi da quelli istituzionali; si è, inoltre, assistito all'aumento del potere computazionale e alla moltiplicazione di piattaforme mediante le quali vengono raccolte e scambiate informazioni circa gli *assets* patrimoniali, le abitudini e la propensione al rischio dei consumatori.

[1] V. G. P. LA SALA, *Intermediazione, disintermediazione, nuova intermediazione: i problemi regolatori*, in AA.VV., *Diritto del FinTech*, a cura di M. CIAN-C. SANDEI, Milano, Wolters Kluwer Italia, 2020, 3.

Tuttavia, se da un lato la fruibilità dei predetti dati si riconnette al fenomeno della c.d. *data-driven economy* – dove gli operatori del settore raccolgono e processano i dati a carattere economico mediante le tecniche di *big data analytics* al fine di offrire ai consumatori dei servizi non standardizzati (in ambito del prestito, del finanziamento, degli investimenti e dei sistemi di pagamento), che rispondano al principio del *know your customer* – dall'altro lato devono farsi i conti con il diritto alla protezione dei dati personali alla luce del Regolamento UE 2016/679 (di seguito anche GDPR, in luogo di *General Data Protection Regulation*)[2] che, abrogando la Direttiva 95/46/CE[3], ha profondamente mutato il quadro normativo, portando il legislatore domestico a un intervento di adeguamento del D. Lgs. n. 196/2003[4] (successivamente Codice Privacy).

Infatti, gli operatori economici non raccolgono soltanto i dati strettamente personali dell'utente (come l'anagrafica, il codice fiscale, l'indirizzo e-mail, etc…), ma anche informazioni circa la preferenza degli strumenti di pagamento, la propensione al contenzioso, il merito creditizio, potendo acquisirli dal medesimo al momento dell'instaurazione del rapporto contrattuale (che può coincidere con l'apertura del conto corrente oppure con il rilascio degli strumenti di pagamento) o potendoli attingere da soggetti, pubblici o privati, esterni agli istituti bancario-finanziari (si pensi alle agenzie di *rating* oppure all'Ufficio di Stato Civile territorialmente competente); e, in conseguenza di ciò, il consumatore appare uno dei principali attori dello scenario del trattamento dei dati personali, come emerge dalle espressioni "interessato al trattamento" o "consenso dell'interessato" che ricorrono a più riprese nel GDPR.

Il Regolamento, innalzando il livello di tutela dei dati personali delle persone fisiche, ha evidenziato le falle di alcuni interventi legislativi che intersecano il tema della *privacy*, come nel caso della Direttiva 2015/2366/UE – anche detta *Payment Service Directive* 2 o PSD 2[5], che ha l'obiettivo di garantire la concorrenza, l'efficienza e la trasparenza dei servizi di pagamento ai fine di rafforzare la fiducia dei consumatori e di creare un *common level play field* per i prestatori di servizi già autorizzati (i *payment initiation service providers* che effettuano il servizio di disposizione degli ordini

[2] Cfr. Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

[3] Cfr. Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati.

[4] Cfr. D.L.vo 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) n. 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE.

[5] V. Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE.

di pagamento e gli *account information service providers* che eseguono servizi di informazione sui conti), cui possano accedere anche *third parties providers*.

Ciò fa comprendere come gli operatori del settore trattino un quantitativo inestimabile di dati personali che valutano in forma aggregata al fine di creare prodotti e servizi *end-to-end* e per garantire processi *paperless*, accompagnati da decisioni automatizzate sul merito creditizio.

In tali segmenti procedurali, caratterizzati dal "rischio della trasparenza" e dal "pericolo della sicurezza", l'educazione digitale e finanziaria dell'utente gioca un ruolo fondamentale, tanto più se si considera la mancanza di armonia tra la PSD 2 e il GDPR: infatti, se la Direttiva favorisce lo scambio dei dati (i quali possono disvelare preferenze e abitudini di acquisto interessanti tanto per gli operatori del settore bancario-finanziario, quanto per le imprese che offrono i relativi prodotti e servizi) dei consumatori tra i prestatori dei servizi di pagamento, il GDPR tutela i dati personali come espressione dell'autodeterminazione del singolo, anche in termini di cessione a terzi; inoltre, la PSD 2, prevedendo che le banche possano consentire ai diversi *providers* (tra cui i *third parties providers*) di accedere ai dati e ai conti dei propri clienti (c.d. *open banking*), incentiva i processi di *collection*, *datafication* e *digitalization*, che potrebbero collidere con i principi ispiratori del GDPR.[6]

2. *L'inquadramento giuridico dei dati finanziari.*

Nell'era dei *big data*, le informazioni personali sono considerate il "nuovo petrolio" dell'economia, fattore di squilibrio tra il potere economico delle entità commerciali che le trattano ed i diritti in capo ai consumatori, specie considerando che nel settore bancario-finanziario vige la regola *services for data*, che evidenzia come la prestazione del consenso al trattamento dei dati personali da parte dell'interessato sia la *conditio sine qua non* per ottenere l'erogazione dei servizi richiesti.

Infatti, il consenso – manifestazione revocabile in qualsiasi momento di volontà libera, specifica, informata e inequivocabile dell'interessato (art. 4 par. 11 GDPR) – è la base giuridica che legittima il trattamento che, ispirato ai principi di liceità, correttezza e trasparenza (art. 5 GDPR), è prodromico all'esecuzione degli obblighi – compresi quelli amministrativi e contabili – derivanti dal contratto del quale l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso, oppure per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (art. 6 GDPR).

[6] Così, M. RABITTI, *Il riparto di competenze tra autorità amministrative indipendenti nella Direttiva sui sistemi di pagamento*, in AA.VV., *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli interessi nella PSD2*, a cura di M. C. PAGLIETTI-M. I. VANGELISTI, Roma, Roma Tre-Press, 2020, 91 ss.

Sebbene la Convenzione di Strasburgo n. 108 del 28.01.1981[7] e il Regolamento UE 2016/679 non categorizzino i dati finanziari, tali sono ricompresi nel più ampio *genus* dei dati personali[8], che evidenziano anche lo *status* economico-patrimoniale dell'interessato.

Tuttavia, ad avviso di chi scrive, non sarebbe scorretto definirli para-sensibili perché necessitano di particolari misure per garantire l'esattezza e la sicurezza[9] del trattamento visto che attengono a rapporti bancari, celano dettagli circa il comportamento debitorio, l'affidabilità o la puntualità nei pagamenti dell'utente, evidenziano lo svolgimento di attività economiche, rivelano informazioni commerciali e comportamenti idonei ad esplicitare i gusti o le abitudini di consumo. Basti pensare, sotto il profilo pratico, che le operazioni di pagamento devono essere ispirate ai concetti di *privacy by design* – ossia pianificazione della gestione della *privacy* mediante la mappatura e il monitoraggio dei dati finanziari, la riorganizzazione dei flussi – e *privacy by default* – impostazione predefinita affinché il trattamento sia adeguato, pertinente e limitato al perseguimento delle finalità di tipo economico, soddisfacendo anche al principio di minimizzazione; inoltre, la tutela dei predetti dati è acuita dalle novità introdotte dal Regolamento UE, come il principio di *accountability*, cioè di responsabilizzazione del titolare (e, indirettamente, del responsabile del trattamento) in termini di tenuta dei registri delle attività di trattamento, adozione dei codici di condotta, svolgimento della DPIA – *data protection impact assessment*, nomina del *Data Protection Officer*.

3. *Il trattamento illecito dei dati personali in ambito bancario-finanziario.*

Il trattamento[10] dei dati personali può avvenire sia con l'ausilio di strumenti automatizzati[11] (fatta eccezione per l'ipotesi contemplata dal

---

[7] V. Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, Strasburgo, 28/01/1981.

[8] L'art. 4 par. 1 GDPR offre la definizione di "dato personale", intendendosi «*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*».

[9] Cfr. Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa, *Manuale sul diritto europeo in materia di protezione dei dati*, Lussemburgo, Ufficio delle pubblicazioni dell'Unione europea, 2018, 383.

[10] Cfr. art. 4 n. 2 GDPR circa il "trattamento", ossia «*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*».

[11] Cfr. art. 4 n.4 GDPR circa la "profilazione", ossia «*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze*

considerando 71 GDPR, laddove prevede che «*l'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online*», da leggersi in combinato disposto con l'art. 22 GDPR), che in modo manuale.

I dati personali, tuttavia, non sono detenuti esclusivamente dal titolare del trattamento (che coincide con l'istituto di credito), ma – per il perseguimento delle finalità di legge, contrattuali o commerciali – possono essere trasmessi a soggetti individuati normativamente (come l'Agenzia delle Entrare per finalità legate all'iscrizione o alla cancellazione dell'ipoteca sugli immobili; Consob, IVASS, Banca d'Italia e Banca Centrale Europea per funzioni di controllo e vigilanza, etc...), soggetti che svolgono servizi assicurativi e finanziari, consulenti, soggetti che prestano assistenza anche telefonica alla clientela, etc…, che tratteranno i dati ricevuti in qualità di "titolari autonomi", salvo il caso in cui siano stati designati dei responsabili per specifici trattamenti.

Laddove dalle condotte dei predetti attori emergano dei profili d'illiceità, tali risponderanno ai sensi dell'art. 167 D.Lgs. n. 196/2003, rubricato "Trattamento illecito di dati".

Infatti, procedendo alla disamina del c. 1 della fattispecie e per quanto d'interesse al predetto ambito, «*salvo che il fatto costituisca più grave reato*», è penalmente responsabile chi, «*al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato*», opera in violazione dell'art. 130 Codice Privacy rubricato "Comunicazioni indesiderate"[12], ossia chi tratta illecitamente i dati che il consumatore ha fornito per finalità commerciali relative all'invio di materiale pubblicitario, anche mediante tecniche di comunicazione a distanza (come corrispondenza postale, telefonate tramite sistemi automatizzati di chiamata, telefax, posta elettronica, messaggi SMS o MMS), circa iniziative, prodotti o servizi della banca o di terzi a fini promozionali, per effettuare azioni di vendita diretta, per verificare la qualità dei prodotti e dei servizi offerti, per realizzare ricerche di mercato.

Centrale è il c. 2 dell'art. 167 Codice Privacy che recita: *«Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septies*

personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica».

[12] L'art. 130 Codice Privacy – rubricato Comunicazione indesiderate – recita che «*…l'uso di sistemi automatizzati di chiamata o di comunicazioni di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il consenso del contraente o utente*» (c. 1), trovando applicazione quanto appena detto «*anche alle comunicazioni elettroniche, effettuate per finalità ivi indicate, mediante posta elettronica, telefax, messaggi del tipo Mms (Multimedia Messaging Service) o Sms (Short Message Service)…*», fatto salvo il diritto di opposizione di cui al comma 3-*bis*.

ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-quinquiesdecies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni».

Il legislatore, rinviando ad altre disposizioni, ha ritenuto penalmente rilevante il trattamento di categorie particolari di dati personali[13] non sotteso da motivi di interesse pubblico rilevante o non conforme agli accorgimenti a tutela dell'interessato (cfr. artt. 2-*sexies*, 2-*quinquiesdecies* Codice Privacy), in violazione delle misure di garanzia (art. 2-*septies* Codice Privacy) o dei principi relativi al trattamento di dati relativi a condanne penali e reati (art. 2-*octies* Codice Privacy).

Trattasi di un reato di pericolo concreto (considerato che la circostanza aggravante *«se dal fatto deriva nocumento»* è stata assorbita nell'inciso *«arreca nocumento all'interessato»*, superando lo schema di reato di pericolo presunto), per la cui integrazione è necessario che il soggetto agente – *rectius* "chiunque" – ponga in essere delle infrazioni procedurali idonee a esporre a pericolo la protezione dei dati personali dell'interessato, cagionando un vero e proprio nocumento, a nulla rilevando le mere irregolarità formali. L'elemento soggettivo del dolo specifico si rintraccia nel fine del profitto in favore di chi lo commette o di altri, ovvero nello scopo di arrecare un danno all'interessato, posta la necessaria e apprezzabile verificazione del nocumento che, rientrando nel *genus* del danno, può essere di tipo economico-patrimoniale o morale[14].

Tale schema si ripete anche al c. 3 dell'art.167 Codice Privacy, che prevede che la pena prevista dal c. 2 si irroghi a chi «*al fine di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45,46 o 49 del Regolamento, arreca nocumento all'interessato*», trovando forte applicazione nel settore *FinTech* per via della dimensione transnazionale e della natura commerciale delle operazioni. Infatti, sebbene le succitate disposizioni siano state abrogate a livello codicistico, il GDPR consente il trasferimento dei dati personali solo verso un Paese terzo o un'organizzazione internazionale in forza di una decisione di adeguatezza della Commissione Europea, in mancanza della quale deve farsi ricorso a

[13] L'art. 9 c. 1 GDPR recita che «*è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*». Sotto il profilo pratico, si tenga conto che i dati sensibili non sono richiesti dal titolare del trattamento, ma possono essere incidentalmente trattati per rispondere a specifiche operazioni richieste dall'interessato, come il pagamento di quote associative in favore di organizzazioni politiche e sindacali o l'emissione di bonifici in favore di associazioni religiose.

[14] Cfr. Cass. Pen. Sez. III, 13 marzo 2019, n.20013, sostiene che «*in tema di reati informatici, per la consumazione del reato di trattamento illecito di dati personali di cui al secondo comma dell'art. 167 del D.Lgs. n. 196/2003, è richiesto che la volontà del soggetto agente sia connotata dal porsi lo scopo ulteriore – alternativamente – del profitto (anche in vantaggio di terzi) o del danno, pur non occorrendo che tale fine venga effettivamente conseguito. Quanto all'elementi del "nocumento", con tale locuzione deve intendersi un pregiudizio giuridicamente rilevante di qualsiasi natura patrimoniale o non patrimoniale, subito dal soggetto passivo*».

clausole tipo, codici di condotta, meccanismi di certificazione e norme vincolanti d'impresa; inoltre, i dati potranno essere trasferiti a fornitori localizzati in USA, purché censiti nel *Privacy Shield*, accordo che tutela i diritti fondamentali delle persone fisiche nell'Unione Europea.[15] (art. 44 ss. GDPR).

Sotto il profilo della procedibilità, «*il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante*» (c. 4) ed «*il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni delle disposizioni di cui al presente decreto*» (c. 5); inoltre, stante il principio del *ne bis in idem* previsto dal considerando 149 GDPR, la pena dev'essere diminuita se il Garante, in base della disciplina interna e sovranazionale, ha già applicato o riscosso per il medesimo fatto una sanzione amministrativa (c. 6).

4. *Ulteriori illeciti penali previsti dal Codice Privacy.*

Per completezza del quadro normativo di riferimento, giova brevemente analizzare le fattispecie residuali previste dal Codice Privacy.

L'art. 167-*bis* Codice Privacy, rubricato "Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala", punisce chi comunica o diffonde[16] un archivio automatizzato o di una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala[17] in

[15] V. Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa, *Manuale sul diritto europeo in materia di protezione dei dati*, cit., 281 ss.

[16] Quanto all'elemento oggettivo della condotta deve rinviarsi all'art. 2-*ter* par. 4 Codice Privacy (oppure all'art. 4 c. 1 lett. l-m Codice Privacy) che recita «*si intende per: a) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione; b) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione*».

[17] Cfr. considerando 91 GDPR, che chiarisce che i trattamenti su larga scala «*mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, nonché ad altri trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti. È opportuno altresì effettuare una valutazione d'impatto sulla protezione dei dati nei casi in cui i dati personali sono trattati per adottare decisioni riguardanti determinate persone fisiche in seguito a una valutazione sistematica e globale di aspetti personali relativi alle persone fisiche, basata sulla profilazione di tali dati, o in seguito al trattamento di categorie particolari di dati personali, dati biometrici o dati relativi a condanne penali e reati o a connesse misure di sicurezza. Una valutazione d'impatto sulla protezione dei dati è altresì richiesta per la sorveglianza di zone accessibili al pubblico su larga scala, in particolare se effettuata mediante dispositivi optoelettronici, o per altri trattamenti che l'autorità di controllo competente ritiene possano presentare un rischio elevato per i diritti e le*

violazione degli artt. 2-*ter*, 2-*sexies*, 2-*octies* Codice Privacy (c.1) oppure in difetto del consenso dell'interessato che è richiesto per le operazioni di comunicazione e diffusione (c. 2).

La disposizione delinea un reato a dolo specifico che si caratterizza per l'intenzione di danneggiamento che può riguardare anche terzi diversi dall'interessato e per la presunzione implicita di nocività, considerato che non ricorre il riferimento al nocumento. Diversamente, l'art. 167-*ter* Codice Privacy, rubricato "Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala", punisce chi, con artifizi o raggiri, ha acquisito un archivio automatizzato (o una parte sostanziale dello stesso), configurandosi un reato commissivo a dolo specifico alternativo, lesivo della tutela della riservatezza dell'individuo e del possessore dell'archivio automatizzato.

Pertanto, in entrambi i casi, potrebbero profilarsi tali condotte all'interno degli enti bancari e finanziari che – per via del volume di dati oggetto di trattamento, il numero di soggetti interessati a tale operazione, estensione spazio-temporale dell'attività – trattano dati definibili su "larga scala".

In ultima analisi l'art. 168 Codice Privacy punisce chi, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiari o attesti falsamente notizie o circostanze, produce atti o documenti falsi (c. 1) o pone in essere delle condotte ostative alla speditezza dei procedimenti e degli accertamenti svolti dall'autorità di controllo (c. 2); mentre l'art. 170 Codice Privacy riconosce la responsabilità penale di chiunque non osservi, pur essendovi tenuto, il provvedimento adottato dal Garante ai sensi dell'art. 58 par. 2 lett. f) GDPR (circa la «*limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento*») oppure i provvedimenti confermativi di prescrizioni contenute nelle vecchie autorizzazioni generali (compatibilmente al Regolamento UE e al Decreto di adeguamento interno).

5. *Quali rimedi a presidio dell'identità digitale?*

A latere delle condotte illecite che i soggetti depositari della tenuta dei dati personali potrebbero porre in essere in ragione delle proprie funzioni istituzionali, è, altresì, centrale il fenomeno della criminalità informatica che ha portato il legislatore ad intervenire normativamente per tutelare il patrimonio dei consumatori (comprensivo sia della dimensione statica del singolo, che del valore dinamico dei risparmi o degli investimenti), la regolare e corretta operatività degli strumenti informatici, svecchiando il Capo II del Titolo XIII del Codice Penale, non apparendo coerente assimilare l'impiego truffaldino dei dispositivi tecnologici all'induzione in errore di cui all'art. 640 c.p.

---

libertà degli interessati, specialmente perché impediscono a questi ultimi di esercitare un diritto o di avvalersi di un servizio o di un contratto, oppure perché sono effettuati sistematicamente su larga scala. Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato. In tali casi non dovrebbe essere obbligatorio procedere a una valutazione d'impatto sulla protezione dei dati».

Infatti, con Legge 23 dicembre 1993 n. 547, il legislatore ha introdotto l'art. 640-*ter* c.p., rubricato "Frode informatica", che punisce «*chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno*». La fattispecie sembra cucita sull'art. 615-*ter* c.p. per coincidenza del bene giuridico tutelato – ossia il domicilio informatico che consiste in uno spazio ideale o fisico dove sono contenuti i dati informatici di pertinenza della sfera individuale – e sullo schema della truffa, distinguendosi dall'art. 640 c.p. per mancanza degli artifizi, dei raggiri e dell'induzione in errore[18].

Ai fini dell'integrazione della fattispecie *de quo* è sufficiente che l'attività fraudolenta – alternativamente consistente nell'alterazione o nell'intervento abusivo – ricada sul sistema informatico in uso alla persona offesa, la quale verrà investita solo in via mediata dalla condotta illecita per difetto della propria cooperazione artificiosa.

Dunque, il sistema informatico o telematico è piegato agli interessi del soggetto agente che può alterare «*in qualsiasi modo*» o intervenire «*senza diritto*» (in assenza di autorizzazione o di altro titolo legittimante) sulla memoria dell'elaboratore – cioè su dati (registrazioni elementari effettuate mediante simboli che, a seguito d'interpretazione, divengono informazioni elaborabili dal *computer*), informazioni o programmi (gruppi di istruzioni che consentono all'elaboratore di compiere specifiche operazioni)[19] – al fine di conseguire un'ingiusta locupletazione a seguito dell'aggressione unilaterale del patrimonio informatico del consumatore.

La manomissione di tali apparecchi, incidendo sulla componente fisica (*hardware*) o logica (*software*), determina una deviazione funzionale del sistema – anche detta "distrazione del sistema" – che, anziché elaborare i dati secondo schemi predefiniti, produrrà degli esiti irregolari (si pensi alla manipolazione del *software* del programma adoperato per il calcolo degli interessi dovuti dalla banca sugli accrediti dei clienti che, attuando un percorso "illogico", defrauda gli arrotondamenti minimi in favore dei legittimati per farli confluire sul conto dell'agente); al contrario, l'intervento

---

[18] Così, A. FANELLI, *Frode informatica*, in AA.VV., *Codice Penale. Rassegna di giurisprudenza e di dottrina. Volume XII – I delitti contro il patrimonio, Libro II, Artt. 624-649*, Milano, Giuffrè Editore, 2010, 563. L'Autore specifica che l'assenza di tali elementi sia giustificata dal fatto che la nuova fattispecie «*a causa delle difficoltà di concepire un inganno ordito ai danni di una macchina, è chiamata a sopperire la truffa in tutti i casi i cui l'elaboratore ha sostituito il processo decisionale di un essere umano nella valutazione di situazioni rilevanti sul piano economico*». Tuttavia, per difetto dell'induzione in errore, la condotta potrebbe astrattamente integrare il delitto di furto con mezzo fraudolento dal momento che la condotta illecita prescinde dalla cooperazione della vittima, atteggiando ad aggressione unilaterale, mediante manipolazione, dei dati informatici.

[19] Cfr. A. FANELLI, *Frode informatica*, cit., 564. L'Autore riporta un caso di *rounding-down fraud*, anche detta "tecnica del salame", che prevede che il sistema sia alterato *ab origine* al momento della creazione: il programma sarebbe messo a punto per consentire al programmatore di accreditare sul proprio conto bancario piccolissime decurtazioni ottenute mediante arrotondamenti per difetto (anziché per eccesso, come richiesto dalla banca committente) sugli interessi di migliaia correntisti.

può consistere in una pluralità di operazioni a contenuto tecnico-informatico che incidono direttamente o indirettamente sull'esito regolare del sistema operativo, determinando l'alterazione o la soppressione dei dati oggetto di elaborazione, l'introduzione nel sistema di dati non autorizzati o falsi[20].

Inoltre, vi è un inasprimento del trattamento sanzionatorio «*se il fatto è commesso con abuso della qualità di operatore del sistema*», attribuendosi tale veste a chi – in qualità di analista, operatore o programmatore – opera sul sistema informatico o telematico per svolgere il proprio incarico (titolo legittimante) ai sensi dell'art. 640-*ter* c. 2 c.p.

L'incessante evoluzione delle tecnologie informatiche ha portato all'introduzione – mediante l'art. 9 c. 1 lett. a) D.L. 14 agosto 2013, convertito con modificazioni nella L. 15 ottobre 2013 n. 119 – del c. 3 dell'art. 640-*ter* c.p., che disciplina una circostanza aggravante indipendente se «*il fatto è stato commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti*», enunciando due specificazioni modali diverse dalla condotta tipizzata al c. 1.

Infatti, se il furto richiede l'apprensione illecita delle chiavi di accesso d'autenticazione, l'indebito utilizzo dell'identità digitale consiste nell'uso non autorizzato di *username* e *password*.

Tale intervento normativo ha inaugurato anche un'evoluzione linguistico-tecnologica[21] nelle Corti, che sovente usano il termine *phishing*[22] per identificare la condotta illecita di cui all'art. 640-*ter* c. 3 c.p.

---

[20]Quanto all'alterazione di un sistema informatico o telematico ai sensi dell'art. 640-*ter* c.p., Cass. Pen., Sez. II, 12 dicembre 2019, n. 50395; Cass. Pen. Sez. II, 11 luglio 2019, n. 30480.

[21] V. M. AGOSTINIS-A. FASULO, *Home banking, abusi nei sistemi informatici e phishing: possibili responsabilità a carico della banca*, in *Rivista di Giurisprudenza ed Economia d'Azienda*, Milano, Franco Angeli, 2014, 151. Gli Autori osservano come nel nostro ordinamento giuridico non vi sia la definizione del *phishing*, termine che deriverebbe dal verbo "*to fish*", quasi ad intendere delle tecniche volte a carpire, mediante un accesso abusivo al sistema informatico o mediante l'invio di *e-mail* – i dati dei rapporti di conto corrente intrattenuti dai clienti con le banche o le poste, al fine di impiegarli fraudolentemente per clonare carte di credito o pagamento, oppure per trasferire i fondi sui conti dei soggetti agenti, che poi li preleveranno creando una dispersione del contante. Tra le varie tecniche di captazione si segnala l'uso del servizio di *home banking*. V. anche A. TENCATI, *Il conto corrente bancario. I contratti tra banche e clienti*, Vicalvi, Key Editore, 2018, p. 149 ss., lì dove si chiarisce che col termine *phishing* s'intende il furto di identità in danno degli utenti del sistema di *home banking* – contratto di servizi, non disciplinato né dal Codice Civile né dal T.U.B., che consente ai medesimi di accedere a prodotti e servizi del comparto bancario-finanziario mediante delle piattaforme informatiche – tramite *e-mail* contraffatte nel mittente e nell'indicazione di siti c.d. civetta, al fine di veicolare i fondi degli utenti su carte prepagate o su conti nella disponibilità degli autori dell'illecito.

[22] Cfr. Trib. Trento, 04 maggio 2016, ha affermato che «*in tema di reati contro il patrimonio, il phishing è quell'attività illecita in base alla quale, attraverso vari stratagemmi, o attraverso fasulli messaggi di posta elettronica o, ancora, attraverso veri e propri programmi informatici e malware, un soggetto riesce ad impossessarsi fraudolentemente dei codici elettronici di un utente, che poi utilizza per frodi informatiche consistenti, di solito, nell'accedere a conti correnti bancari o postali che vengono rapidamente svuotati. La suddetta truffa presuppone, poi, la partecipazione di un terzo "collaboratore", c.d. financial manager, ossia colui che si presta a che le somme che l'hacker trafuga dal conto corrente nel quale è entrato abusivamente vengano accreditate*

Trattasi di una condotta di *social engineering* volta a carpire i dati personali dell'utente (come chiavi di autenticazione all'*home banking*, codici delle carte di pagamento, numero del conto corrente) per accedere abusivamente ed in suo luogo ai servizi bancari *on-line*. Preludio del *phishing attack* è la ricezione di un'*e-mail*[23] apparentemente proveniente dall'ente preposto (posta, istituto di credito, etc…) mediante cui, a causa dell'apposizione di loghi e recapiti che simulano la grafica istituzionale, la vittima è indotta a connettersi alla *web page* indicata nel corpo del testo e ad autenticarsi, rendendo le proprie credenziali note all'agente, il quale può, inoltre, captarle qualificandosi come rappresentante della persona giuridica nel corso di una chiamata (*phishing VoIP*) o adoperando dei *software* autoinstallanti (*trojan*, *malware* e *keylogger*) in grado di decifrare il sistema informatico o telematico e trasmettergli automaticamente le informazioni dell'utente.

Non vi è univocità interpretativa circa la qualificazione giuridica di suddette condotte.

Pare plausibile parlare di truffa semplice nell'ipotesi in cui la vittima sia erroneamente indotta – mediante la ricezione di *e-mail* fraudolente e *link* di siti-clone – ad inserire le proprie credenziali (seppur desta perplessità la mancanza di compartecipazione negli atti di disposizione patrimoniale); mentre, l'alterazione unilaterale del dispositivo informatico o telematico sarebbe astrattamente idonea ad integrare il delitto di frode informatica.

Se la distinzione concettuale tra le fattispecie di cui agli artt. 640 e 640-*ter* c.p. appare cristallina (laddove la prima richiede l'apporto del soggetto passivo e la seconda si concreta in una manomissione unilaterale del sistema informatico o telematico), dal punto di vista pratico pare difficoltoso stilare

---

sul proprio conto corrente al fine, poi, di essere definitivamente trasferite all'estero con operazioni di money transfert».

Per quanto concerne la responsabilità dell'istituto di credito, cfr. Cass. Civ., Sez. I, 03 febbraio 2017, n. 2950, secondo cui «*la responsabilità contrattuale dell'istituto di credito in caso di operazioni bancarie non "riconosciute" dal correntista è esclusa soltanto ove la banca provi il dolo di questi o l'adozione di comportamenti talmente incauti da non poter essere fronteggiati in anticipo. In mancanza di tale prova, il rischio è posto a carico dell'istituto di credito che, agendo secondo la diligenza professionale dell'avveduto banchiere, valutata tenendo conto di tutti i rischi tipici delle specifiche attività poste in essere, è tenuto a prevederlo e gestirlo*». In dottrina, nota di S. MARTINELLI, *Sicurezza informatica degli istituti di credito e responsabilità contrattuale*, in Giur. It, 2017, X, 2069 ss., che scrive che «*in materia di operazioni effettuate sul conto online e non riconosciute dal cliente, la responsabilità della banca è esclusa solo ove essa provi il dolo del cliente o l'incauto comportamento da questi adottato, tale che, per la sua imprevedibilità, non poteva essere fronteggiato in anticipo mediante l'adozione di misure di sicurezza adeguate ad evitarlo. La Corte, nel fondare la sua decisione, tiene conto, in particolare, della particolare diligenza richiesta all'operatore bancario, della migliore allocazione del rischio d'impresa, della tutela del contraente debole e della necessità di garantire la fiducia degli utenti nella sicurezza del sistema*». V. anche G. MINICUCCI, *Le frodi informatiche*, in AA.VV., *Cybercrime*, Milano, Utet, 841.

[23]Così, M. AGOSTINIS-A. FASULO, *Home banking, abusi nei sistemi informatici e phishing: possibili responsabilità a carico della banca*, cit., 154, a tal proposito giova segnalano che è preferibile diffidare da indirizzi *e-mail* lunghi e con caratteri inusuali, dalla richiesta di inserimento dei codici di accesso alla *home banking* mediante *pop-up* (anziché tramite la pagina del sito).

attorno al *phishing* un giudizio di tipicità per via della poliedricità delle condotte illecite.

Tant'è che non possono escludersi degli elementi di contatto con l'art. 494 c.p., anche se l'invio delle *e-mail* in luogo dell'ente istituzionale non equivale a sostituzione della persona fisica: per tali ragioni, l'orientamento prevalente sostiene che il *phisher* debba rispondere del reato di sostituzione di persona in concorso con gli artt. 615-*ter* e 640 c.p. perché, inducendo in errore l'utente, ottiene le credenziali di accesso al servizio informatico o telematico per disporre abusivamente le operazioni bancario-finanziarie in suo favore[24].

Le discrepanze interpretative, inoltre, scontano la sofisticazione della tecnica c.d. di abboccamento atteso che talora il corpo dell'e-*mail* appare capzioso, tal altra il *pisher* dissimula le vesti di famigliari e colleghi della vittima (*spear phishing*). Spesse volte si parla di *pharming* per indicare un tipo truffa che consiste nell'alterazione del funzionamento della rete istituzionale mediante la modifica della corrispondenza numerica del *server* DNS affinché l'utente, pur avendo selezionato l'indirizzo *web* corretto, venga re-indirizzato su un pagina identica a quella del sito istituzionale; invece, si adopera l'espressione *Man in The Middle Attack* per identificare l'*hackeraggio* della casella di posta della vittima (impresa o privato) al fine d'intercettare le comunicazioni relative a operazioni commerciali ed inviare all'*account* violato

[24] Cfr. Cass. Pen., Sez V, 20 gennaio 2016 n. 11918, espone che nel primo segmento della condotta potrebbe configurarsi il reato di sostituzione di persona (sebbene ciò ingenera dubbi in capo a chi, ritenendo che si tratti di una fattispecie a forma vincolata, ha evidenziato come l'agente si sostituisca ad istituti bancari e postali, non a persone fisiche); nel secondo segmento si integrerebbe l'accesso al servizio informatico altrui, mediante cui l'agente porrebbe in essere delle operazioni in suo favore (difettandosi, quindi, dell'elemento dell'induzione in errore, potendosi rintracciare la cooperazione della vittima solo nell'erronea prestazione del consenso per l'installazione di *software* spia); Trib. Milano, 7 novembre 2011, sostiene che «*commette reato di sostituzione di persona, truffa e utilizzo indebito di carte di credito chi illecitamente sottrae numeri di carte di credito inviando a diversi soggetti sms ingannevoli nei quali, prospettando acquisti mai effettuati dai legittimi titolari, invita questi ultimi a contattare un numero telefonico dove una voce registrata, spacciandosi per il call center dell'istituto emittente, richiede i dati delle suddette carte. I dati così raccolti, in alcuni casi, sono utilizzati per effettuare degli acquisti*»; Trib. Milano, 7 ottobre 2010, afferma che «*chi utilizza tecniche di "phishing " per ottenere, tramite artifici e raggiri e inducendo in errore l'utente, le credenziali di autenticazione necessarie ad accedere abusivamente a spazi informatici esclusivi del titolare (ad es. relativi alla gestione dei conti correnti "on-line") e a svolgere, senza autorizzazione, operazioni bancarie o finanziarie, può rispondere dei delitti di cui agli artt. 494 (sostituzione di persona), 615-ter (accesso abusivo a sistemi informatici o telematici) e 640 c.p. (truffa). Sono penalmente responsabili coloro che, senza essere concorsi nel reato presupposto, nella piena consapevolezza della provenienza illecita o, comunque, accettandone il rischio - purché non desunto da semplici motivi di sospetto, bensì da una situazione fattuale inequivoca - a seguito di proposte di collaborazione in internet, tramite e-mail, contatti in chat o messaggi allocati su pagine "web", e la prospettazione di facili guadagni in relazione alla semplice attività richiesta ai cd. "financial manager", pongono all'incasso e successivamente trasferiscono somme di denaro, tutte provenienti da delitti non colposi*».

In dottrina, M. AGOSTINIS-A. FASULO, *Home banking, abusi nei sistemi informatici e phishing: possibili responsabilità a carico della banca*, cit., 152, nel tentativo di dare un inquadramento, il *phishing* potrebbe astrattamente integrare le fattispecie previste dagli artt. 640, 640-*ter*, 615-*ter* o 617-*sexies* c.p.

la variazione delle coordinate bancarie per ottenere il corrispettivo delle operazioni[25].

Alla luce di ciò, tali discrasie interpretative sembrerebbero conseguenza di un intervento legislativo superficiale ed inadeguato innanzi alla poliedricità delle condotte fraudolente, apparendo – a distanza di diversi anni – ancora attuale il comunicato con cui la Commissione delle Comunità Europee[26] ribadiva la necessità di una tutela a tutto tondo dell'identità digitale, da graduarsi in base alle diverse fasi e forme del furto, apparendo auspicabile l'iniziativa del legislatore europeo al fine di armonizzare i sistemi penali degli Stati Membri, trattandosi di un fenomeno criminoso a carattere globale.

6. *In conclusione*.

Il processo di digitalizzazione dell'economia ha profondamente mutato le relazioni finanziarie e sociali che s'intrecciano all'interno di dimensione immateriale, fluida, iperconnessa, *real-time*, dove i dati, motore dell'economia, circolano ad una velocità inarrestabile.

Nel panorama dei servizi finanziari digitali, i *big data* abbracciano sempre più il tema della tutela della persona e della propria identità digitale, che deve fare i conti sia con l'uso massivo di internet e delle tecnologie informatiche, che con la raccolta e il trattamento dei dati personali. In tale cornice il diritto veicola l'evoluzione tecnologica verso binari di tutela, enfatizzando la correttezza dei servizi offerti e l'*empowerment* dei consumatori: da un lato vi è il Regolamento (UE) 2016/679 che, bilanciando le istanze consumeristiche e lo sviluppo del mercato dei mega-dati, appresta idonei strumenti a tutela dei dati personali, anche consentendo agli Stati Membri di stabilire delle norme concernenti misure punitive (cfr. art. 84 GDPR, considerando che l'Unione Europea, ai sensi dell'art. 83 par. 2 TFUE, ha solo un potere generale di indirizzo in materia criminale, non potendo il Regolamento disciplinare delitti e illeciti contravvenzionali); dall'altro lato il Codice Penale tutela l'individuo, la sua dimensione digitale e i propri dati personali, che rappresentano il prolungamento della dimensione umana.

---

[25] V. F. Di Resta, *Tutela dell'interessato e sanzioni*, in *La nuova "Privacy Europea". I principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, Torino, Giappichelli, 2018, 178. *A latere* del *pharming*, recentemente si parla di *vishing* per identificare la tecnica mediante cui i frodatori carpiscono i dati della vittima del reato mediante sistemi *voip* e *call canter*, oppure lo *smishing* che prevedere l'ottenimento delle password mediante gli SMS. Ancora si parla di *Man In The Middle* (MITM) per identificare la condotta del truffatore che, durante una sessione di lavoro al PC, accede alla comunicazione tra l'utente e l'istituto di credito ponendo in essere atti di disposizione del denaro sul conto corrente proprio o di terzi, potendo anche sfruttare la debolezza del *browser* mediante la tecnica del *Man in The Browser* (MITB). In tale ultimo caso viene adoperato un programma malevolo, che si frappone tra il sistema centrale dell'intermediario ed il singolo utente, il quale, navigando su una pagina esattamente identica a quella istituzionale, inserisce le proprie credenziali.

[26] Cfr. Commissione delle Comunità Europee, COM (2007) 267, *Comunicazione della Commissione al Parlamento Europeo, al Consiglio e al Comitato delle Regioni – Verso una politica generale di lotta contro la cibercriminalità*, Bruxelles, 22 maggio 2007.

Il nostro presente è profondamente mutato l'8 maggio 1997, quando è entrata in vigore la L. 31 dicembre 1996 n. 195, ed il nostro avvenire sarà tanto mutevole quanto apparirà inarrestabile l'ondata rivoluzionaria portata dalla *privacy*, costruzione destinata a non essere mai compiuta.

All'intero di un mercato così complesso ed innovativo, la ricostruzione dei diritti dev'essere coerente con la dimensione tecnologica all'interno della quale sono esercitati, al fine di estendere le garanzie della libertà personale non solo all'*habeas corpus*, ma anche – riprendendo le parole di Stefano Rodotà[27] – all'*habeas data*. In conclusione, il rispetto dei diritti fondamentali dell'uomo è una sfida vera e propria che, per quanto difficile, potrà essere "vinta" solo se si comprenderà che l'evoluzione dell'era digitale non involge il singolo in quanto tale, ma anche la sua identità sempre più plastica.

[27] V. Garante Privacy, *Relazione 2004 – Discorso del Presidente Stefano Rodotà*, 16.