A12

Giorgia Manzini

La *cybersecurity* ai tempi del *Coronavirus*

Prefazioni di
Gabriele Faggioli
Antonia Manzini

Aracne editrice

www.aracneeditrice.it
info@aracneeditrice.it

www.gioacchinoonoratieditore.it
info@gioacchinoonoratieditore.it

via Vittorio Veneto, 20
00020 Canterano (RM)
(06) 45551463

ISBN 978-88-255-3601-0

I edizione: luglio 2020

Ai miei figli
e a tutti i piccoli eroi del lockdown,
che hanno vissuto con serenità e ottimismo
una situazione impossibile.

Indice

Prefazione

di GABRIELE FAGGIOLI
Presidente CLUSIT (Associazione Italiana
per la sicurezza informatica)

È accettabile comprimere i diritti fondamentali dei cittadini nei momenti di emergenza?

Una domanda di questo tipo fino a pochi mesi fa sarebbe stata interpretata come mero esercizio teorico e invece questo è l'interrogativo che in molti si fanno in questi incredibili mesi.

Sono mesi caratterizzati dalla accettazione di limitazioni importantissime sia nella vita privata delle persone che nella vita lavorativa. Miliardi di cittadini al mondo chiusi in casa. Attività economiche paralizzate.

Interi grandissimi paesi sono ancora nel pieno dell'esplosione del virus e nessuno può dire con certezza cosa accadrà nei prossimi mesi anche in Europa, e in Italia.

Ma questi mesi passati, e quelli che ci aspettano, ci stanno accompagnando in un nuovo futuro, un futuro che forse sarebbe comunque arrivato seppur con tempi molto più dilatati.

Centinaia di milioni di persone al mondo, o forse miliardi, hanno imparato a restare collegati con i propri parenti e amici grazie alle tecnologie digitali.

Moltissime imprese riescono a produrre e a generare ricavi grazie al digitale ed anzi talune hanno colto nella pandemia una grandissima occasione di modernizzazione, trasformazione dei servizi, mutamento del modello di organizzazione.

La pubblica amministrazione è riuscita in larghissima parte a erogare i servizi essenziali.

Certo, tutto è migliorabile. Tutto è criticabile.

Ma intanto molto, moltissimo è stato fatto.

Sicuramente sono stati raggiunti obiettivi che fino a pochissimi mesi fa sarebbero stati inimmaginabili se non a seguito di lente trasformazioni negli anni.

Nella tragedia di chi ha perso la vita e di chi ancora soffre e purtroppo di chi subirà il contagio nei prossimi giorni e mesi, è però eccezionale che sia stato possibile tutto questo.

L'importanza del digitale e il ruolo fondamentale delle tecnologie appare oggi evidente a tutti.

Ma l'evoluzione digitale dei cittadini, delle imprese, della pubblica amministrazione deve essere una "sicura". Non ci può essere digitalizzazione senza sicurezza e senza il rispetto dei diritti essenziali delle persone.

I mesi che sono appena trascorsi hanno insegnato alcune cose.

Innanzitutto i criminali (informatici) non si arrestano neanche davanti alla pandemia. Anzi. Azioni importantissime sono state compiute proprio sfruttando la pandemia. La paura del contagio, la ricerca spasmodica in internet di mascherine, guanti, disinfettanti, la ricerca di informazioni, il lavoro remoto hanno permesso di porre in essere attacchi di *phishing* estremamente efficaci per non parlare delle truffe *online* legate a finti siti che proponevano finte vendite di prodotti che per settimane sono stati introvabili.

Ma non solo i cittadini sono stati oggetto di attacco. Strutture ospedaliere in Italia e nel mondo hanno subito attacchi *ransomware* estremamente efficaci a dimostrazione che i criminali (informatici) non arretrano neanche davanti allo sforzo estremo di salvare vite umane (ma qualcuno di loro si sarà ammalato?).

Il lavoro remoto di massa (e l'utilizzo massivo di tecnologie per restare in contatto salvaguardando la socialità) ha ovviamente allargato in modo esponenziale la superficie di attacco con quindi maggiore facilità nel trovare "polli" da spennare.

Ma non sono solo i criminali (informatici) ad aver creato problemi.

La pressione della opinione pubblica, la necessità di fare tutto in fretta spesso con organizzazioni "esplose" ha determinato anche errori importanti (talvolta giustificati con scuse forse vere forse puerili) che hanno avuto risultato sui media e che rischiano di far perdere fiducia nella pubblica amministrazione.

Insomma, sono stati mesi convulsi dove nessuno era preparato ad affrontare un'emergenza di questo impatto.

Eppure, seppur in un contesto così delicato, i temi della sicurezza informatica e dei diritti delle persone sono rimasti al centro del dibattito e della attenzione.

Da una parte non c'è dubbio che l'importanza di una digitalizzazione sicura è nell'agenda di moltissime aziende e pubbliche amministrazioni come dimostrano gli studi del CLUSIT e dell'Osservatorio *Cybersecurity & Data Protection* del Politecnico di Milano. Gli investimenti sono in aumento così come le azioni di *awareness* e di formazione spinte anche dalle migliaia di DPO e di figure specialistiche che il mercato continua a assorbire senza tregua.

Dall'altro il tema della protezione dei dati e dei diritti inviolabili delle persone è oggetto di continue conferme.

L'Autorità Garante italiana ha comminato sanzioni multimilionarie, il *privacy shield* è stato dichiarato invalido dalla Corte di Giustizia Europea per assenza di garanzie sufficienti, le polemiche sulle APP di *tracing* non accennano a placarsi e sono positive nel loro intento di fare emergere gli spunti di miglioramento possibile ma soprattutto i Garanti europei hanno fatto sentire il loro peso nel dare indicazioni in merito alle azioni possibili da parte delle aziende e delle pubbliche amministrazioni per supportare il controllo del contagio e le azioni di contenimento.

E qui torno alla domanda iniziale: è accettabile comprimere i diritti fondamentali dei cittadini nei momenti di emergenza?

La risposta per quanto mi riguarda è no. Ma forse è la prospettiva da cui spesso si parte formulando questa domanda che non è a mio avviso corretta.

Come ha detto l'Autorità Garante italiana in più occasioni, e anche in taluni provvedimenti, non possono e non devono esistere iniziative "fai da te".

Le normative esistono, e sono normative spesso sufficientemente elastiche per permettere in taluni casi l'utilizzo di tecnologie a vantaggio della salute dei cittadini. Soprattutto nei momenti emergenziali come quello che stiamo vivendo le normative danno la possibilità di porre in essere azioni a vantaggio della

collettività. Azioni temporanee, che devono essere interrotte non appena possibile.

Azioni che se poste in essere in modo sicuro e rispettoso dei principi normativi esistenti sono non solo legittime, ma doverose.

Il libro che Vi accingete a leggere contiene moltissimi approfondimenti e Vi darà spunti di riflessione di grande rilevanza e rappresenta l'ulteriore evidenza dell'interesse che ruota intorno ai temi della sicurezza informatica. Buona lettura!

Prefazione

di ANTONIA MANZINI
Divisione Risparmio Gestito e Servizi
di Investimento BANCA D'ITALIA[1]

Questo testo si occupa di temi molto importanti nella fase attuale di graduale uscita dal *lockdown* in Italia e altrove. Il necessario maggior ricorso alle tecnologie digitali per il lavoro, per la didattica, per la vita quotidiana ha reso ancor più di attualità il tema della circolazione dei dati. La produzione di dati al giorno d'oggi è immensa e la loro sicurezza è decisiva per la vita di aziende e famiglie.

Lo sviluppo tecnologico è un aiuto ma, ricorda l'autrice, è sempre un'arma a doppio taglio. Algoritmi di intelligenza artificiale possono individuare *fake news* ma anche crearle, difendere servizi vitali dagli attacchi informatici ma anche aiutare gli hacker a penetrare *computer* e sistemi informativi.

In un momento in cui una parte molto maggiore della vita di tutti si svolge attraverso canali digitali, il *cybercrime* avrebbe potuto comportare danni devastanti, si pensi al blocco dei sistemi dell'INPS o a quelli di un importante operatore bancario. L'autrice opportunamente ricorda, a tal proposito, che l'Italia è il primo paese europeo e il decimo al mondo nella classifica dei paesi più colpiti da *cyber* attacchi e il tema è dunque di grande importanza.

Il testo passa quindi a un inquadramento delle varie fattispecie di attacchi informatici, ben descritti, nell'ambito del diritto penale italiano, tema su cui c'è ormai una ampia giurisprudenza pure richiamata.

[1] Le opinioni sono espresse a titolo personale e non impegnano la responsabilità dell'Istituto.

Un altro argomento trattato è quello delle *fake news*, altro tema caldo per l'emergenza sanitaria. Si scontrano qui esigenze basilari contrapposte, la libertà di informare da una parte, il diritto a non essere disinformati dall'altra. Non si parla qui ovviamente di differenti opinioni e valutazioni sui diversi argomenti della vita pubblica ma di notizie apertamente false create ad arte per finalità di destabilizzazione politica. I *social network* sono il veicolo perfetto per la diffusione di questa disinformazione e nonostante gli sforzi delle aziende che gestiscono i *social*, il flusso di *fake news* rimane cospicuo. La pandemia ha, ancora una volta, esacerbato il tema. Nuovamente ci viene in soccorso la tecnologia; algoritmi di *machine learning* possono essere impiegati per scovare *fake news*, tracciarle alla fonte e tappare la falla, per così dire. Ma, come sempre, tecniche simili possono contribuire anche a diffonderle.

In tutto questo, il tema della sicurezza dei dati personali diviene un aspetto decisivo dei diritti della persona nell'epoca digitale. L'argomento è complesso perché al di là del furto di dati, è spesso l'utente di *social* a fornire spontaneamente informazioni. Questo rende anche le polemiche sulle app di tracciamento piuttosto sterili. L'autrice ricorda come l'Unione Europea abbia promulgato, in materia, la legge più avanzata al mondo (il regolamento GDPR) che però non può difendere appunto l'utente da se stesso, per così dire, di fronte all'istantaneo fluire dell'interazione degli utenti sui *social*. L'invasività delle "*big tech*" nella vita sociale e personale è uno dei temi centrali della nostra epoca e non solo per la professione giuridica.

Capitolo I

L'infosfera espansa dal *lockdown* come teatro sociale di *cybercrimes*

Il confinamento prolungato della popolazione per contenere il contagio da *Covid–19* ed affrontare l'emergenza dell'intasamento delle terapie intensive ha dirottato la vita di un paese intero *online*. La fase mai sperimentata prima del *lockdown* ha reso evidente la necessità di interventi di potenziamento delle infrastrutture e di sostegno delle imprese fornitrici di servizi di comunicazioni elettroniche. Siamo stati tutti perennemente e contemporaneamente collegati a distanza, per lavorare, per studiare, per acquistare, per informarci e per intrattenerci nelle lunghe giornate a casa. Finalmente, le iniziative di digitalizzazione e innovazione tecnologica del paese si sono imposte quali misure urgenti e necessarie. Si è ammesso lo svolgimento in videoconferenza delle sedute degli organi di governo comunali, provinciali e regionali, ma una più accesa discussione ha suscitato il voto *online* in Parlamento. Non si è trovato il coraggio di innovare le modalità di espressione del consenso, poiché ogni scelta urtava contro la normalità che conoscevamo.

Nell'emergenza sanitaria, anche il Notariato si è interrogato sull'opportunità dell'atto pubblico a distanza, dato che gli studi notarili sono rimasti sempre aperti, in quanto attività essenziale al servizio della popolazione. Ci si è chiesti allora come soddisfare le esigenze giuridiche della collettività e garantire nel contempo il distanziamento sociale. *De iure condito* gli atti pubblici che i notai ricevono sono cartacei, ovvero informatici sottoscritti con firma digitale o con firma elettronica, ma pur sempre in presenza del notaio: la presenza fisica del notaio è una garanzia e un imperativo categorico, come lo era *#stateacasa* durante le settimane di emergenza. È intuibile quanto il rogito sia per natura un assembramento di persone, che configgeva contro i divieti del

Governo. Come si è superato l'*empasse* notarile ai tempi del *coronavirus*? Si poteva percorrere la strada dell'atto pubblico a distanza, che avrebbe consentito di realizzare appieno il distanziamento sociale con l'ausilio della tecnologia e di fornire un servizio continuo alla collettività, oppure scegliere la via di applicare rigorosamente i protocolli di sicurezza sanitaria e di ridurre al minimo l'attività notarile, circoscrivendola agli atti indifferibili e urgenti, dichiarati tali dalle parti con un'ennesima autocertificazione. Ha prevalso quest'ultima soluzione per il giustificato timore di modificare, con la fretta dell'emergenza, regole secolari legate alla territorialità della competenza notarile e alla compresenza fisica dei contraenti. A ciò si aggiunga che, anche nel settore notarile, l'Italia presentava situazioni estremamente eterogenee, con esigenze diversissime: si pensi alle città metropolitane della Lombardia flagellate dal contagio, ove gli spostamenti risultavano più lunghi e gli assembramenti più pericolosi, rispetto ai piccoli centri di provincia in altre regioni meno colpite dal *virus*, ove spostarsi per un rogito era più facile e meno rischioso. In quella contingenza, la cui durata era incerta, l'unica apertura verso il *Cyber Space* (*cyber* spazio) di "gisponiana" memoria, che ha consentito anche ai notai di operare oltre il *Meat Space* (mondo reale) ai fini del contenimento del contagio e della limitazione alla mobilità è stata quella accolta dall'art. 106 del d.l. "Cura Italia" n. 18 del 17 marzo 2020[1] relativo alle norme in materia di svolgimento delle assemblee di società ed enti. È consentito, cioè, che le assemblee ordinarie o straordinarie di società di capitali, cooperative e mutue assicuratrici possano prevedere, anche in deroga alle diverse disposizioni statutarie, l'espressione del voto in via elettronica o per corrispondenza e l'intervento all'assemblea mediante mezzi di telecomunicazione, potendosi altresì svolgere l'assemblea anche esclusivamente mediante mezzi di telecomunicazione che garantiscano l'identificazione dei partecipanti, la loro partecipazione e l'esercizio del diritto di voto, senza in ogni caso la necessità che si trovino nel medesimo

[1] Convertito con modifiche nella legge 24 aprile 2020 n. 27, in vigore dal 30 aprile 2020.

luogo, ove previsti, il presidente, il segretario o il notaio. Previsione dirompente con applicabilità limitata alle assemblee convocate entro il 31 luglio 2020 ovvero entro la data successiva fino alla quale sarà in vigore lo stato di emergenza sul territorio nazionale relativo al rischio sanitario connesso all'insorgenza della epidemia da *Covid–19*.

Meno complesso, dal punto di vista pratico, almeno per i notai da tempo in avanzato stato di digitalizzazione, è stato il tema del telelavoro e dello *smart working* per i dipendenti. Dal punto di vista giuridico, invece, ciò ha aperto in generale questioni delicatissime in materia di responsabilità del datore di lavoro per contagio da *Covid–19* del dipendente a casa: malattia o infortunio sul lavoro? Inps o Inail? Le conseguenze di una impostazione certa di questo tema saranno essenziali per una vitale ripresa delle attività economiche, che inevitabilmente conserveranno quanto di innovativo ha funzionato durante il *lockdown*.

È innegabile che le ICT digitali (le tecnologie dell'informazione e della comunicazione) siano state le protagoniste assolute di questi tempi: hanno dato sollievo a tutti noi nelle settimane di quarantena nazionale, producendo tangibili modificazioni delle nostre relazioni umane e assumendo una più accentuata funzione ambientale, antropologica, sociale e interpretativa della realtà[2]. Si è concretizzato, cioè, quel luogo immaginario di fantasticherie e allucinazione tecnologiche definito *Cyber–Space* (*cyber* spazio) dallo scrittore canadese William Ford Gibson nel racconto di fantascienza "*Burning Chrome"*, contrapposto al *Meat Space* (mondo reale).

Fino a pochi mesi fa sembrava esorbitante ripartire le epoche dell'umanità, o i modi di vivere dei popoli, nella "preistoria", in cui vigeva l'assenza di registrazione di informazioni, nella "storia", in cui le informazioni vengono registrate e trasmesse con ICT, ma non prevalgono su altre tecnologie che riguardano risorse primarie ed energia, e nella "iperstoria", in cui il benessere individuale e sociale dipendono strettamente dalle ICT. In questi

[2] L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, 2017.

tempi di pandemia e ripresa di una nuova normalità, è emerso con evidenza quanto il progresso e la nostra stessa sopravvivenza siano risultati non solo strettamente collegati, ma soprattutto dipendenti dall'efficiente gestione del ciclo di vita dell'informazione.

L'età della "storia" nel senso anzidetto coinvolge ancora molte popolazioni, che fanno affidamento sulle ICT per registrare, trasmettere e utilizzare dati: in queste società storiche, le ICT non risultano dominanti sulle altre tecnologie fondate sull'uso di energia. Diversamente, l'età dell'"iperstoria" riguarda già quelle società come la nostra, in cui le ICT e le loro capacità di processare dati sono condizioni essenziali per assicurare e promuovere il benessere sociale, la crescita individuale e lo sviluppo in generale. Si classificano, in tal senso, come società iperstoriche, quelle dei paesi membri del G7 (Stati Uniti, Francia, Canada, Germania, Giappone, Italia e Regno Unito) che nel 2020 si è svolto per la prima volta a distanza con il supporto della tecnologia, in conseguenza della pandemia da *Covid–19*: in questi paesi una grande percentuale del prodotto interno lordo dipende da beni intangibili, fondati sull'uso d'informazione, piuttosto che da beni materiali, prodotti dai processi agricoli o manifatturieri.

Ma cosa rappresentano giuridicamente questi beni intangibili definiti "dati informatici", che abbiamo moltiplicato enormemente durante il *lockdown*? La risposta a tale quesito è carica di conseguenze rilevanti ai fini della tutela dei dati dai *cybercrimes*. Sul punto, ha sovvertito il precedente orientamento la Cassazione penale, sezione II, in data7 novembre 2019, con sentenza n. 11959 depositata il 10 aprile 2020, qualificando i *file* come "cose mobili" ai sensi della legge penale per fisicità strutturale, possibilità di misurarne le dimensioni e trasferibilità da un luogo all'altro. Ne è conseguito, nel caso di specie, l'inquadramento della sottrazione definitiva di dati informatici mediante copiatura da un personal *computer* aziendale, affidato all'agente per motivi di lavoro e restituito con *hard disk* formattato nell'ambito del delitto di appropriazione indebita, a tutti gli effetti di legge.

È evidente che l'equiparazione giurisprudenziale dei *files* a cosa mobile consente di attribuire una maggior tutela ai dati informatici in un quadro del sistema penale italiano, in cui la nozione di cosa mobile non risulta positivamente definita dalla legge, ma presupposta nella fattispecie del furto, con la disposizione che assimila a cosa mobile l'energia elettrica e ogni altra energia economicamente valutabile (art. 624, 2° comma c.p.).

La Cassazione, quindi, ha enucleato in via interpretativa i requisiti della nozione penalistica di cosa mobile, nonché le caratteristiche descrittive dei dati informatici, per giungere a un punto di sovrapposizione ed applicare ai *files* la tutela giuridica prevista per l'appropriazione indebita *ex* art. 646 c.p.

Orbene da un lato, il ragionamento è partito dall'individuazione di alcuni caratteri minimi della cosa mobile agli effetti della legge penale, rappresentati dalla materialità e fisicità dell'oggetto, che deve risultare definibile nello spazio e suscettibile di essere spostato da un luogo ad un altro, rendendo possibile la sottrazione della cosa al controllo del proprietario.

Dall'altro lato, è stata assunta la definizione di *file* secondo le nozioni informatiche comunemente accolte dalle specifiche ISO, ossia come l'insieme di dati, archiviati o elaborati, cui sia stata attribuita una denominazione secondo le regole tecniche uniformi. Si tratta della struttura principale con cui si archiviano i dati su un determinato supporto di memorizzazione digitale, struttura che possiede una dimensione fisica determinata dal numero delle componenti necessarie per l'archiviazione e la lettura dei dati inseriti nel *file*. Tali componenti, basate sulle cifre binarie cosiddette "bit", dalla crasi delle parole inglesi *binary digit*, unità di misura all'interno di ogni dispositivo in grado di elaborare o conservare dati informatici, che vengono raggruppate in celle da 8 "bit" denominate *byte* (ISO/IEC 2382:2015 – 2121333), sono dotate di una propria fisicità e occupano uno spazio preciso e quantificabile corrispondente alla memoria che occupano.

Da questi elementi descrittivi la Cassazione ha desunto che il *file*, pur non potendo essere materialmente percepito dal punto di vista sensoriale, possiede una dimensione fisica costituita dalla

grandezza dei dati che lo compongono, come dimostrato dall'esistenza di unità di misura della capacità di un *file* di contenere dati e dalla differente capienza dei supporti fisici in cui i *files* possono essere conservati e elaborati, nonché è suscettibile di essere spostato e sottratto con operazioni tracciabili.

Seppur in chiave repressiva, tale orientamento della Suprema Corte costituisce una svolta per la sicurezza dei dati informatici, a maggior ragione nel *post*–Umanesimo che ci si prospetta dopo la pandemia. L'economia italiana, infatti, dovrà fondarsi su risorse basate sull'informazione, nella cosiddetta economia della conoscenza, con servizi ad alta intensità d'informazione nell'ambito di commercio, proprietà, comunicazione, finanza, assicurazione e intrattenimento e dovrà orientare più profondamente all'informazione interi settori pubblici, quali l'educazione, la pubblica amministrazione e la sanità.

La natura degli attacchi cibernetici che hanno caratterizzato l'infosfera dell'emergenza *Covid–19*, di cui l'infodemia ha rappresentato solo una delle tante criticità, ci ha confermato di appartenere già a pieno titolo alla fase dell'evoluzione umana dell'"iperstoria", l'unica che può essere minacciata in termini informazionali da un *cyber*–attacco. Se riguardo al fattore "tempo" viviamo quindi nell'iperstoria e riguardo al fattore "spazio" siamo immersi nell'infosfera, riguardo alla nostra identità assistiamo ad una duplicazione di esperienze umane *onlife*, che durante il *lockdown* hanno preso il sopravvento su quelle fisiche, nell'ambito delle interazioni sociali, della salute e dell'istruzione: durante la pandemia, le ICT hanno svelato a tutto campo la loro natura di potenti tecnologie del sé.

Subirà, quindi, un'ennesima variazione anche la prima legge di Gordon Moore, uno dei fondatori di INTEL, di cui è noto il diagramma che descrive empiricamente lo sviluppo della microelettronica, in progressione esponenziale a partire dagli anni '70. La complessità dei microcircuiti, cioè, raddoppierebbe periodicamente, con un periodo originalmente previsto in dodici mesi, allungato a due anni fra gli anni '70 e '80, e un assestamento successivo fissato sui diciotto mesi. La capacità predittiva della

legge di Moore è stata più volte messa in discussione e recentemente affiancata da un piano di sviluppo (ITRS, *International Technology Roadmap for Semiconductors*) che considera le principali caratteristiche dei dispositivi del futuro, con previsioni a medio e lungo termine di otto e quindici anni, aggiornate ogni 2 anni. A livello planetario, cioè, si tende a contenere il costo proibitivo dello sviluppo di nuove tecnologie favorendo la focalizzazione sugli stessi obiettivi degli sforzi di tutti.