

“Internet delle cose” e problematiche giuridiche: alcune considerazioni

ROBERTA RUGGIERI¹

SOMMARIO: 1. Introduzione: i vantaggi dell’IoT – 2. I benefici più evidenti – 3. Le problematiche relative alla privacy – 4. Le problematiche correlate ai dispositivi indossabili – 5. Il problema dei droni – 6. Alcune conclusioni circa la sicurezza dei dispositivi

1. Introduzione: i vantaggi dell’IoT

Tutti gli oggetti e tutti gli aspetti della realtà e della vita saranno presto interconnessi tramite i sensori: reti, cioè, ad altissima velocità in grado di raccogliere, elaborare e interpretare dati. Cambieranno, così, gli stili di vita, il modo di comunicare, di relazionarsi e di lavorare.

Si realizzerà, finalmente, in modo pervasivo ciò che è già stato definito “Internet of Things” (IoT), grazie al quale gli oggetti del nostro mondo quotidiano semplificheranno la vita degli individui e, al contempo, i nuovi dispositivi IoT produrranno nuovi tipi di dati.

Nel sistema del mondo commerciale, l’Internet of Things incrementerà l’efficienza aziendale, permetterà di sfruttare l’intelligenza di una vasta gamma di attrezzature, renderà migliori le attività e aumenterà la soddisfazione dei clienti. Esso avrà, anche, un impatto profondo sulla vita delle persone: migliorerà la sicurezza pubblica, il trasporto e l’assistenza sanitaria grazie a un’informazione più accurata e a comunicazioni più veloci.

Ci sono, infatti, almeno tre vantaggi principali dell’IoT con riferimento all’impatto che avrà in ogni azienda, e sono vantaggi includenti: la comunicazione, il controllo e la riduzione dei costi.

¹ Dottoressa in Giurisprudenza, Perfezionata in Data Protection e Investigazioni Digitali presso l’Università degli Studi di Milano.

Per ciò che riguarda la comunicazione, l'IoT trasmette informazioni a persone e sistemi, come lo stato e la salute delle attrezzature, i dati provenienti da sensori in grado di monitorare i segni vitali di una persona.

In passato, nella maggior parte dei casi, non si aveva accesso a questo tipo di informazioni oppure le stesse venivano raccolte manualmente. Ad esempio: un sistema HVAC abilitato IoT oggi può riferire se il filtro dell'aria è pulito e funziona correttamente. Così, nel settore sanitario, l'Internet of Things oggi può aiutare un ospedale a tenere traccia della posizione di ogni attrezzatura, dalle sedie a rotelle agli strumenti per i defibrillatori cardiaci utili ai chirurghi. E nel settore dei trasporti, l'Internet delle cose è in grado di fornire il monitoraggio in tempo reale degli oggetti in spedizione e la condizione dei vari plichi.

Considerando il controllo e l'automazione, in molti casi, in un mondo connesso, un'azienda o un consumatore sarà in grado anche di controllare un dispositivo da remoto. Ad esempio, un'azienda potrà accendere o spegnere una parte specifica di attrezzature o regolare la temperatura a distanza. Già adesso un consumatore può utilizzare l'IoT per sbloccare l'automobile o avviare una lavatrice. Stabilite, perciò, le linee guida, un processo può inviare avvisi per anomalie e, eventualmente, fornire una risposta automatica. Ad esempio, se le pastiglie dei freni su un camion sono sul punto di guastarsi, il processo di Internet può automaticamente programmare la manutenzione.

Per quanto riguarda la riduzione dei costi, molte aziende adotteranno l'IoT al fine di risparmiare denaro.

Con l'IoT un'azienda potrà risparmiare denaro riducendo al minimo i guasti e permettere alla stessa di eseguire la manutenzione programmata. I sensori possono anche misurare elementi, come il comportamento di guida e la velocità, per ridurre i costi di carburante e l'usura. Nuovi contatori intelligenti nelle case e nelle aziende possono anche fornire dati che aiutino le persone a comprendere il consumo di energia e le opportunità di risparmio sui costi.

Abstract

“Internet delle cose” e problematiche giuridiche: alcune considerazioni

L'articolo è incentrato sull'IoT e sui problemi relativi alla privacy. Negli ultimi anni gli sviluppi tecnologici hanno determinato un'evoluzione della Rete. Si assiste alla nascita dell'Internet delle cose, o propriamente detto Internet degli oggetti o IoT, acronimo dell'inglese Internet of Things.

L'interrogativo centrale è il seguente: quando ogni essere umano e ogni cosa saranno collegati, quali confini bisognerà fissare per garantire la tutela del diritto individuale alla privacy?

È chiaro che se non si trova il giusto equilibrio fra trasparenza e diritto alla privacy, lo sviluppo dell'Internet delle cose rischia di procedere a rilento o, ancor peggio, di interrompersi irrimediabilmente.

“Internet of Things” and legal problems: a few remarks

This article focused on the IoT and the problems of privacy. In the last few years, the development of technologies has created an evolution of the net, that is to say the IoT, acronym of the English term “Internet of Things”. The most important question is: when every man and everything will be net, which boundary lines will be fixed to guarantee the protection of the individual right to privacy? If it is not possible to find a balance between transparency and the right to privacy, the development of the Internet of Things will risk to proceed slowly or will necessary stop.

Roberta Ruggieri

Smart contracts:

traiettorie di un'utopia divenuta attuabile

STEFANO CAPACCIOLI

SOMMARIO: 1. Introduzione – 2. Contratti telematici – 3. Blockchain e criptovalute – 4. Inquadramento civilistico – 5. Smart contracts – 5.1. Introduzione giuridica – 5.2. Parti contrattuali – 5.3. Livello di automazione – 5.4. Livello di separazione – 6. Analisi – 6.1. – Casi particolari – 7. Conclusioni (aperte)

1. Introduzione

Uno degli argomenti più complicati del panorama *FinTech*¹ è costituito dagli *smart contracts*, materia che conduce a riflessioni e ragionamenti che si sovrappongono e che tendono a confondersi.

Gli *smart contracts* non corrispondono alla traduzione di “contratti intelligenti”, né tantomeno hanno alcun riferimento alla *buzzword* “smart”, che peraltro sta riempiendo gli scritti di molti commentatori (anche perché suona bene e ha un significato positivo).

Per sgombrare il campo dagli equivoci, lo *smart contract* non è un contratto, né si sostituisce al contratto in alcuna forma.

In realtà l'intuizione del concetto di *smart contract* è da ricondurre a Nick Szabo, che in un post² del 1994 scrisse:

Uno smart contract è un protocollo di transazione computerizzato che esegue i termini di un contratto. Gli obiettivi generali del disegno dello smart contract sono il soddisfacimento di condizioni contrattuali comuni (come ad esempio i termini di pagamento, i privilegi, la riservatezza, e anche l'esecuzione), la ridu-

¹ Per *FinTech* si intende la tecnofinanza (*Financial Technology*), vale a dire la fornitura di servizi finanziari attraverso le tecnologie dell'informazione.

² Cfr. N. SZABO, *Smart Contracts*, 1994, in <http://szabo.best.vwh.net/smart.contracts.html> (sito web consultato, e documento disponibile online, il 22 febbraio 2016).

zione al minimo delle eccezioni sia dannose che accidentali e la minimizzazione della necessità di intermediari fiduciari. Gli obiettivi economici correlati includono l'abbassamento dei costi di perdita a causa di frodi, di arbitrato e di esecuzione e degli altri costi di transazione.

L'intuizione consisteva nella creazione di un protocollo informatico che riducesse o eliminasse le possibilità d'inadempimento. L'idea è innovativa e rivoluzionaria, anche se con forti difficoltà tecniche e tecnologiche, quali, ad esempio, l'impossibilità di sostituire il giudizio umano con quello della macchina o di un algoritmo.

Talvolta, però, i visionari intercettano delle innovazioni tecnologiche (e in questo caso contribuiscono anche a crearle) che rendono fattibile ciò che è e sembra utopico.

L'innovazione delle criptovalute³ ha reso possibile questo protocollo che fino a ieri restava più teorico che pratico o meglio, che ricadeva in categorie concettuali conosciute invece che in campi inesplorati.

Lo sviluppo tecnologico recente fonda le sue radici nella realizzazione di alcune idee di Wei Dai⁴ e di Timothy C. May⁵, di cui si presenta una traduzione del Manifesto dei Cripto Anarchici apparso in una *mailing list* nel 1992 ma che risale al Settembre del 1988 (!):

Uno spettro si aggira nel mondo moderno, lo spettro della Cripto anarchia. La tecnologia informatica è sul punto di fornire la possibilità a individui e gruppi di comunicare e interagire con gli altri in un modo del tutto anonimo. Due persone possono scambiarsi messaggi, condurre affari e negoziare contratti elettronici senza mai conoscere il nome vero o l'identità legale dell'altra. Le interazioni su reti saranno irrintracciabili, con vasto re-instradamento di pacchetti crittografati e involucri inalterabili che implementano protocolli crittografici con la quasi assoluta certezza contro qualsiasi manomissione. La reputazione avrà importanza primaria, con molta più centralità nelle transazioni che i rating di credito

³ Cfr. S. CAPACCIOLI, "Introduzione al trattamento tributario delle valute virtuali: criptovalute e bitcoin", su «Diritto e Pratica Tributaria Internazionale», CEDAM, n. 1/2014, pag. 27-68.

⁴ Cfr. <http://www.weidai.com/bmoney.txt> (sito web consultato, e documento disponibile online, il 22 febbraio 2016).

⁵ Cfr. T.C. MAY, *The Crypto Anarchist Manifesto*, 1988, in <http://www.activism.net/cyberpunk/crypto-anarchy.html> (sito web consultato, e documento disponibile online, il 1 marzo 2016).

Abstract

Smart contracts: *traiettoria di un'utopia divenuta attuabile*

Lo smart contract non è un contratto ma è un protocollo per computer che facilita, verifica, fa rispettare la negoziazione o l'esecuzione di un contratto; può anche evitare la necessità di una clausola contrattuale. In questo articolo si analizzano le implicazioni tecniche e giuridiche, proponendo uno schema di analisi, individuando elementi vulnerabili e proponendo interpretazioni sostenibili. La base teorica inizia dall'intuizione di Nick Szabo, resa pienamente possibile dall'avvento delle criptovalute.

Smart contracts: the path from utopia to feasibility

A smart contract is not a contract but it is a computer protocol that facilitates, verifies or enforces the negotiation or execution of a contract or it avoids the need for a contract clause. This Article analyzes the smart contracts and under a technical and legal perspective and it proposes an analytical framework, sustainable interpretations, and potential vulnerabilities. The theoretical basis is based on Nick Szabo studies, intuition that becomes possible with the introduction of cryptocurrencies.

Stefano Capaccioli

Il processo civile telematico in appello

VINCENZO CONTE

SOMMARIO: 1. Introduzione – 2. Tecnologia e giurisdizione – 2.1. I principi di efficienza, garanzia e qualità per l'efficacia della giurisdizione – 2.2. Tecnologia e giurisdizione – 2.3. L'organizzazione del sistema giudiziario tra iniziative strategiche e innovazioni – 2.4. Il PCT nel "distretto" della Corte di Appello di Milano – 2.5. Iniziative strategiche connesse al PCT – il ruolo degli UNEP – 2.6. I rapporti fra Dirigenti e MAGRIF: incompatibilità tra RID e MAGRIF – 2.7. RID e UDI: collegialità dell'Ufficio dei Referenti Distrettuali per l'Informatica – 2.8. Gli Uffici per l'Innovazione – 2.9. L'Ufficio per il Processo – I Tirocinanti in Corte di Appello – 3. Il Passaggio del fascicolo di primo grado in appello – 3.1. Iscrizione a ruolo del fascicolo di secondo grado – 3.2. Richiesta e trasferimento del fascicolo – 3.3. Ipotesi e proposte di modifiche evolutive in Corte di Appello – 3.4. Ipotesi e proposte di modifiche evolutive in 1° grado – 3.5. Visualizzazione dello storico e atti del primo grado – 3.6. Richiesta cartacea del fascicolo di primo grado – 3.7. Consolle del magistrato – 3.8. Impatti della presente evolutiva – 4. La designazione del Collegio – 4.1. Inserimento, nei registri di cancelleria, dell'intero collegio giudicante – 5. Altri interventi previsti in Corte di Appello – 5.1. Introduzione dell'esperto quale membro del collegio – 5.2. Previsione dell'ordinanza di inammissibilità con filtro collegiale – 5.3. Firma e controfirma remota – 5.4. Allarme provvedimenti monocratici – 5.5. Adeguamento maschere per l'appello

1. Introduzione

Il Processo Civile Telematico in Corte di Appello di Milano, un Ufficio Giudiziario che per struttura, composizione, problematiche è diverso dagli uffici giudiziari di primo grado, e sul quale l'impatto del PCT è vissuto, sia come occasione di svolta culturale, nella consapevolezza che il modo di fare giurisdizione sta cambiando, e sia come ufficio di vertice, che guarda al proprio distretto, già avviato telematicamente, e in alcuni casi virtuoso, assume risvolti particolarmente interessanti e meritevoli d'attenzione.

La Corte di Appello, soprattutto in ambito PCT, ha assunto il ruolo e l'impegno di chiamare a raccolta il distretto, fare rete, creare gruppi di lavoro in cui i più virtuosi mettano a disposizione degli altri le loro esperienze e le loro capacità, condividere gli umori, essere ufficio di riferimento, ma anche e soprattutto dare risposte, non solo sotto forma di pronunce giurisprudenziali, ma in quanto capace di prendere per mano gli uffici meno virtuosi e portarli a livello degli altri, affinché il dialogo con ognuno di loro sia costruttivo e partecipativo.

L'attuazione del PCT in Appello passa attraverso una scelta organizzativa a "cerchi concentrici" con previsione di una sede di lavoro più ampia, che coinvolga il Distretto in tutte le sue componenti (magistrati, avvocati, personale di cancelleria, UDI, CISIA, fornitore) – attraverso attraverso l'individuazione di referenti – e una sede di sperimentazione più ristretta.

Nel primo ambito, sono state elaborate linee guida omogenee e soluzioni tecniche condivise diffuse e veicolate nel distretto.

Il secondo ambito, sperimenta soluzioni tecniche condivise in relazione: 1) allo svolgimento dell'udienza telematica mediante utilizzo di consolle; 2) alla predisposizione di una bozza di formalizzazione degli atti tipo (sentenza/atti costitutivi del difensore) nonché all'individuazione di modalità di allegazione dei documenti, per una migliore gestione del flusso telematico nel processo di secondo grado.

Il Processo Civile Telematico in Corte di Appello è stato reso possibile anche grazie ai progetti di informatizzazione dell'Amministrazione della Giustizia finanziati con fondi Expo che hanno consentito agli uffici giudiziari milanesi di essere scelti come sedi sperimentali-pilota a livello nazionale.

Il contratto di affidamento alla società fornitore dei Sistemi, individua le migliorie urgenti alla Consolle del Magistrato per la Corte d'Appello di Milano e relativi servizi di supporto. Il Progetto prevede la realizzazione degli interventi legati a:

- a. passaggio del fascicolo informatico dal primo al secondo grado;
- b. rendere più fluido il lavoro del collegio sulla Consolle del Magistrato;
- c. evoluzioni varie sul SICID (Sistema Informatico Contenzioso Civile) e Consolle del Magistrato

Abstract

Il processo civile telematico in appello

L'obiettivo é quello di illustrare il PCT in Corte di Appello a Milano, ufficio in cui lavoro come cancelliere addetto all'Ufficio Innovazione. Si parte dalle caratteristiche dell'ufficio di secondo grado, come la composizione collegiale senza trascurare una impostazione giuridica spesso distante dal mondo dell'informatica. Si analizzano gli elementi caratterizzanti il PCT in appello, e cioè, "il passaggio del fascicolo di primo grado in appello" e la "Designazione del collegio". Si chiude con gli interventi richiesti per adeguare il Sicid (Registro Informatizzato di Cancelleria) all'appello: la terminologia degli Stati Evento, le maschere utilizzate, finora hanno fatto riferimento esclusivamente al primo grado. La nuova funzionalità denominata "Designazione del Collegio", o in previsione, la "firma collegiale" e la "Consolle dell'udienza collegiale", sono strumenti studiati esclusivamente per il processo di appello.

The electronic civil trial ("PCT" in Italian) in appeal

The objective is to illustrate the PCT in the Court of Appeal in Milan, the office in which I work as clerk of the court, in charge of Office Innovation. The paper starts from the characteristics of the second degree office, such as its collegial composition, without neglecting a legal setting which is often far-removed from the world of IT. The elements characterising the PCT in appeal are analysed and, that is, "the transition of the case file from first degree to appeal" and the "*Designazione del Collegio*" (Designation of the Panel of Judges). It closes with the actions required to adjust the Sicid (Computerised Register of the Office of the Clerk of the Court) at appeal: the terminology of the *Stati Evento*, the masks used so far have referred exclusively to the first degree. The new functionality called "*Designazione del Collegio*", or as planned, the "*firma collegiale*" (collegial signature) and the "*Consolle dell'udienza collegiale*" (Collegial hearing console), are tools which have been developed exclusively for the appeal trial.

Vincenzo Conte

Alcune questioni problematiche circa il voto elettronico

SILVIA ELIA¹

SOMMARIO: 1. Il diritto di voto – 2. I sistemi di *Electronic Voting* – 3. Panoramica sulle criticità e sui benefici dei sistemi di voto elettronico – 4. Il voto elettronico nei processi elettorali – 5. Il voto elettronico nei processi decisionali-deliberativi e partecipativi – 6. *E-Voting* e *E-Democracy* – 7. Conclusioni

1. Il diritto di voto

Le tematiche inerenti il voto elettronico sono complesse ed allo stesso tempo particolarmente interessanti poiché coniugano da un lato principi solidi e fondamentali come la libertà e la democrazia e, dall'altro lato, le potenzialità offerte dalle nuove tecnologie dell'informazione e della comunicazione in continua evoluzione.

Per affrontare correttamente il tema si ritiene utile, preliminarmente, effettuare alcuni brevi cenni generali ai principi generali in materia di voto per poi valutarne (l'eventuale) compatibilità con i sistemi di votazione elettronica e i possibili ambiti applicativi.

Il diritto di voto può essere definito come il diritto a prendere parte ad un processo elettorale o decisionale-deliberativo manifestando la propria volontà attraverso l'espressione di una preferenza² costituendo allo stesso tempo un dovere civico ex art. 48 Cost. L'atto materiale del voto è, quindi, un elemento comune a diverse tipologie di procedimenti, ovvero quelli elettorali per le elezioni politico-istituzionali e referendarie, nei processi decisionali-deliberativi ed elettivi svolti in ambito privatistico (assemblee di società, associazioni o enti generalmente intesi), infine può

¹ Laureata in Giurisprudenza presso l'Università degli Studi di Milano, Master Universitario di primo livello in Diritto delle Nuove Tecnologie e Informatica Giuridica, Avvocato del Foro di Milano.

² Vedi la voce "diritto di voto" in Enciclopedia Treccani, <http://www.treccani.it/enciclopedia/diritto-di-voto/>.

trovare applicazione in attività di tipo consultivo-partecipativo; ciascuna delle aree sopra citate ha le proprie peculiarità che vanno ad incidere sull'utilizzo dei sistemi elettronici, nella presente analisi si cercherà quindi di illustrare tali specificità.

Sempre in termini generali, nei processi elettorali/elettivi, un soggetto può essere titolare di una duplice capacità di elettorato, attivo e passivo; l'elettorato attivo è la capacità giuridica di partecipare in qualità di elettore ad una votazione esprimendo la propria preferenza per uno o più candidati che concorrono a rivestire cariche pubbliche o private, l'elettorato passivo è la capacità giudica individuale a ricoprire cariche elettive.

Nell'ordinamento italiano l'analisi sul diritto di voto deve necessariamente muovere dalla Costituzione Repubblicana, la quale detta alcuni principi fondamentali in materia di voto, ed in particolare, dall'articolo 48 Cost.³; la norma sancisce al primo comma il principio del suffragio universale, riconoscendo a tutti i cittadini maggiorenni l'elettorato attivo e passivo mentre nel secondo comma fissa quattro requisiti essenziali del voto, quali: "personalità, uguaglianza, libertà e segretezza"⁴.

La personalità del voto implica che il diritto possa essere esercitato solo dal titolare dello stesso attraverso l'espressione di un solo ed unico voto, ciò al fine di evitare il voto delegato e il voto per procura, non ammessi nel nostro ordinamento; solo in caso di grave impedimento fisico – e con l'adozione di determinate cautele – è consentito all'elettore disabile di avvalersi di un accompagnatore⁵. Il requisito dell'uguaglianza intende attribuire al singolo voto il medesimo valore degli altri senza alcuna distinzione, discriminazione o influenza derivante dal sogget-

³ Art. 48 Costituzione Italiana: «1. Sono elettori tutti i cittadini, uomini e donne, che hanno raggiunto la maggiore età. 2. Il voto è personale ed eguale, libero e segreto. Il suo esercizio è dovere civico. 3. La legge stabilisce requisiti e modalità per l'esercizio del diritto di voto dei cittadini residenti all'estero e ne assicura l'effettività. A tale fine è istituita una circoscrizione Estero per l'elezione delle Camere, alla quale sono assegnati seggi nel numero stabilito da norma costituzionale e secondo criteri determinati dalla legge. 4. Il diritto di voto non può essere limitato se non per incapacità civile o per effetto di sentenza penale irrevocabile o nei casi di indegnità morale indicati dalla legge».

⁴ Cfr. A. GRATTERI, *Il valore del voto, nuove tecnologie e partecipazione elettorale*, Padova, Cedam 2005, par. II, pp. 75-99; E. BETTINELLI, "La lunga marcia del voto elettronico in Italia", in «Quaderni dell'osservatorio Elettorale», 2002, pp. 10-18.

⁵ Art. 55 Dpr n. 361/1957, sul punto cfr.: E. BETTINELLI "Diritto di voto", in «Digesto delle discipline pubblicistiche», Torino, 1990, pp. 227 ss.

Abstract

Alcune questioni problematiche circa il voto elettronico

La presente analisi mira a fornire una breve panoramica generale delle tematiche inerenti la materia del voto elettronico; partendo dal dato normativo ed individuando i principali ambiti applicativi saranno illustrati alcuni sistemi di e-voting mettendo in evidenza le problematiche, i punti di forza e di debolezza di tali tecnologie e le possibili soluzioni; infine verranno forniti alcuni spunti di riflessione.

A set of problems related to electronic voting

This paper provides a brief overview of the topics related to the field of electronic voting; it will be described the background legal framework and the main application areas, then it will be observed typical features of e-voting systems and the different potential solutions and options, as well as an overview of strengths and weaknesses of this technologies, lastly the article will conclude with some reflections.

Silvia Elia

La *jihād* 2.0: profili economici, tecnologici, giuridici

MARIATERESA FIOCCA¹, IVAN DI PIETRO², NICOLA TIGRI²,
FRANCESCO CICIRIELLO³

SOMMARIO: 1. Premessa – 2. La *jihād* 2.0: “modernità liquida” – 3. Le asimmetrie rispetto alle parti avversarie e i rispettivi costi – 4. Le fonti di finanziamento – 5. L’economia della paura – 6. Le nuove frontiere tecnologiche della *jihād* 2.0 – 6.1. I diversi livelli del web – 6.2. La *jihād* sul web – 6.2.1. Propaganda – 6.2.2. I mezzi di scambio: il “mito” delle valute virtuali – 7. Strumenti di contrasto della *jihād* 2.0 e il “captatore di Stato” – 8. Conclusioni

1. Premessa

Il terrorismo islamico si sta evolvendo. L’istituzione dello Stato Islamico costituisce la base per la creazione di una nuova forma di lotta agli infedeli. Si può dire che la nuova *jihād* assuma caratteristiche di “liquidità” in diversi settori: dalla pervasività della propaganda, agli infiniti canali di finanziamento.

In questo contesto, la tecnologia assume un ruolo centrale, sia per la semplicità con cui consente di comunicare con i futuri martiri di Allah, sfruttando, paradossalmente, le piattaforme telematiche degli stessi infedeli (si pensi ai *social network*), sia per l’uso “bellico” che se ne può fare (*cyber warfare*).

D’altro canto, nonostante la ancora più marcata asimmetria che caratterizza il nuovo terrorismo, a svantaggio dell’Occidente, la tecnologia può essere utilizzata come strumento d’*intelligence*, prevenzione e repressione, nonostante tutti i limiti derivanti, oltre che dalla tecnolo-

¹ Professore di Economia presso la Scuola Nazionale dell’Amministrazione (SNA), Presidenza del Consiglio.

² Dottore in Giurisprudenza.

³ Dottore in Ingegneria Informatica e Ph.D in Sistemi artificiali intelligenti.

gia stessa, da ciò che è considerato *politically correct* e dai vincoli imposti dall'impianto di valori delle democrazie occidentali.

È in questo complesso contesto sociologico ed economico che la tecnologia crea un substrato in cui si affrontano forze contrapposte.

2. La jihād 2.0: “modernità liquida”

Rispetto ai conflitti convenzionali o simmetrici, la *jihād* di “seconda generazione” appare una guerra “liquida” (mutuando la metafora di Zygmunt Bauman⁴): liquida è la sua percezione circa i confini di altri territori/Stati che tende ad “inondare” per impadronirsene, insieme alle proprie risorse (tipicamente, giacimenti di petrolio); mille i rivoli con cui si finanzia; tanti gli *asset* occidentali di cui progressivamente si impadronisce per combattere l'avversario stesso (dalla finanza alla tecnologia), “inonda” il cuore del “nemico lontano” inducendolo fino alla revisione della propria Carta costituzionale (Francia); mettendo in discussione il diritto internazionale, secondo cui è un obbligo l'accoglimento di profughi in fuga da guerre e persecuzioni; raggiungendo le Istituzioni UE, e mettendo a dura prova la coesione comunitaria, pregiudicando l'*acquis* di Schengen e l'accesso alla “rotta balcanica” di migliaia di rifugiati; destruttura la normalità degli stili di vita, della quotidianità, delle *routine* (via “economia della paura”). Liquido è l'oro di cui l'Isis si serve quale principale risorsa economica⁵.

Inoltre, l'attuale *jihād* – pur mostrando tratti comuni ad al-Qaeda del periodo di bin Laden e di al-Zarqawi – quali la trilogia terrorismo-criminalità-collusione –, esprime un “*new deal*” più pragmatico, ambizioso e moderno⁶: possiede un proprio territorio – un sedicente Stato –; ha una banca centrale e batte moneta; salvo importanti eccezioni⁷, si è pres-

⁴ Cfr. Z. BAUMAN, *Modernità liquida*, Laterza, Bari, 2011.

⁵ Cfr. par. 5.

⁶ La rottura con al-Qaeda risale al 2013, con il conseguente messaggio ai giovani *jihādisti* che l'Isis è il “nuovo”. Cfr. M. MOLINARI, *Il Califfato del terrore. Perché lo Stato islamico minaccia l'Occidente*, Milano, Bur 2015.

⁷ Si sospetta che, tra il 2013 e il 2014 – con trasferimenti di circa 2 milioni di dollari al mese – il suo maggiore finanziatore sia stato il Qatar, che, nella sua ambivalenza, intrattiene comunque buoni rapporti anche con gli USA, di cui ospita un comando del-

Abstract

La jihād 2.0: profili economici, tecnologici, giuridici

Il presente contributo ha l'obiettivo di esaminare l'attuale *jihād* – chiamata a tale proposito *jihād 2.0*, così da differenziarla da quella scaturita con bin-Laden – sotto diversi profili.

La prima parte fornisce il contesto socio-economico, che enfatizza l'evoluzione nel tempo della *jihād* (qui parliamo di prima e seconda generazione rispettivamente). Tali aspetti ci conducono a valutare la modernità del nuovo terrorismo, perfino impadronendosi degli *asset* occidentali più sofisticati. Fra questi, la tecnologia, naturalmente.

Quest'ultima è centrale nell'analisi svolta, e viene trattata in modo estremamente diffuso e aggiornato. Vengono proposti anche alcuni contro-argomenti per spiegare come sia limitata la sovrapposizione fra terrorismo e valute virtuali, quali il più noto Bitcoin.

Infine, vengono analizzati gli aspetti giuridici legati alla *jihād*, insieme ai nuovi problemi di natura giuridica che sorgono con essa, nonché i limiti di cui vengono a soffrire le attuali legislazioni (sia a livello internazionale che nazionale) per contrastare questo terrorismo.

Jihād 2.0: Economic, technological, legal aspects

The present paper is aimed at exploring the nowadays *jihād* – purposely called here *jihād 2.0*, in order to differentiate it from that one stemming from bin-Laden – from several viewpoints.

The first part provides us with a socio-economic context emphasizing the evolution of *jihād* across time (we talk about the first and the second generations respectively). Such aspects lead us to appreciate the modernity of the new terrorism, even by capturing the most sophisticated Western “assets”. Obviously enough, among them, technology.

The core of the paper is devoted particularly to such an aspect, in quite a comprehensive and updated overview. Some counter-arguments are also proposed in that they try to explain the little overlapping between terrorism and virtual currencies, such as the quite well-known Bitcoin.

Eventually, the legal aspects associated to the *jihād* are explored together with the new legislative problems such a terrorism arise as well as the limits that today law (both the international and the domestic ones) suffers to contrast such a terrorism.

Mariateresa Fiocca, Ivan Di Pietro, Nicola Tigri, Francesco Ciciriello

Tra tutela dell'identità personale e tutela dell'*account* nella decisione n. 56 dell'11 febbraio 2016 del Garante per la protezione dei dati personali

COSTANZA MARTANI¹

SOMMARIO: 1. Il caso – 2. Policy di *Facebook* – 3. Applicabilità della normativa nazionale – 4. Diritto alla protezione dei dati personali, diritto al nome, diritto all'identità personale quali diritti fondamentali che contribuiscono a definire l'autodeterminazione informativa

1. Il caso

Un utente di *Facebook*, titolare di valido *account* aperto dal medesimo, a proprio nome, utilizzando i servizi offerti da *Facebook Italy srl*, si rivolgeva nel novembre del 2015 al Garante per la protezione dei dati personali (d'ora in avanti Garante) con ricorso presentato ex art. 145 e ss. del Codice per la protezione dei dati personali² (d'ora in avanti Codice), rappresentando di essere stato vittima di minacce, tentativo di estorsione nonché sostituzione di persona ed indebita intrusione in sistema informatico da parte di una persona, anche essa utente di *Facebook*, con la quale (in seguito a richiesta di "amicizia") aveva inizialmente intrattenuto corrispondenza telematica confidenziale ma che, in seguito aveva posto in essere l'illecita condotta sopra evidenziata. L'utente non aveva accettato di sottostare alle richieste estorsive svolte da tale soggetto, di talché l'autore dell'illecito dava seguito alla minaccia creando un falso *account* a nome del ricorrente, utilizzando i dati personali di quest'ultimo nonché la sua immagine ed inviando a tutti i contatti di *Facebook* del ricorrente medesimo, fotografie e video creati ad arte con fotomontaggi, gravemente lesivi dell'onore e del decoro oltre che della immagine sia privata che pubblica dell'utente.

¹ Avvocato del Foro di Perugia.

² D.lgs. n. 196 del 30 giugno 2003.

In particolare le fotografie e i video artefatti con fotomontaggio, inviati dal falso *account* a tutti i contatti del ricorrente, ritraevano quest'ultimo intento in attività sessuali anche con minori.

Appresa la grave circostanza per essere stata segnalata dai riceventi delle false fotografie, l'utente si rivolgeva prontamente a *Facebook* tramite il servizio *online* (non essendo prevista altra possibilità di contattare il *social network* per un pronto intervento finalizzato a bloccare ed eliminare il falso *account* oltre che tutti i messaggi e le fotografie immessi in rete). Solo dopo circa 24 ore il ricorrente aveva avuto notizia dai propri contatti che il falso profilo *Facebook* era stato eliminato, alcuna comunicazione perveniva invece da *Facebook* allo stesso. L'utente aveva dunque inviato a *Facebook Ireland Ltd*, titolare del trattamento dei dati degli utenti *Facebook*, una richiesta di accesso ai dati sia ai sensi della Sezione V della Direttiva 95/46/CE, così come recepita nella Sezione IV dell'*Irish Data Protection Act* sia ex art. 7 del Codice di protezione dei dati personali, chiedendo la conferma dell'esistenza e la comunicazione in forma intellegibile di tutti i dati ed informazioni detenuti in relazione ai profili *Facebook* aperti a nome del ricorrente e con la sua immagine nonché di conoscere l'origine dei dati, la finalità del trattamento, le modalità del medesimo, gli estremi identificativi del titolare del trattamento e del responsabile, i soggetti o le categorie di soggetti ai quali i dati erano stati comunicati o che potevano venire a conoscenza degli stessi, richiedendo inoltre la cancellazione ed il blocco del falso *account* e dei dati inseriti e condivisi sul *social network* in violazione di legge e relativa attestazione che tale intervento fosse stato portato a conoscenza, anche per quanto riguarda il contenuto, di coloro ai quali i dati erano stati comunicati o diffusi, opponendosi al trattamento di tali dati.

Facebook dava riscontro a tale richiesta tramite *e-mail* nella quale invitava il ricorrente a leggere le informazioni ivi contenute per conoscere le tipologie e le modalità di accesso ai dati personali trattati da *Facebook*, limitandosi ad invitarlo a «consultare la nostra "Normativa sui dati" (<https://www.facebook.com/about/privacy/>), contenente una descrizione dei seguenti elementi: le categorie di dati che sono elaborati da *Facebook*, i dati personali che *Facebook* riceve dai suoi utenti, lo scopo o gli scopi dell'elaborazione di questi dati, la fonte o le fonti dei dati se sono note, i destinatari o le categorie di destinatari a cui sono o possono essere rivela-

Abstract

Tra tutela dell'identità personale e tutela dell'account nella decisione n. 56 dell'11 febbraio 2016 del Garante per la protezione dei dati personali

La decisione in commento dell'Autorità Garante per la protezione dei dati personali sancisce la supremazia del diritto al nome rispetto al “diritto all'account”. La *policy* del *social network Facebook* non offre tutela al dato personale, lo depersonalizza attraendolo nella proprietà dell'*account* creato attraverso lo strumento identificativo dell'*e-mail*. La minaccia del “diritto all'account” incombe dunque sui diritti fondamentali sanciti a livello nazionale, comunitario ed internazionale quali il diritto alla protezione dei dati personali, il diritto al nome e il diritto all'identità personale.

The right to personal identity vs the “right to account” in the Italian Data Protection Authority Decision No 56 of 11 February 2016

This article analyses the decision in which the Italian Data Protection Authority ratifies the supremacy of the right to one's own name over “the right to account”. In fact, the social network Facebook does not offer protection to personal data; it depersonalizes the data and attracts them into the account property by using the e-mail identifier. “The right to account” poses a threat to fundamental rights protected by the national, European and international legal systems such as the right to protection of personal data, right to one's own name and the right to personal identity.

Costanza Martani

“Internet of Things” e l’importanza del diritto alla privacy tra opportunità e rischi

ERIKA CATERINA PALLONE¹

SOMMARIO: 1. Introduzione – 2. Smart things – 3. Wearable Computing – 4. Quantified Self – 5. Domotica – 6. Radio Frequency Identification – 7. Privacy e rischi – 8. Profilazione – 9. Normativa applicabile – 10. Conclusioni

1. Introduzione

L’Internet delle Cose (*Internet of Things*) è la nuova rivoluzione di Internet, in cui il mondo fisico e il mondo virtuale convergono nella creazione di piattaforme, oggetti, case, macchine e perfino città cosiddetti “intelligenti”.

L’inarrestabile evoluzione delle nuove tecnologie e di Internet ha determinato la nascita e proliferazione di una società elettronica “innerata di sensori pronti a raccogliere ogni informazione”².

In linea generale con l’espressione “*Internet of Things*” ci si riferisce a una infrastruttura costituita da innumerevoli sensori direttamente collegati o incorporati nei dispositivi e negli strumenti utilizzati nella vita quotidiana, progettati per rilevare, immagazzinare e processare dati in loco o attraverso il collegamento ad altri dispositivi, strumenti e oggetti³.

¹ Dottoressa in Giurisprudenza. Perfezionata in “Informatica Giuridica” presso l’Università degli Studi di Milano. Cultrice della materia “Informatica Giuridica”.

² Cfr. G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell’era tecnologica*, Milano, Raffaello Cortina 2015, pp. 134-138.

³ Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI PERSONALI, *Parere 8/2014 sui recenti sviluppi nel campo dell’Internet degli oggetti*, 16/09/2014, p. 4, in Internet all’indirizzo http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_it.pdf (sito web visitato il 21 dicembre 2015), nel quale l’Internet degli oggetti viene definito come: “un’infrastruttura nella quale miliardi di sensori incorporati in dispositivi comuni di uso quotidiano

Lo IERC⁴ (*Iot European Research Cluster*) definisce l'*Internet of Things*, come “Una dinamica infrastruttura di rete globale con funzionalità di autoconfigurazione basate su protocolli di comunicazione standard e interoperabili dove gli oggetti fisici e virtuali hanno un’identità, caratteristiche fisiche e personalità virtuali, che utilizzano interfacce intelligenti e che sono perfettamente integrati nella rete dell’informazione”⁵.

Il motivo per cui, ad oggi, trattare un tema come quello dell'*Internet of Things* diviene di fondamentale importanza, è basato sull’enorme portata di tale fenomeno a livello di diffusione globale e potenzialità insite nello sviluppo di piattaforme di tal genere.

In poche parole, si va delineando una società caratterizzata da oggetti di uso quotidiano dotati di sensori in grado di rilevare, raccogliere e trasmettere dati relativamente all’utilizzo che viene fatto di quell’oggetto intelligente (*smart thing*), anche e soprattutto in correlazione con altri oggetti con le medesime capacità.

Sul punto, in termini non molto diversi, si era già soffermato in una relazione del 2004 redatta dall’allora Presidente del Garante per la protezione dei dati personali, Stefano Rodotà, il quale aveva già individuato i rischi e i pericoli per la *privacy* dei soggetti coinvolti, insiti in quelle “etichette intelligenti” di cui alcuni dispositivi erano dotati per la localizzazione o per l’identificazione di soggetti affetti da particolari patologie⁶.

(“oggetti” a sé stanti oppure oggetti connessi ad altri oggetti o persone) sono progettati per registrare, trattare, conservare e trasferire dati e, essendo associati a identificativi univoci, interagiscono con altri dispositivi o sistemi che sfruttano le capacità di collegamento in rete”.

⁴ Lo IERC, quale gruppo di ricerca europeo sull’Internet delle Cose, ha l’obiettivo di giungere ad una visione comunemente condivisa dell’Internet delle Cose, attraverso linee di ricerca a livello europeo e globale, in modo da far emergere le grandi potenzialità e funzionalità derivanti dall’Internet delle Cose, e in modo da coordinare, a livello europeo, il suo sviluppo e il suo funzionamento. In Internet all’indirizzo web <http://www.internet-of-things-research.eu/index.html> (sito web visitato il 27 gennaio 2016).

⁵ In Internet all’indirizzo http://www.internet-of-things-research.eu/about_iot.htm (sito web visitato il 27 gennaio 2016), la definizione in lingua originale «A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual “things” have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network».

⁶ Cfr. G. ZICCARDI, op. cit., pp. 85-88 e la Relazione 2004 del Garante per la protezione dei dati personali, Discorso del Presidente Stefano Rodotà, all’indirizzo

Abstract

“Internet of Things” e l’importanza del diritto alla privacy tra opportunità e rischi

L’articolo ha scopo di fornire un panorama di carattere generale sulla nascita e lo sviluppo dell’*Internet of Things*, partendo da una sua definizione per poi trattare quelle che sono le sue caratteristiche principali.

È evidente che ad oggi l’*Internet of Things* rappresenti la nuova rivoluzione di Internet, in cui mondo fisico e mondo virtuale convergono in piattaforme, oggetti, case e città “intelligenti”.

I soggetti coinvolti in questo settori sono diversi, ognuno portatore di interessi in conflitto l’uno con l’altro.

Da una parte vi sono gli interessi economici dei produttori e distributori degli oggetti intelligenti, nonché degli autori di software e piattaforme per il funzionamento dell’Internet delle Cose, dall’altra vi è la necessità che sia sempre garantita la privacy e la protezione dei dati personali dei soggetti coinvolti.

Internet of Things and the importance of the right to privacy between opportunities and risks

The article aims to provide an overview of a general nature about the birth and development of the Internet of Things, starting with a definition and then treat those who are its main features.

It is obvious that today the Internet of Things represents the new Internet revolution, in which the physical world and the virtual world converge in “smart” platforms, objects, houses and cities.

The subjects involved in this sector are different, each bearer of interests in conflict with one another.

On the one hand there are the economic interests of manufacturers and distributors of intelligent objects and the software authors and platforms for the operation of the Internet of Things, on the other hand there is the need to safeguard the privacy and personal data protection of people involved.

Erika Caterina Pallone

Stati Uniti d'America, Federazione Russa e Italia: consenso e informativa nella disciplina del trattamento dei dati personali (e confronto tra i diversi approcci normativi)

EKATERINA VOLKOVA¹

SOMMARIO: 1. La protezione dei dati personali nell'epoca della globalizzazione: una breve premessa – 2. La privacy nell'ordinamento statunitense – 3. Consenso e informativa nella disciplina degli Stati Uniti d'America – 4. I dati personali nel contesto normativo della Federazione Russa – 5. In particolare: la rilevanza del consenso e dell'informativa – 6. I principi del trattamento dei dati personali nel modello europeo – 7. Conclusioni

1. La protezione dei dati personali nell'epoca della globalizzazione: una breve premessa

Nell'era della globalizzazione, diventa sempre più difficile mantenere riservate le informazioni riferite alla propria persona; il processo di globalizzazione nel trasferimento di dati, l'evoluzione tecnologica (ad esempio: il cloud computing), l'utilizzo di tecniche di *behavioural advertising* e gli attuali problemi di sicurezza nazionale e di ordine pubblico sono soltanto alcuni tra i tanti fattori che hanno portato la questione *privacy* al centro della discussione degli ultimi anni, e che impongono di cercare di definire un quadro normativo coerente e comune per il trattamento di dati personali nell'Unione Europea.

La portata della condivisione e della raccolta di dati è aumentata in modo vertiginoso: la tecnologia attuale consente, sia alle imprese private sia alle autorità pubbliche, di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività e, sempre più spesso, gli stessi

¹ Dottoressa in Giurisprudenza e in Economia, Master in diritto delle nuove tecnologie e informatica giuridica dell'Università degli Studi di Bologna.

privati rendono pubbliche sulla rete informazioni personali che li riguardano. Le nuove tecnologie non hanno infatti trasformato solamente l'economia, ma anche le relazioni sociali.

In un simile contesto, la Commissione Europea ha ufficialmente presentato, nel gennaio 2012, il cosiddetto «pacchetto protezione dati»², con lo scopo di garantire un quadro coerente e un sistema armonizzato su questa materia nell'Unione Europea. L'attenzione merita di essere indirizzata soprattutto sul Regolamento Europeo di recente approvato ed entrato in vigore³, avente come finalità l'aggiornamento della normativa concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati nonché l'estensione della normativa europea a tutte le società extra-Unione Europea che trattano dati personali di cittadini o istituzioni comunitarie.

Il nuovo Regolamento Europeo sulla privacy si profila come una riforma che andrà innanzitutto a beneficio delle persone fisiche, rafforzando i loro diritti alla protezione dei dati e la loro fiducia nell'ambiente digitale; semplificherà notevolmente, poi, il quadro giuridico per le imprese e il settore pubblico.

Ciò dovrebbe stimolare lo sviluppo dell'economia digitale in tutto il mercato interno dell'Unione Europea ed oltre, in linea con gli obiettivi della strategia dell'Europa 2020 e dell'Agenda digitale europea.

La riforma incrementerà la fiducia nelle autorità di tutela e faciliterà gli scambi di informazioni e la cooperazione tra le autorità stesse nella lotta contro le forme gravi di criminalità, garantendo nel contempo alle persone fisiche un livello elevato di protezione.⁴

Nell'ottica di agevolare l'adozione di una ormai indifferibile cornice normativa sovranazionale in materia di protezione dei dati personali, il

² Il pacchetto *de quo* si compone altresì di una proposta di Direttiva indirizzata alla regolamentazione dei settori di prevenzione, contrasto e repressione dei crimini nonché all'esecuzione delle sanzioni penali che sostituirà e integrerà la decisione quadro 977/2008/CE sulla protezione dei dati personali scambiati dalle autorità di polizia e giustizia.

³ Il riferimento è al Regolamento del Parlamento Europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione dei dati COM (2012) 9 final, approvato e in vigore dal 24 maggio 2016.

⁴ Sul punto cfr. ancora la Comunicazione della Commissione UE: "*Salvaguardare la privacy in un mondo interconnesso Un quadro europeo della protezione dei dati per il XXI secolo*" (Bruxelles, 25.1.2012; COM(2012) 9 final.

Abstract

Stati Uniti d'America, Federazione Russa e Italia: consenso e informativa nella disciplina del trattamento dei dati personali (e confronto tra i diversi approcci normativi)

Lo scopo del medesimo articolo è confrontare tre approcci normativi (quello degli Stati Uniti di America, della Federazione Russa e dell'Italia) relativi al trattamento dei dati personali, concentrandoci sulla tematica della necessita di ottenere il consenso e di fornire un'informativa e sull'armonizzazione internazionale dei flussi di dati transfrontalieri.

Nell'epoca della globalizzazione e della tecnologia il trattamento dei dati personali diventa più sensibile e richiede una protezione avanzata. Percio è necessario acquisire una buona padronanza della normativa dei diversi Paesi in ambito di trattamento dei dati personali. L'articolo mira a scoprire il livello di protezione dei dati personali nei Paesi sopramenzionati e ad analizzare il ruolo della privacy nei sistemi legislativi interni.

L'articolo descrive il sistema normativo statunitense: il modello di privacy, gli atti principali, l'autorità competente, la nozione del consenso e i suoi limiti, la necessita di dotarsi di un'informativa.

Per quanto riguarda i dati personali nel contesto normativo della Federazione Russa, l'articolo ha affrontato la problematica di individualizzare il dato personale e la necessita di effettuare il primo trattamento dei dati dei cittadini russi nella Federazione Russa, sono stati descritti i requisiti principali del consenso per il trattamento dei dati personali e l'informativa.

Alla fine è stata predisposta una descrizione generale del modello Europeo relativo al trattamento dei dati principali, basandosi sul contesto giuridico italiano. Gli esempi sopramenzionati fanno vedere come cambia la configurazione della privacy da un paese all'altro: dal diritto fondamentale dell'individuo al diritto del consumatore”.

United states of America, Russian Federation and Italian Republic: notice and consent - the conditions for processing personal data (comparison with the different legal systems).

The purpose of the present article is to compare three legal systems (american, russian and italian) relating to the processing personal data, focusing on the ne-

cessity to obtain the consent and to provide the notice and of the international harmonization of cross-border data flows.

In the age of globalization and technology the processing personal data becomes more sensitive and requires a strong security. So it is important to acquire a high knowledge of the legislation of the various countries in the field of personal data processing.

The article aims to find out the level of protection personal data in the above-mentioned countries and to analyze the role of privacy in domestic legal systems. The article describes the US regulatory system: the privacy model, the regulatory enactments, the competent authorities, the notion of consent and its limitations, the necessity to submit the notice.

With regard to the personal data within the legal framework of the Russian Federation, the article is addressed to the problem of definition of the personal data and the necessity to carry out the first Russian citizens data processing in the Russian Federation, to the description of the essential elements of the notice and the consent for the processing personal data.

Furthermore there was outlined the overview of the European model for the processing personal data, based on the Italian legal framework.

The aforementioned examples show how the configuration of privacy changes from one country to another: from the fundamental right of the individual to the consumer's right.

Ekaterina Volkova