Cento e una voce di informatica giuridica

a cura di

Agata C. Amato Mangiameli

Guido Saraceni

Giappichelli

A

[1] Accesso abusivo

G.S.

Ai sensi dell'art. 615-*ter* c.p., "chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione sino a tre anni". La disposizione – posta all'interno del titolo XII del libro II del Codice penale, subito dopo il reato di violazione di domicilio, sanzionato dall'art. 614 c.p. – prende dunque in considerazione due condotte: la prima è rappresentata dal vero e proprio accesso non autorizzato ('abusivo') ad un sistema informatico o telematico, mentre la seconda consiste nell'illecito 'mantenimento'. Quest'ultima ipotesi si configura tutte le volte in cui un soggetto si trattiene all'interno di un sistema informatico o telematico, superando il limite temporale stabilito dal titolare. Oppure, nel caso in cui, pur rispettando suddetto limite, violi un limite teleologico, utilizzando il sistema per finalità diverse ed ulteriori rispetto a quelle per cui ne era stato inizialmente autorizzato l'accesso.

Parte della dottrina ritiene che il reato in questione debba essere considerato plurioffensivo, ovvero, che la condotta prevista dall'articolo 615-*ter* c.p. aggredisca, contemporaneamente, molti ed eterogenei beni giuridici. Indubbiamente, l'accesso abusivo espone il titolare del sistema informatico, o dei dati in esso contenuti, ad una molteplicità di pericoli, poiché, una volta entrato all'interno del sistema, il reo potrebbe carpire informazioni riservate; impedirne il corretto funzionamento, danneggiando gravemente i file o i programmi, oppure, potrebbe appropriarsi di codici di accesso riservati ed utilizzare queste informazioni per ottenere un vantaggio patrimoniale.

Eppure, la tesi per la quale si tratterebbe di un reato in sé plurioffensivo incontra molte ed a mio avviso non superabili obiezioni. Dobbiamo infatti ritenere che il bene giuridico tutelato dalla norma sia esclusivamente uno: l'inviolabilità del domicilio informatico – inteso come 'spazio

ideale' di esclusiva pertinenza di una persona fisica o giuridica. Questa interpretazione trova conforto nella collocazione sistemica della disposizione; nella giurisprudenza che, unanime, sottolinea come per la configurabilità del reato non sia necessario che il soggetto agente prenda concretamente visione di dati o di informazioni riservate; nel numero e nel tipo di circostanze aggravanti previste ed infine nel fatto che ulteriori condotte criminose risultano puntualmente sanzionate da altre e più specifiche norme.

Ancor di più, se l'art. 615-*ter* c.p. avesse avuto il fine di tutelare la riservatezza, il soggetto passivo avrebbe dovuto essere esplicitamente identificato con il titolare dei dati contenuti all'interno del sistema. Invece l'articolo *de quo* non opera alcun riferimento al titolare dei dati o financo alle informazioni eventualmente custodite nel computer, rafforzando il convincimento che il legislatore non abbia inteso tutelare la privacy [v. voce], ma, più esattamente, lo *ius excludendi alios*.

Ragionando per iperbole, il reato si verrebbe dunque a configurare anche nel caso in cui il sistema dovesse risultare privo di dati sensibili, oppure, del tutto sprovvisto di dati. Detto in altre parole, l'accesso abusivo ad un sistema informatico o telematico non è stato sanzionato dal legislatore penale perché, attraverso di esso, vengono posti in pericolo molti ed eterogenei beni giuridici, ma perché la condotta descritta nell'art. 615-*ter* c.p. danneggia concretamente l'inviolabilità del domicilio (informatico) – un bene giuridico di primissimo piano che assurge al rango di vero e proprio valore costituzionale.

Tra gli elementi costitutivi del reato, un ruolo di primo piano spetta, indubbiamente, alla nozione di misure di sicurezza, dato che la norma subordina la rilevanza penale della condotta al fatto che sia stato violato un sistema protetto da suddette misure. Per questo motivo, il reato di accesso abusivo a sistema informatico può correttamente essere considerato un reato a forma vincolata. Se il titolare di un sistema informatico o telematico non predispone alcuno strumento a difesa del proprio domicilio informatico, non può richiedere che un intruso venga punito ai sensi dell'art. 615-*ter* c.p. Tutto ciò premesso, è importante sottolineare che la disposizione in esame contiene un'espressione vaga ed in un certo qual modo fuorviante.

Se da un lato il legislatore ha fatto bene a non definire tecnicamente il concetto di misure di sicurezza, lasciando l'utente libero di approntare i mezzi che più ritenga idonei a tutelare il proprio domicilio informatico – e consentendo all'evoluzione tecnologica di fare il suo corso –, dall'altro, la giurisprudenza e la dottrina risultano unanimi nel ritenere che l'utilizzo del plurale – misure di sicurezza – non debba essere preso alla lettera, rappresentando una mera scelta stilistica. Il reato si perfeziona, dunque, anche se viene violata una sola misura di sicurezza, non rilevando né il numero né, tantomeno, la raffinatezza delle difese adottate dal titolare. Ciò che rileva è che la presenza della misura di sicurezza possa essere percepita dall'esterno del sistema. Il valore di una misura di sicurezza risiede quindi nel suo significato simbolico, perché attraverso di essa il titolare manifesta la volontà di proteggere il proprio domicilio, escludendo gli estranei.

Considerando la questione dal punto di vista tecnologico, notiamo come le misure di sicurezza possano essere divise in due grandi categorie: misure di sicurezza digitali e misure di sicurezza non-digitali. Le prime possono a loro volta essere distinte in misure di sicurezza software [v. voce] – come, ad esempio, una password [v. voce] o un firewall – e misure di sicurezza hardware [v. voce] – come, ad esempio, un badge per la firma digitale o un sistema per il riconoscimento biometrico. Le seconde possono invece essere utilizzate per proteggere il sistema informatico o telematico inteso nella sua estrinseca materialità – pensiamo, ad esempio, ad una cassaforte.

A tal riguardo, è bene sottolineare che il tentativo di reato è senza ombra di dubbio ipotizzabile nell'ipotesi in cui il soggetto agente provi a violare una misura di sicurezza informatica, dato che, in tal caso, potrebbero ricorrere i requisiti della idoneità e della non equivocità dell'azione richiesti dal Codice penale *ex* art. 56; al contrario, risulta difficile ipotizzare un tentativo di accesso informatico quando il sistema di sicurezza è protetto da una misura di sicurezza non-digitale, come, ad esempio, una cassaforte o una porta blindata. In questi casi sarebbe particolarmente arduo, se non impossibile, provare la non equivocità degli atti posti in essere dal reo, ovvero, dimostrare che il soggetto abbia forzato la cassaforte o guadagnato l'accesso ai locali in cui era custodito il sistema informatico con il fine certo ed esclusivo

di accedere al sistema e non con la diversa finalità di danneggiare, distruggere o rubare.

La finalità perseguita dal reo non rileva, invece, per il perfezionarsi della fattispecie: l'elemento soggettivo del reato è chiaramente rappresentato dal dolo generico. Ciò che conta è che il soggetto abbia la coscienza e la volontà di accedere ad un sistema informatico o telematico munito di misure di sicurezza.

Per quanto concerne il *tempus commissi delicti*, è opportuno operare una distinzione tra il vero e proprio accesso abusivo – reato a consumazione istantanea – ed il mantenimento. Nel caso in cui il soggetto agente violi un limite teleologico, ci troveremo ancora di fronte ad un reato a consumazione istantanea; mentre, nel caso in cui il reo decida di trattenersi all'interno del sistema superando un limite temporale, il reato sarebbe permanente.

Nella sua forma semplice, l'accesso abusivo è perseguibile a querela di parte, invece, nella forma aggravata è perseguibile anche d'ufficio; inoltre, nel caso in cui si verifichi una circostanza aggravante, la pena massima sale da tre a cinque anni di reclusione.

Le aggravanti previste dal legislatore riguardano le modalità della condotta – il reato è aggravato se il soggetto è palesemente armato, ovvero agisce con violenza su persone o cose –; la natura del sistema informatico o telematico – il reato è aggravato nel caso in cui la condotta riguardi sistemi informatici "di interesse militare, o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico"; le conseguenze della condotta – nel caso in cui dal fatto derivi la distruzione o il danneggiamento del sistema; l'interruzione anche parziale del suo funzionamento ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti – e lo *status* personale del reo – ovvero, nel caso in cui il reato sia stato commesso da pubblico ufficiale o incaricato di pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla propria funzione; da chi esercita, anche abusivamente, la professione di investigatore privato o con abuso della qualità di operatore di sistema.

La *ratio* delle aggravanti appena illustrate è facilmente percepibile. Per

quanto attiene alle modalità della condotta, il legislatore ha preso in considerazione la maggiore pericolosità sociale di un soggetto che usa o minaccia violenza pur di realizzare il proprio disegno criminoso; con riguardo alla natura dei sistemi, è stata ponderata la natura pubblica e collettiva del bene giuridico leso; relativamente alle conseguenze della condotta, è stato valutato il maggior danno arrecato al soggetto passivo; infine, per ciò che concerne lo *status* del soggetto agente: il legislatore ha ritenuto di dover punire con maggiore severità l'investigatore privato, probabilmente in considerazione del fatto che, in questo caso, l'accesso abusivo nasce all'interno di un rapporto di lavoro; il pubblico ufficiale e l'incaricato di pubblico servizio, in ragione del ruolo che questi soggetti svolgono all'interno della società e l'operatore di sistema, perché è legato al soggetto passivo da uno specifico vincolo contrattuale: come una lama a doppio taglio, la condotta criminale di quest'ultimo lede contemporaneamente due beni giuridici di primissimo piano, mortificando l'inviolabilità del domicilio informatico nello stesso momento in cui recide il rapporto fiduciario che si era venuto a creare tra il system operator ed il suo datore di lavoro.

Bibliografia minima essenziale

Amato Mangiameli A.C., Saraceni G., *I reati informatici. Elementi di teoria generale e principali figure criminose*, Giappichelli, Torino, 2019.

Bartoli R., *L'accesso abusivo a sistema informatico (art. 615 ter c.p.) a un bivio ermeneutico teleologicamente orientato*, in *Diritto Penale Contemporaneo*, 1/2012, pp. 123-127.

Bellacosa M., *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle Sezioni Unite*, in *Diritto Penale Contemporaneo*, 2 febbraio 2015 (*https://archiviodpc.dirittopenaleuomo.org/d/3642-il-luogo-di-consumazione-del-delitto-di-accesso-abusivo-a-un-sistema-informatico-o-telematico-in-at*).

Borgobello M., *Il reato di accesso abusivo a sistema informatico di cui all'art. 615 ter c.p. alla luce della giurisprudenza più recente*, in *Giurisprudenza penale web*, 2/2021 (*https://www.giurisprudenzapenale.com/2021/02/21/il-reato-di-accesso-abusivo-a-sistema-informatico-di-cui-allart-615-ter-c-p-alla-luce-della-giurisprudenza-piu-recente/*).

Contrafatto V., *I reati informatici*, Key, Milano, 2017.

Cuomo L., Razzante R., *La nuova disciplina dei reati informatici*, Giappichelli, Torino, 2009.

D'Aiuto G., Levita L., *I reati informatici. Disciplina sostanziale e questioni processuali*, Giuffrè, Milano, 2012.
Foscarini A., *I reati informatici e le digital evidence nel processo penale italiano*, s.l., 2018.
Perri P., *Privacy, diritto e sicurezza informatica*, Giuffrè, Milano, 2007.

[2] Accountability

L.P.

Il principio di accountability (o di responsabilizzazione, come tradotto dal legislatore italiano), di cui all'art. 5, par. 2, del Regolamento (UE) 2016/679 (il *Regolamento Generale sulla Protezione dei Dati* o GDPR) rappresenta un'assoluta novità per l'impianto normativo a salvaguardia dei diritti e delle libertà delle persone fisiche con riguardo al trattamento dei dati personali [v. voce], comportando un rivoluzionario cambio di prospettiva. Con la sua previsione, infatti, mutano radicalmente sia il ruolo che gli obblighi del titolare del trattamento, ossia della "persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali" (art. 4, par. 1, n. 7 del GDPR). Figura, questa, centrale e strategica per garantire la tutela sostanziale del diritto fondamentale alla protezione dei dati personali in qualsiasi realtà imprenditoriale, di piccole o grandi dimensioni, sia essa privata o pubblica.

In virtù di siffatto principio, è richiesto al titolare di assumere – fin dalle primissime fasi di progettazione di prodotti e servizi il cui utilizzo incida sui dati degli utenti e per tutta la filiera del trattamento – un comportamento dinamico e proattivo, che non si limiti a una mera check-list degli adempimenti normativi, ma provveda a valutare attentamente in autonomia – senza chiedere preventivi *placet* alle Autorità di controllo – le misure (tecniche, fisiche, logiche od organizzative) che, a seconda del contesto e delle circostanze, è opportuno adottare per raggiungere il massimo livello di sicurezza dei dati. Del resto, le decisioni basate sulla contestualizzazione possono rivelarsi più efficaci di quelle operate al solo fine di adeguarsi a dei criteri astratti stabiliti dalla legge. Questo è il motivo per cui il Regolamento (UE) non contiene un elenco tassativo e puntuale delle misure di sicurezza da attivare – esprimendosi unicamente in termini di loro adeguatezza al rischio, vale a dire di effettiva protezione delle persone fisiche – affinché i dati non vengano sottratti,

persi o usati in maniera distorta rispetto alle finalità per cui sono stati raccolti. Di conseguenza, la scelta delle modalità di attuazione dei principi fondamentali e delle regole di fondo della normativa europea, oltre che flessibile e adattabile al mutare delle esigenze e degli strumenti tecnologici utilizzati di volta in volta per trattare i dati, è rimessa alla discrezionalità del titolare, in nome di una responsabilizzazione consapevole e, come verrà chiarito più avanti, anche documentata.

In verità, il GDPR fornisce delle indicazioni operative volte ad orientare l'identificazione delle misure e degli accorgimenti idonei a garantire il rispetto dell'accountability, nonché a dimostrarne in qualche modo l'osservanza, anche se nulla può esonerare il titolare dalle possibili attività di verifica ad opera delle Autorità di controllo. A tal proposito, preme qui segnalare: l'adozione di codici di condotta e l'ottenimento di certificazioni (artt. 40-42); la designazione di un Data Protection Officer (art. 37) [v. voce]; la redazione delle valutazioni d'impatto sulla protezione dei dati (o DPIA) quando un trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche e a monte del trattamento stesso (art. 35); la corretta autorizzazione e istruzione delle persone fisiche che trattano i dati personali sotto l'autorità diretta del titolare (art. 29); l'individuazione e la successiva nomina degli eventuali responsabili del trattamento (art. 28). Inoltre, l'art. 32 stabilisce alcuni parametri che il titolare deve considerare per elaborare un proprio piano di sicurezza quanto più adeguato ed efficace rispetto al rischio inerente alle caratteristiche delle operazioni che coinvolgono i dati personali, bilanciando interessi contrapposti con piena autonomia di giudizio e guardando sì ai costi, ma anche allo stato dell'arte e alle migliori tecnologie disponibili.

Tutto ciò è perfettamente in linea con un'inedita impostazione – che potremmo definire rischio-centrica –, per cui colui che maneggia i dati deve porre grande attenzione ai possibili impatti negativi sui diritti e sulle libertà fondamentali degli interessati, al fine di implementare delle misure tecniche e organizzative finalizzate a mitigarli, rendendosi così accountable. E proprio questo approccio basato sulla valutazione *ex ante* dei rischi è alla base del concetto di accountability, quale strategia operativa che pone l'accento sulla 'sostanza' dell'adempimento in chiave di creatività e proattività del titolare, come pure sulla sua verificabilità, nei fatti e non solo sulla carta, da parte delle Autorità di controllo.

Più nello specifico, il Regolamento (UE) attribuisce al titolare il compito di decidere autonomamente – in ragione di processi, bisogni e meccanismi interni alla sua organizzazione – modalità, garanzie e limiti del trattamento di dati, purché ciò avvenga nel rispetto dei principi generali sanciti dall'art. 5, par. 1, del GDPR: di liceità, correttezza, trasparenza, limitazione delle finalità e della conservazione, minimizzazione, esattezza, integrità e riservatezza. Principi, che il titolare non solo è chiamato ad osservare, ma *ex* art. 5, par. 2, del GDPR deve essere, altresì, in grado di comprovare di avere rispettato, soprattutto con riguardo all'adeguatezza e all'efficacia delle misure di sicurezza concretamente impiegate.

È allora evidente come l'accountability combini due differenti aspetti, che emergono nettamente dalla lettura dell'art. 24 del GDPR e che coinvolgono entrambi proprio il titolare. Da un lato, la responsabilità di costruire un sistema di gestione dei dati quanto più possibile sicuro, approntando misure e/o procedure – che siano adatte alla tipologia e alle finalità del trattamento, alla natura dei dati trattati, nonché alla gravità dei rischi prevedibili per i diritti e le libertà degli interessati – da riesaminare costantemente e, se necessario, aggiornare a seguito dell'insorgenza di nuove vulnerabilità. Dall'altro lato, la necessità di rendicontare quanto eseguito in tema di protezione dei dati personali, precostituendo un apparato documentale da esibire all'uopo agli interessati o alle Autorità di controllo, in modo tale da provare di avere adempiuto correttamente alle disposizioni di legge. È il c.d. onere processuale della prova. Diversamente, il titolare potrebbe incorrere nelle ingenti sanzioni amministrative pecuniarie inflitte ai sensi dell'art. 83, par. 5, lett. a) del GDPR, che per le imprese possono arrivare fino al 4% del fatturato globale dell'anno precedente alla violazione di dati personali (c.d. data breach [v. voce]).

In tal senso, uno strumento fondamentale, introdotto *ex novo* dalla normativa europea e disciplinato all'art. 30 del GDPR, è rappresentato dal registro delle attività di trattamento, compilato dal titolare per tenere traccia appunto di tutti i trattamenti in essere nella propria struttura organizzativa, e che, qualora richiesto, deve essere messo a disposizione del Garante per la Protezione dei Dati Personali, visto che all'atto della verifica offre sicuramente un quadro completo del grado di compliance aziendale.

In un'ottica pragmatica di applicazione del principio di accountability, particolare attenzione, poi, va dedicata a quella tecnica comunemente sintetizzata dall'espressione inglese 'data protection by default and by design' (cfr. art. 25 del GDPR), ossia alla configurazione *ab origine* di ogni trattamento di dati secondo i dettami del Regolamento (UE), per porre realmente l'interessato al centro dell'attività informatica, garantendone i diritti in ogni tempo. Detto altrimenti, il titolare deve impiegare delle misure che assicurino la protezione dei dati fin dalla progettazione (by design) e per impostazione predefinita (by default), riducendo al minimo sia la quantità di dati personali da raccogliere sia la portata del trattamento effettuato successivamente alla loro acquisizione (c.d. minimizzazione), così come anticipando la tutela degli interessati addirittura alla fase della semplice ideazione di un prodotto, un applicativo o un servizio che necessitano di informazioni personali.

Al fine di implementare l'accountability, dunque, l'utilizzo della crittografia [v. voce], del mascheramento dei dati o di una pseudonimizzazione accorta che consenta di attribuire i dati personali a un interessato specifico soltanto adoperando delle informazioni ulteriori (o chiavi di reidentificazione) non a disposizione di tutti (cfr. art. 4, par. 1, n. 5 del GDPR), possono fare senz'altro la differenza come indici virtuosi del trattamento di dati, consentendo di prevenire eventuali danni piuttosto che ripararli.

D'altronde, dinanzi al risvolto sociale, economico e politico assunto oggi dai dati personali, il valore e l'esigenza della loro protezione e, più in generale, della sicurezza informatica, non è più esclusivamente una prerogativa dell'interessato, ma diventa anche un'opportunità in termini di operatività ed efficienza per le aziende private e le amministrazioni pubbliche titolari, facendo sì che la riforma europea disveli tutto il suo potenziale.

Se così è, proprio l'accountability può rappresentare una garanzia in termini di vantaggio competitivo e di fiducia del cliente per tutti quei gestori di prodotti e servizi della società dell'informazione che richiedono l'utilizzo di dati personali, qualora sappiano predisporre misure e soluzioni 'privacy oriented', cioè specificamente volte a rinvigorire la sempre più compromessa sfera privata degli individui.

Bibliografia minima essenziale

Bolognini L., Pelino E., Bistolfi C., *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè, Milano, 2016.

Borrillo B., *La tutela della privacy e le nuove tecnologie: il principio di accountability e le sanzioni inflitte dalle Autorità di controllo dell'Unione europea dopo l'entrata in vigore del GDPR*, in *Dirittifondamentali.it*, 2/2020, pp. 326-356.

Celella R., *Il principio di responsabilizzazione: la novità del GDPR*, in *Ciberspazio e Diritto*, 1-2/2018, pp. 211-224.

Ciccia Messina A., Bernardi N., *Privacy e Regolamento europeo*, Ipsoa, Milano, 2017.

D'Ambrosio M., *Progresso tecnologico, "responsabilizzazione" dell'impresa ed educazione dell'utente*, Edizioni Scientifiche Italiane, Napoli, 2017.

Finocchiaro G., *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019.

Mantelero A., *Responsabilità e rischio nel Regolamento UE n. 2016/679*, in *Le nuove leggi civ. comm.*, 1/2017, pp. 144-164.

Mazzoni F., *Regolamento Europeo 2016/679: alcune normazioni di riferimento per declinare sul campo il principio dell'accountability*, in *Ciberspazio e Diritto*, 1-2/2019, pp. 197-239.

Riccio G.M., Scorza G., Belisario E. (a cura di), *GDPR e Normativa Privacy. Commentario*, Wolters Kluwer, Milano, 2022.

Russo G., Polini M., *I principi di accountability e di effettività nel nuovo Regolamento*, in M. Maglio, M. Polini, N. Tilli (a cura di), *Manuale di diritto alla protezione dei dati personali. La privacy dopo il Regolamento UE 2016/679*, Maggioli, Santarcangelo di Romagna, 2017, p. 127 ss.

Ziccardi G., *Il GDPR e i suoi adempimenti*, in G. Ziccardi, P. Perri (a cura di), *Tecnologia e diritto*, vol. II, Giuffrè, Milano, 2019.

A

Algoritmo

[3] ***a.*** Nozioni preliminari
b. Implicazioni

G.P.
M.N.C.

a. Il termine algoritmo deriva dalla latinizzazione del nome del matematico persiano Abū Ja'far Muḥammad ibn Mūsā al-Khuwārizmī, vissuto tra il 780 e l'850 d.C. e considerato anche il padre dell'algebra. Con l'espressione algoritmo ci si riferisce a un insieme (o, meglio, ad una sequenza ordinata) di operazioni idonee a risolvere una determinata classe di problemi oppure a condurre al risultato di una certa operazione (espressione) matematica.

Si osservi, però, perché si abbia un algoritmo non è sufficiente essere in presenza di un procedimento (o, meglio, di un insieme di passaggi), ma è essenziale che ciascuna operazione prevista sia: a) atomica (ovvero che non sia ulteriormente scomponibile in altri sotto-passaggi); b) inequivoca (cioè, che sia non soltanto chiara, ma che sia anche priva di qualsivoglia elemento di ambiguità); c) finita e definita (ossia, limitata nel numero delle operazioni e dei dati richiesti); d) circoscritta (ovvero, destinata a giungere alla conclusione dell'operazione in un lasso temporale ben determinato); e) effettiva (idonea a produrre un risultato univoco, a prescindere da chi sia l'esecutore materiale dei diversi step previsti). Di qui – e non a caso – la possibilità di affermare che un algoritmo ben fatto porterà chiunque, uomo o macchina che sia, a ottenere lo stesso risultato.

In questa sede, è importante rimarcare che, sebbene il termine si riferisca soprattutto all'ambito matematico e informatico, è possibile parlare di algoritmo anche con riguardo alla sequenza di istruzioni di un elettrodomestico o, più semplicemente, dinnanzi ad una ricetta di cucina. Fermo il fatto che, per poter essere definita empiricamente come un algoritmo, però, quest'ultima non dovrà essere ambigua (ad esempio non potrà presentare espressioni generiche e indeterminate come 'salare e

pepare a piacimento') e non dovrà contenere passaggi scomponibili a loro volta. Se così – e sulla base degli aspetti strutturali sinteticamente individuati – può dirsi che, nonostante non vi sia una definizione formale di algoritmo, esso può comunque essere descritto come una sequenza ordinata e finita di passi elementari che conduce a un ben determinato risultato in un tempo finito.

Decisivi in argomento gli studi di Church e quelli di Turing, per il quale se un problema è umanamente calcolabile, allora esisterà una macchina in grado di risolverlo, cioè di calcolarlo. Ma se così, la classe di funzioni calcolabili va a coincidere con quella delle funzioni che sono poi concretamente calcolabili da parte della macchina. Altrimenti detto, secondo Turing, una funzione può essere ritenuta computabile se esiste una macchina (cioè un insieme di istruzioni) in grado di calcolarla. Ragion per cui, nonostante l'esiguità dei mezzi tecnici a disposizione, le macchine di Turing sono comunque in grado di computare qualsiasi funzione che sia computabile dal più potente degli elaboratori elettronici. Tale concetto è alla base della nozione teorica di calcolabilità: difatti, un problema è calcolabile quando è risolvibile mediante un algoritmo.

Vien da sé che, in ambito informatico l'algoritmo sia fondamentale per la programmazione dello sviluppo di un software [v. voce]: se si vuole automatizzare e risolvere un dato problema, infatti, bisogna codificare un algoritmo *ad hoc* capace di risolvere quel determinato problema attraverso uno specifico programma, scritto in un certo linguaggio e che sarà poi eseguito dal calcolatore. In breve, può dirsi che l'algoritmo costituisce la logica di elaborazione del problema che consente poi al calcolatore di risolvere il problema iniziale.

b. Si badi: quella degli algoritmi è una storia addirittura millenaria, che affonda le proprie radici nell'antico Egitto e nella Babilonia del 1.800-1.600 a.C., nell'arco della quale l'opera *Kitab al-hisab al-hindi* del già citato Al-Khuwarizmi (che spiega il sistema di numerazione indiano, introduce un simbolo speciale per lo zero e illustra le regole per compiere le quattro operazioni principali anche con le frazioni) viene unanimemente considerata come un importante punto di svolta, che segna un prima e un dopo nella matematica; alla quale, nel corso del

1200, ha fornito un apporto decisivo Ludovico Pisano (meglio noto come Fibonacci).

Nel suo celebre *Liber Abaci*, infatti, Fibonacci non si è limitato alla mera traduzione del testo arabo (per altro indispensabile alla sua concreta diffusione), ma ha provveduto anche ad integrare la matematica indo-arabica con quella euclidea, prospettando, così, un volume in cui la materia – per la prima volta in assoluto – veniva spiegata e resa accessibile ai commercianti: veri destinatari del testo, in quanto costretti ad avvalersene quotidianamente nel corso degli scambi e delle transazioni, come pure, per la soluzione di tutte le diverse questioni pratiche contingenti. Ed è proprio in questa peculiare genesi storica che, a suo modo, può rintracciarsi l'origine della più generale e condivisa definizione di algoritmo: strumento di calcolo, ma anche – e soprattutto – procedimento idoneo a risolvere qualunque problema tramite il computo, o più correttamente, attraverso una "sequenza di istruzioni in base alle quali il calcolatore elabora un processo di calcolo" (Zellini 2018).

Atteso che il lemma in esame rinvia ad una nozione generalmente nota, oltre che alquanto risalente, non si può non convenire sul fatto che l'algoritmo – soprattutto nel corso degli ultimi decenni – abbia conquistato una diffusione e un rilievo sociale mai visti prima e, per molti aspetti, anche radicalmente inediti. Oggi, infatti, l'importanza di cui gode l'algoritmo trascende le asettiche funzioni logico-computazionali, tipiche delle primissime fasi della sua nascita e del suo sviluppo. Paradigmatico, in tal senso, è senza dubbio l'*incipit* con cui Pedro Domingos – interrogandosi sull'algoritmo definitivo – avvia la sua riflessione, nella quale, per l'appunto, pone immediatamente l'accento sul fatto che: "viviamo nell'epoca degli algoritmi" (Domingos 2016, p. 1).

È interessante sottolineare che i fattori che hanno concorso a questo cambio di prospettiva sono stati diversi, fra questi: *i) in primis*, la nascita del World Wide Web [v. voce] e la progressiva diffusione di dispositivi sempre più performanti e – quel che più conta – perennemente connessi alla rete e fra loro (si pensi all'IoT [v. voce] e alla domotica [v. voce]); *ii)* l'acquisizione da parte degli algoritmi della capacità di misurarsi con informazioni di qualunque genere, non già, semplicemente, con dati numerici; *iii)* il fatto che, negli anni, gli algoritmi di tipo deterministico (nei quali ad ogni input corrisponde un solo output pro-

grammato e già noto in partenza) siano stati, via via, affiancati dagli algoritmi di natura non-deterministica (in cui ad ogni input può corrispondere più di un output), ossia, da algoritmi capaci di processare simultaneamente moli impressionanti di dati e di svolgere funzioni statistico-probabilistico-previsionali, avvalendosi, ora, dell'apprendimento supervisionato, ora, di quello autonomo (Mezza 2018; Laura 2019; Vespignani 2019).

Protagonisti indiscussi di tutti i principali dibattiti contemporanei (non solo tecnico-informatici e scientifici, ma anche giuridici, politici, economici…), gli odierni algoritmi sembrano ora inverare – in chiave digitale e, per così dire, passando dalla carne al silicio – quel celebre "*calculemus*", al quale invitava Leibniz, oppure il noto motto "*non disserto, sed computo*", avanzato da Hobbes. Non v'è, infatti, frangente della vita che non sembri essere già colonizzato e, talvolta, persino diretto dalle scienze matematiche. Ma non è tutto, perché, se, da un lato, muovendo dalla consapevolezza che "non c'è calcolo che non ne possa implicare un altro e poi ancora un altro", si assiste ad un'inesausta corsa all'algoritmo successivo, un algoritmo che si auspica ancor più potente, rapido ed infallibile; da un altro lato, sembra diventato quasi impossibile distinguere la linea di demarcazione fra "la scienza del calcolo e […] la mera tecnologia sociale" (Amato Mangiameli 2021, pp. 129 e 133).

Gli algoritmi in pratica – con quel loro preciso, utile, eppure assai criptico procedere – dischiudono (e in parte realizzano) una nuova dimensione, quella dell'infosfera [v. voce], che è fatta "di complesse dipendenze reticolari, di reazioni a catena meccaniche […], di connessioni obbligate" (Floridi 2017, p. 31), ed in cui si impone quella misteriosa e penetrante forma di potere e di regolazione che va sotto il nome di scienza delle previsioni.

Àuguri digitali del terzo millennio, gli algoritmi – grazie ad un ensemble di analisi computazionali e di procedure di profilazione [v. voce] sempre più sofisticate e affidabili – non solo ci avvisano di ciò che sta per accadere, ma ci suggeriscono anche cosa sarebbe opportuno fare, avvalendosi, a seconda dei casi e delle situazioni, di seducenti inviti all'acquisto, oppure, di raccomandazioni comportamentali di vario genere. Si concretizza, così, quell'intricato e non sempre trasparente meccanismo di controllo-previsione-regolamentazione, basato su di un'al-

ternanza di "estrazione e reindirizzazione ubique, attivazione (tunning, herding, condizionamento), catene di rifornimento del surplus comportamentale, processi industriali basati sulle macchine, fabbricazione di prodotti predittivi, mercati dinamici dei comportamenti futuri e targettizzazione […]". Un meccanismo che, in virtù (e a causa) del machine learning [v. voce], anche quando produce il risultato desiderato (l'analisi, la previsione, la targettizzazione, la realizzazione di una strategia di nudging [v. voce]), non di rado, può riattivarsi pressoché subito, continuando a prospettare nuove e "ulteriori pratiche di tunning, herding e condizionamento" (Zuboff 2019, p. 461).

Guardando alle tante possibili implicazioni del loro procedere non si può non sottolineare che – da un certo punto di vista e *mutatis mutandis* – gli algoritmi contemporanei sembrano rinnovare quella specie di sodalizio, che ha sempre permeato la stretta relazione fra le logiche poste a fondamento (e garanzia) del potere, nelle sue diverse forme, ed il ricorso alla capacità calcolante-misurativa-predittiva. Una relazione che, adesso, si ripropone in chiave decisamente più larvata e pulviscolare, facendo emergere nuove e inaspettate forme di *arcana imperii* ed aprendo il varco a un'occulta tirannia (cfr. Cardon 2016; Banasayang 2020).

Il richiamo a due recenti vicende può rivelarsi, a suo modo, estremamente funzionale. La prima vicenda riguarda un evento, svoltosi a Berlino nel febbraio del 2020, che ha visto protagonista Simon Weckert. Lo street artist tedesco appassionato di tecnologia, grazie a uno stravagante escamotage, non si è limitato a inscenare una performance, ma ha realizzato anche un interessante esperimento sociale. Dopo aver riposto novantanove smartphone connessi alla rete in una sorta di carrellino-trolley, Weckert ha iniziato a passeggiare per le strade completamente deserte della città. L'intento dell'artista era quello di provare a ingannare l'algoritmo di Google Maps, simulando un fittizio ingorgo stradale a fronte di una situazione reale di assoluta assenza di traffico. Il risultato è stato al contempo esilarante e sconcertante, l'artista, infatti, ha facilmente giubilato l'algoritmo dell'app, riuscendo in questo modo a condizionare le scelte di tutte le persone che, in quel frangente, erano connesse all'applicazione, alle quali l'applicazione aveva 'giustamente' suggerito di optare per percorsi alternativi. La seconda vicenda, dai toni mol-

to diversi, si è svolta a Firenze nell'ottobre del 2022, quando uno dei tanti rider di Glovo – dei quali l'azienda gestisce e monitora il lavoro tramite app – nel pieno rispetto di quanto previsto dal contratto, mancando una consegna, si è visto recapitare in automatico dall'algoritmo una mail di licenziamento. Il paradosso è che, nel caso di specie, l'algoritmo – nel suo procedere – non poteva certo tener conto di una variabile inattesa, ovvero che quell'omissione a carico del rider, in realtà, era stata dovuta ad un incidente stradale dagli esiti mortali.

Bibliografia minima essenziale

(***a.***)

Church A., *Introduction to mathematical logic*, Princeton University Press, Princeton, 1956.

Luccio F., *La struttura degli algoritmi*, Bollati Boringhieri, Torino, 1982.

Turing A.M., *Computability and λ-definibility*, in *The Journal of Symbolic Logic*, 4/1937, pp. 153-163.

(***b.***)

Amato Mangiameli A.C., *Algoritmi e big data. Dalla carta sulla robotica*, in *Rivista di Filosofia del diritto*, 1/2019, pp. 107-124.

Amato S., *Emozioni sintetiche e sortilegi al silicio*, in T. Casadei, A. Andronico (a cura di), *Algoritmi ed esperienza giuridica*, *Ars interpretandi*, 1/2021, pp. 129-151.

Banasayang M., *La tirannia dell'algoritmo*, trad. it., Vita e Pensiero, Milano, 2020.

Cardon D., *Cosa sognano gli algoritmi. Le nostre vite ai tempi dei big data*, trad. it., Mondadori, Milano, 2016.

Domingos P., *L'algoritmo definitivo. La macchina che impara da sola e il futuro del nostro mondo*, trad. it., Bollati Boringhieri, Torino, 2016.

Floridi L., *La quarta rivoluzione industriale. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina, Milano, 2017.

Laura L., *Breve e universale storia degli algoritmi*, Luiss University Press, Roma, 2019.

Mezza M., *Algoritmi della libertà. La potenza di calcolo tra dominio e conflitto,* Donzelli, Roma, 2018.

Taddei Elmi G., *Algoritmi giuridici. Ius condendum o "fantadiritto"*, Pacini, Pisa, 2020.

Valerio C., *La matematica è politica*, Einaudi, Torino, 2020.

Vespignani A., *L'algoritmo e l'oracolo. Come la scienza predice il futuro e ci aiuta a cambiarlo*, il Saggiatore, Milano, 2019.

Vineis P., Carra L., Cingolani R., *Prevenire. Manifesto per una tecnopolitica*, Einaudi, Torino, 2020.
Zellini P., *La dittatura del calcolo*, Adelphi, Milano, 2018.
Zuboff S., *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri,* trad. it., Luiss University Press, Roma, 2019.

A

[4] Amministrazione digitale

M.M.

Già solo ad una prima analisi semantica, il lemma amministrazione digitale esprime la combinazione tra due vocaboli di cui l'uno (digitale) qualifica l'altro (amministrazione), per indicare non soltanto il sistema di gestione digitalizzata della pubblica amministrazione – che consente di trattare la documentazione e di gestire i procedimenti con sistemi informatici, grazie all'uso delle tecnologie dell'informazione e della comunicazione (ICT) [v. voce] – ma anche per condensare l'esito di un graduale processo evolutivo che ha lasciato confluire le nuove tecnologie nelle attività dell'amministrazione pubblica.

Del resto, la pervasività dell'incalzante rivoluzione digitale [v. voce] non avrebbe non potuto interessare l'esercizio del potere pubblico tout court e, in particolare, quello della pubblica amministrazione. La contaminazione del digitale nell'organizzazione e nell'esercizio delle funzioni pubbliche è un fenomeno che non si manifesta da oggi. Nel tempo, infatti, l'azione amministrativa ed il rapporto amministrazione-amministrato sono stati interessati da progressivi processi di tecnologizzazione, i quali ne hanno profondamente inciso ogni aspetto organizzativo-gestionale, proiettandone una rinnovata figurazione.

Dall'immagine ottocentesca d'impronta francese, la quale riflette un'organizzazione monista ordinata intorno al principio gerarchico e al principio di uniformità, all'evoluzione successiva che palesa graduali ed ampie dilatazioni della stessa attività amministrativa intesa sia in senso soggettivo che oggettivo, e sino all'entrata in vigore della Carta costituzionale, la quale riconforma la concezione tradizionale sul calco dei principi di buon andamento e di imparzialità (artt. 97-98 Cost.), sono innumerevoli le trasformazioni che hanno attraversato l'amministrazione tanto da costituire uno degli ingranaggi più complessi della macchina statale.

Per certo, però, le trasformazioni tecnologiche hanno generato la più