Dividere Facebook? Zuckerberg risponde al cofondatore Hughes: ‘Dannoso per gli utenti’

Dividere **Facebook** per evitare un monopolio di fatto? Non se ne parla proprio: è un’idea inutile e avrebbe anche un effetto dannoso sugli utenti. E’ quanto sostiene **Mark Zuckerberg**, che risponde in maniera netta alle accuse lanciate pochi giorni fa da **Chris Hughes**, il cofondatore del social network.

Durante la sua visita in Francia dove ha incontrato anche il Presidente **Emmanuel Macron** – ha risposto nel corso di un’intervista rilasciata a *France2*. “*La mia reazione? Credo che quello che propone non sia assolutamente utile*”, ha detto Zuckerberg.

Secondo Hughes la dimensione di Facebook rende l’azienda troppo potente, e “non americana”, un ostacolo alla libera concorrenza e ai principi del Paese a stelle e strisce. Per questo – rilanciando una proposta già avanzata dalla senatrice democratica e candidata alle presidenziali **Elizabeth Warren** – ha chiesto che il “*moloch*” dei social (che controlla anche **Instagram** e **Whatsapp**, oltre al servizio di messagistica interno Messenger) venga diviso in almeno tre parti, così da assicurare un maggiore controllo.

Dimensione globale per contrastare le interferenze

Tutto il contrario di quello che pensa Zuckerberg, convito che proprio la dimensione globale di Facebook e la potenza economica della sua azienda, siano una tutela in più per gli

utenti. “*Se abbiamo interesse a proteggere la democrazia e le elezioni* – ha detto Mark – *allora c’è bisogno di una compagnia come la nostra, che investe miliardi di dollari ogni anno nella creazione di strumenti utili e all’avanguardia per contrastare le interferenze nelle elezioni. Il nostro budget per la sicurezza quest’anno è maggiore degli interi ricavi di quando ci siamo quotati in borsa all’inizio di questo decennio. E questo riusciamo a farlo proprio perché siamo stati in grado di far crescere un business di successo capace di sostenere queste spese*”.

Fake news, privacy e business

La lotta a pagine e notizie “fake” trova conferma nell’ultimo “taglio” effettuato dalla piattaforma su migliaia contenuti dopo la segnalazione della Ong Avaaz,ma anche nel report sulle attività di lobbying che Facebook ha portato avanti nel corso degli anni, in cui però alla tutela della privacy degli utenti si affianca quella degli investimenti, con pressioni sul mondo della politica.

Una attenzione alla privacy che alcuni ritengono ormai fuori tempo massimo e autoassolutoria, in particolare dopo gli scandali sulla gestione dei dati degli utenti – il più eclatante è quello legato a Cambridge Analytica – che a breve potrebbe costare una multa salata alla piattaforma social.

https://www.key4biz.it/dividere-facebook-zuckerberg-risponde-al-cofondatore-hughes-dannoso-per-gli-utenti/257755/

Whatsapp, Facebook e Instagram unificati? I rischi di questa aggregazione

Rubrica settimanale **Cosa Compro**, frutto della collaborazione fra Key4biz e **SosTariffe**. Un servizio al consumatore: qualità, virtù e difetti dei prodotti hitech di uso quotidiano. Per consultare tutti gli articoli **clicca qui**.

È un periodo particolarmente attivo per **WhatsApp**, il servizio di instant messaging più utilizzato del pianeta: secondo le ultime indiscrezioni, pare che l'app sia pronta per implementare a livello globale alcune funzioni finora presenti solo in fase beta. Non solo: **Facebook** ha confermato, seppur indirettamente, l'arrivo dell'unificazione tra l'app di messaggistica e il social network. Vedremo, infine, quali smartphone non avranno più il supporto dell'app già dalla fine dell'anno e l'inizio del 2020.

Nuova funzione: effettuare e ricevere pagamenti sull'app

Ma andiamo con ordine, partendo prima da una nuova feature che dovrebbe essere presto presente anche nei nostri mercati: WhatsApp, infatti, permetterà agli utenti di **inviare e ricevere denaro con i propri contatti**, sfruttando carte e account bancari compatibili con il servizio. La società garantisce la massima sicurezza sulle transazioni e pare che i primi test in Asia abbiano ottenuto dei buoni risultati. Per ora **non è stata svelata alcuna data ufficiale di lancio**, ma le nuove assunzioni in Europa farebbero pensare ad un'accelerazione in tal senso.

Whatsapp, Facebook e Instagram con una chat unificata?

E proprio i contatti sono il tema centrale di un'altra novità che Facebook ha intenzione di introdurre: **l'unificazione dei servizi di messaggistica delle app controllate dal social network**. L'idea di fondo, in pratica, è di poter riuscire a comunicare tra amici e contatti WhatsApp, Instagram e Facebook, senza necessariamente avere il numero di telefono di un utente. L'integrazione tra le varie applicazioni conferma la volontà di Zuckerberg e soci di **semplificare e rendere i tre servizi maggiormente legati tra loro**, soprattutto per quanto riguarda le comunicazioni tra utenti: una scelta che, tuttavia, cozza con quanto la stessa Facebook aveva dichiarato a seguito dell'acquisizione di WhatsApp, quando aveva garantito la separazione netta tra le due piattaforme.

L'idea di un ecosistema di messaggistica unico, invece, è trapelata dopo alcuni servizi pubblicati sul **New York Times** a gennaio di quest'anno e che riprendevano delle importanti testimonianze anonime provenienti dal gruppo coinvolto nel progetto. Si parlava di un servizio di chat con un alto livello di sicurezza e **crittografia end-to-end** per tutti gli iscritti a Facebook, Instagram e WhatsApp e la possibilità di contattare qualsiasi utente delle piattaforme, **senza necessariamente essere iscritti a tutte e tre**.

Quali rischi

Quali potrebbero essere le conseguenze di questa aggregazione? È ancora presto per dirlo e vorremo avere maggiori informazioni, soprattutto sul **tema privacy e trattamento dei dati** per dare un giudizio definitivo: è anche vero, però, che

i continui scandali su Facebook su questi temi, il disastro **di Cambridge Analytica** e tanti altri dubbi rendono il progetto di unificazione dei tre servizi abbastanza preoccupante.

Attendiamo, quindi, di avere tutte le notize in merito, così da comprendere esattamente quale strada Zuckerberg ha intenzione di percorrere per recuperare la fiducia di utenti, aziende e governi.

Whatsapp: fine del supporto per tutti i Windows Phone

Vi segnaliamo, infine, un'altra notizia importante legata a WhatsApp: pare che il servizio, dopo la prima ondata di tagli avvenuta un paio di anni fa, **smetterà di funzionare anche su altre piattaforme software datate e/o quasi inutilizzate**. Ecco la lista definitiva e il termine ultimo dopo il quale WhatsApp non funzionerà più:

- Android 2.3.7 e versioni precedenti, dopo il 1° febbraio 2020;
- iOS 7 e versioni precedenti, dopo il 1° febbraio 2020;
- **tutti i sistemi operativi di Windows Phone**, dopo il 31 dicembre 2019.

WhatsApp aggiunge anche la seguente nota: "*dato che non sviluppiamo più per questi sistemi operativi, alcune funzioni **potrebbero smettere di funzionare in qualsiasi momento***".

Insomma, se possedete un vecchio Android, un vecchio iPhone o un qualsiasi dispositivo Windows Phone (compresa l'ultima versione Windows 10 Mobile) e volete continuare ad utilizzare WhatsApp, **è giunto il momento di cambiare telefono**: se volete risparmiare un po' e godere di particolari sconti e vantaggi, potete consultare **le offerte cellulari con smartphone incluso** proposte dai principali operatori telefonici italiani su

SOSTariffe.it, dove riuscirete sicuramente a trovare delle proposte ad hoc per le vostre necessità.

https://www.key4biz.it/whatsapp-facebook-e-instagram-unificati-i-rischi-di-questa-aggregazione/257462/

Ex-Intelligence Analyst Charged With Leaks to Reporter

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/O9pvq5rGBjM/ex-intelligence-analyst-charged-leaks-reporter

---

Canadian Telecom Firm Freedom Mobile Exposed Customer Details

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/w0S9yqy2pWc/canadian-telecom-firm-freedom-mobile-exposed-customer-details

Sicurezza informatica e privacy, entra in gioco l'informatica quantistica con il "qubit"

Nelle ultime ore ha fatto scalpore l'attacco informatico del collettivo LulzSec_ITA, che ha sottratto e diffuso online oltre 30.000 credenziali di PEC di membri dell'Ordine degli Avvocati di Roma. nomi eccellenti, tra cui il sindaco di Roma, Virginia Raggi.
Un fatto grave, che evidenzia le ancora troppo grandi vulnerabilità delle organizzazioni e allo stesso tempo l'efficacia delle azioni dei cyber criminali, a cui però è possibile porre rimedio.
Nel mondo, secondo Cybersecurity Ventures, dal 2013 ad oggi, sono stati rubati giornalmente 3.809.448 dati personali e sensibili: ogni secondo, in sostanza, vengono sottratti dati da 44 account per mezzo di attacchi informatici.

Questo significa, che password di accesso, numeri di carte di credito e messaggi di chat, sono tutti protetti da complicati algoritmi matematici, che sono alla base dei moderni sistemi di crittografia. Sistemi avanzatissimi, ma ancora non perfetti.
Nello **studio** intitolato "***All-fiber self-compensating polarization encoder for Quantum Key Distribution***",pubblicato dalla rivista *Optics Letters*, il gruppo di ricerca "*QuantumFuture*" del dipartimento di Ingegneria dell'informazione dell'**Università di Padova** ha proposto un nuovo sistema di crittografia basato sullo scambio di "*quantum bit*" (o "***qubit***").

Stiamo parlando di informatica quantistica e il *qubit* è la versione quantistica del bit classico: “*mentre il bit classico può assumere solo due valori distinti, 0 oppure 1, il qubit si può trovare in una “sovrapposizione” quantistica tra i due stati |0> e |1>”,* si legge in un articolo pubblicato sul sito dell’ateneo *ilbolive.unipd.it*.
I ricercatori di Padova presentano quella che è definita la “***distribuzione quantistica di chiave***”, o in sigla QKD, che permette di “*creare una chiave di cifratura condivisa e sicura tra due utenti*”: “*La chiave è creata codificando i qubit nella polarizzazione (la polarizzazione della luce è legata alla direzione di oscillazione del campo elettrico) di singoli fotoni scambiati tra essi*”.

La sicurezza è garantita dalle **leggi della meccanica quantistica**, che assicurano che “*nessun altro utente può avere informazioni sulla chiave. Tali leggi assicurano che non esiste la “fotocopiatrice quantistica” (un qubit non può essere copiato) e che una qualunque misura sul qubit ne altera il suo stato*”.
“***Ci si aspetta che la QKD abbia un profondo impatto sulla privacy e sulla sicurezza dei cittadini*** – ha dichiarato nell’articolo **Giuseppe Vallone**, che ha guidato questa ricerca all’interno del gruppo QuantumFuture coordinato dal co-autore **Paolo Villoresi** – *il nostro schema semplifica la generazione di qubit codificati nella polarizzazione dei fotoni. La polarizzazione è in particolare la codifica più adatta alle comunicazioni quantistiche in spazio libero, come da satellite verso Terra o tra i terminali mobili, in quanto non viene perturbata durante la propagazione*”.

Il sistema sviluppato dal gruppo di ricerca “*QuantumFuture*”, “*per codificare efficientemente e rapidamente i qubit nella polarizzazione dei singoli fotoni*”, chiamato **schema POGNAC** (da *Polarisation Sagnac*), permette di avere un dispositivo

compatto, completamente in **fibra ottica** e "*autocompensante*": "*è stato realizzato con componenti commerciali, tipicamente usati per le comunicazioni classiche in fibra, permettendo di modulare la polarizzazione più di un miliardo di volte al secondo e al contempo semplificando il setup e riducendo i costi totali del dispositivo. Grazie a questi due fattori chiave – stabilità e alta velocità di modulazione – questo schema risulta ideale per i protocolli di QKD in spazio libero e in fibra*".

https://www.key4biz.it/sicurezza-informatica-e-privacy-entra-in-gioco-linformatica-quantistica-con-il-qubit/257160/

Pubblicità cartacea indesiderata, cosa fare per non riceverla più a casa

È attivo dal 6 maggio 2019 il servizio gratuito di iscrizione per i cittadini al **Registro Pubblico delle Opposizioni** per non ricevere **pubblicità cartacea indesiderata** agli indirizzi postali presenti negli elenchi telefonici pubblici.

Telemarketing esteso alla posta cartacea

L'estensione dell'ambito di applicazione del Registro alla posta cartacea – stabilita dall'art.1, comma 54, della **Legge 4 agosto 2017**, n. 124 e regolamentata dal D.P.R. n. 149/2018 – ha equiparato il trattamento per finalità di **marketing** degli indirizzi postali presenti negli elenchi telefonici pubblici a quello delle relative numerazioni, estendendo l'opt-out

telefonico a **quello cartaceo.**

Cosa prevede la legge

Come previsto dal Regolamento attuativo, entro 90 giorni dall'entrata in vigore del provvedimento è stata completata la realizzazione tecnica del Registro **esteso alla posta cartacea**. Al fine di garantire ai cittadini un tempo congruo per bloccare l'invio di posta pubblicitaria indesiderata, gli **operatori di marketing** dovranno attendere i termini stabiliti dal medesimo Regolamento per poter utilizzare, previa verifica con il Registro Pubblico delle Opposizioni, gli indirizzi postali presenti negli elenchi telefonici degli utenti che non hanno espresso l'opposizione.

Il trattamento degli indirizzi postali per fini commerciali rimarrà valido anche a seguito dell'iscrizione nel Registro solo se gli operatori avranno raccolto apposito consenso dell'interessato, secondo la normativa vigente in materia di privacy e in particolare il **Regolamento (UE) 2016/679.**

Cos'è il Registro delle Opposizioni

Il servizio, attivo dal 2011 per le opposizioni alle chiamate di **telemarketing**, è stato realizzato e sarà gestito dalla **Fondazione Ugo Bordoni** – che svolge attività di supporto alla Pubblica Amministrazione nel campo dell'ICT – su affidamento del **Ministero dello Sviluppo Economico** attraverso un contratto di servizio.

Cosa fare per non ricevere più la

posta

Per chi desidera non ricevere più la pubblicità cartacea gli intestatari di un numero presente negli elenchi telefonici pubblici a partire dal **6 maggio 2019** possono iscriversi al **Registro** esprimendo l'opposizione sia alle chiamate di telemarketing sia alla pubblicità cartacea.

Gli utenti già iscritti al servizio per non ricevere la pubblicità telefonica potranno richiedere l'iscrizione per non ricevere nemmeno quella cartacea. L'opposizione può essere espressa mediante quattro modalità disponibili: **web**, **numero verde, email e raccomandata.**

La campagna di Key4biz contro il telemarketing selvaggio

- **Telemarketing a un bivio: tornare all'anno zero per riformare il settore**
- **Telemarketing verso una svolta? La parola ai protagonisti (video)**
- **'Chiamate moleste insopportabili, la legge va cambiata'. Intervista ad Antonello Soro (Garante Privacy)**
- **Telemarketing, Antonello Soro (Garante Privacy): 'In 5 anni 25mila segnalazioni'**
- **'Telemarketing, estendere le tutele a tutti i numeri fissi e mobili non in elenco'. Intervista ad Alessandro Luciano (FUB)**
- **'Chiamate moleste, serve una riforma del sistema call center'. Intervista a Massimiliano Dona (UNC)**
- **Chiamate moleste: perché il Governo non vuole i cellulari nel Registro delle Opposizioni?**
- **'Chiamate moleste, i cittadini non sono un elenco marketing'. Intervista ad Anna Cinzia Bonfrisco (Cor)**
- **'Telemarketing, troppi call center non rispettano le regole'. Intervista a Paolo Sarzana (Assocontact)**
- **Telemarketing, Garante Privacy: il Registro delle**

Opposizioni va migliorato

- **‘Telemarketing, estendere le tutele a tutti i numeri fissi e mobili non in elenco’. Intervista ad Alessandro Luciano (FUB)**
- **Chiamate moleste: perché il Governo non vuole i cellulari nel Registro delle Opposizioni?**
- **‘Chiamate moleste, serve una riforma del sistema call center’. Intervista a Massimiliano Dona (UNC)**
- **‘Chiamate moleste, i cittadini non sono un elenco marketing’. Intervista ad Anna Cinzia Bonfrisco (Cor)**
- **‘Telemarketing, troppi call center non rispettano le regole’. Intervista a Paolo Sarzana (Assocontact)**

Pubblicità cartacea indesiderata, cosa fare per non riceverla più a casa

---

Relazione annuale Garante Privacy, il discorso integrale di Antonello Soro

Signor Presidente, Autorità, Signore e Signori, presentiamo questa Relazione in conclusione del nostro mandato.

In questi anni è profondamente mutato il contesto sociale, economico, culturale e, con esso, il senso e l’orizzonte dell’azione dell’Autorità, così come il valore e la portata del diritto affidato alla sua tutela.

Le nuove tecnologie, che hanno consentito straordinarie e irrinunciabili conquiste per l’umanità, hanno progressivamente trasferito nello spazio digitale una parte significativa delle

attività private e pubbliche.

I dati, proiezione della persona in questa nuova dimensione della vita, alimentano lo sviluppo in ogni campo delle scienze e costituiscono il fondamento della nuova economia.

Il digitale è divenuto agente potentissimo di trasformazione sociale, struttura e sovrastruttura insieme: la cornice entro cui si dispiegano libertà e responsabilità, spingendo l'uomo a trascendere i suoi stessi limiti.

E con l'ambiguità di ogni tecnica, ma anche con la forza propria delle rivoluzioni epocali, il digitale può essere presupposto tanto di espansione quanto di limitazione delle libertà, se si inverte il rapporto tra mezzo e fine.

Governarne l'innovazione in funzione della tutela della persona e delle libertà è, allora, il vero obiettivo, da cui dipendono presente e futuro delle nostre società, con implicazioni che si estendono a ogni campo della vita individuale e collettiva. Dal lavoro alla salute e alla ricerca scientifica, ma anche alla giustizia, che in alcuni Paesi sta già avviandosi a divenire "predittiva", affidando agli algoritmi persino quelle decisioni dirimenti sull'uomo (colpevolezza, libertà, punibilità), che sembra- vano l'ultimo baluardo del dominio della razionalità umana.

Le tecnologie digitali intervengono nella definizione di criteri valoriali, orien- tando sempre più le decisioni sia individuali che collettive e, per altro verso, con- corrono a delineare l'esercizio della sovranità, modificando equilibri geopolitici prima indiscussi.

Lo stesso antagonismo commerciale tra USA e Cina sottende una competizione per l'egemonia tecnologica, che disegna la nuova geografia del potere planetario.

Il possesso e lo sfruttamento dei dati, che si accumulano nell'infosfera, sono la posta in palio.

A confronto sono due potenze che hanno maturato le proprie posizioni di vantaggio competitivo sulla raccolta massiva di dati, resa possibile da norme poco attente alle implicazioni di tale forma di "accumulazione estrattiva" sulle libertà individuali.

Tuttavia, se negli USA si sta avviando un percorso di rafforzamento della privacy, a seguito della sentenza **Schrems** e delle rivelazioni su **Cambridge Analytica** – che hanno dimostrato come la protezione dei dati sia un presupposto indispensabile di autonomia e sovranità – la realtà cinese sembra muoversi in senso assai diverso.

E l'entità dei rapporti commerciali tra Europa e Cina è tale da non poter più prescindere da una cornice di garanzie adeguate, soprattutto per la tutela dei dati, all'esito di auspicabili riforme quali quelle che hanno consentito la conclusione del **Privacy Shield** con gli USA e del recente accordo con il Giappone.

La sinergia tra assenza di norme efficaci a tutela della privacy e dirigismo (anche) economico favorisce, infatti, una sostanziale osmosi informativa tra i provider e il Governo cinese che, anche per ragioni culturali, può massivamente raccogliere dati personali, da riutilizzare per le finalità più diverse: dalla sicurezza nazionale alla promozione dell'**intelligenza artificiale.**

E persino per la realizzazione di un sistema di controllo sociale fondato sul capillare monitoraggio e la penalizzazione di comportamenti ritenuti socialmente indesiderabili, con la preclusione all'accesso persino a determinate scuole o ad altri servizi di welfare.

La "vita a punti" dei cinesi sembra così indicare il rischio di un nuovo totali- tarismo digitale, fondato sull'uso della

tecnologia per un controllo ubiquitario sul cittadino e su un vero e proprio capitalismo della sorveglianza.

La potenza del *machine learning* ha raggiunto livelli tali da farne temere l'uso spregiudicato a fini militari, in un contesto in cui sempre più le ostilità tra gli Stati si dispiegano nella realtà cibernetica.

I microchip cognitivi, applicati al comparto della Difesa, potrebbero mutare radicalmente, nell'incertezza del diritto internazionale, il futuro campo di battaglia, con la disponibilità di sistemi mobili robotizzati in grado di emulare la percezione e i processi decisionali dell'uomo.

Per altro verso, vengono progettati algoritmi per valutare tanto l'idoneità allo sviluppo dell'embrione da impiantare in utero, quanto la prognosi di sopravvivenza dei pazienti ricoverati.

La vita e la morte – i temi ultimi su cui ancora residuava mistero – divengono, così, oggetto anch'esse di valutazioni predittive affidate ad algoritmi che, se non esenti da pregiudizi (di genere, etnia, ceto) rischiano di replicare, in progressione geometrica, le discriminazioni da cui avevano promesso di liberarci.

Le esperienze di questi ultimi anni rendono sempre più urgente affrontare il tema della democrazia nella società digitale e gli effetti distorsivi dello slittamento, della profilazione e del *nudging*, dal piano commerciale a quello politico.

Significativa, in tal senso, la vicenda **Facebook-Cambridge Analytic**a, og- getto di un nostro provvedimento inibitorio ed alla base della recente norma dell'Unione, che sanziona l'uso illecito di dati personali per condizionare i risultati elettorali.

La prospettiva è aggravata dalla concentrazione di tali informazioni (e del conseguente potere di condizionamento) in

capo a poche imprese, capaci così di spiegare effetti determinanti su questioni di rilevanza pubblica primaria.

Si destrutturano, così, presidi democratici essenziali, quali quelli volti a garantire la libera formazione del consenso elettorale e la fisiologica competizione tra partiti.

Torna, invertito, lo schema gramsciano dell'egemonia sovrastrutturale, fondata oggi sulla capacità di orientare i comportamenti con la persuasione per- manente.

Sul piano sociale, ne risulta un effetto di polarizzazione estremistica dovuta alla prevalenza, accordata dall'algoritmo, a contenuti aggreganti, fondati sull'ostilità nei confronti del "nemico opportuno".

Nella società disintermediata, dalle esistenze – si è detto – "*in apparenza tra- sparenti, ma sempre più chiuse in universi impermeabili*", il 'pensiero lento', mediato dalla razionalità, risulta assai meno interessante.

Paradossalmente, quindi, il potenziale globalismo digitale rischia di promuovere, anziché capacità generativa, il riflesso autistico e antagonista delle "bolle" risultanti dai filtri e del pregiudizio conformativo, determinando un pericoloso ermetismo sociale.

Neutralità, statuto proprietario e, più in generale, sostenibilità etica e giuridica della tecnologia divengono, quindi, una questione democratica ineludibile.

Così come la sovranità si fondava, classicamente, sull'esclusività dell'uso legit- timo della forza, oggi si basa sul dominio della potenza di calcolo, che non può quindi sottrarsi a una progettualità etica, politica e anche giuridica: non può, in altri termini, restare avulsa dalla forma democratica.

È questo l'obiettivo dell'Europa che, non solo con il codice

etico per l’intelli- genza artificiale ma soprattutto con i principi fondativi della disciplina di protezione dati, intende coniugare innovazione e dignità.

Determinante, in questo senso, il principio di trasparenza algoritmica e il diritto di contestare la decisione assunta in via automatizzata, consentendo anche l’intervento umano per sottrarre le decisioni sulle persone al totale determinismo delle macchine. Che, se da un lato possono ridurre il rischio di errori e di un uso scorretto della discrezionalità, dall’altro non possono sostituire l’attività valutativa dell’uomo, nella sua complessità, assicurando quelle garanzie di partecipazione, tra- sparenza e accesso, in cui si esprime la democrazia.

Del resto, se in questo campo l’Europa potrà assumere un ruolo trainante sarà non tanto e non solo per le risorse stanziate, quanto piuttosto per la leadership culturale che può promuovere, mettendo la tecnica al servizio dell’uomo, secondo il principio di responsabilità.

Questo è il contesto in cui la protezione dati ha visto mutare profondamente il proprio orizzonte di senso, sino a divenire essenziale presidio di libertà e democrazia nella complessità della società digitale.

E di fronte all’incessante progresso di una tecnologia che sembra aver smarrito il valore del limite, questa disciplina rappresenta un efficace strumento di tutela non solo dell’identità ma anche della dignità dell’uomo rispetto al potere della tecnica, per impedire la riduzione della persona a cosa, la monetizzazione della libertà: un fattore di riequilibrio delle asimmetrie che caratterizzano i rapporti tra i cittadini e i detentori del potere pubblico e privato.

Il diritto alla protezione dei dati personali viene sempre più invocato di fronte alle innumerevoli “servitù volontarie” cui rischiamo di consegnare noi stessi, in cambio di utilità e

servizi che paghiamo al prezzo di porzioni piccole o grandi della nostra libertà. Emerge così un nuovo sottoproletariato del digitale, un "Quinto Stato" formato da quanti siano disposti a cedere, con i propri dati, la libertà, in cambio dei servizi offerti in rete solo apparentemente 'a prezzo zero'.

Si muove in questa ambiguità la proposta di attribuire un "dividendo dei dati" agli utenti della rete, per consentire loro di beneficiare almeno in parte della ricchezza prodotta, con i propri dati, dai big tech. E, pur mirando a riequilibrare rapporti – quali quelli tra utenti e titolari delle piattaforme – caratterizzati da un'incolmabile asimmetria, anche questa proposta non si emancipa dall'idea della monetizzazione dei dati personali, che rappresenta oggi un tema ineludibile per le democrazie.

Non più la merce ma il dato incorpora, infatti, una relazione tra persone e assume il ruolo tradizionalmente svolto da capitale e lavoro, nella sua duplice veste, tuttavia, di risorsa economica e di oggetto di un diritto fondamentale.

Di qui anche la funzione proconcorrenziale della privacy: si pensi al diritto alla portabilità che, soprattutto se accompagnato dall'interoperabilità dei sistemi, potrebbe contrastare i fenomeni anticompetitivi del *lock-in*.

Si pensi anche alla possibile qualificazione, come pratiche commerciali scor- rette, delle informative reticenti o, come abuso di posizione dominante, di illecite concentrazioni di *data set* anche di terze parti, secondo dinamiche emerse, ad esempio, nel provvedimento sul caso **Facebook-Whatsapp.**

Gli obblighi di correttezza e trasparenza del trattamento, imposti dalla disciplina di protezione dati, possono in questo senso rappresentare una risposta determinante ai principali fallimenti del mercato digitale, superando lo schermo della territorialità, grazie alla prevista applicazione del

Regolamento a chiunque offra beni, servizi o monitori il comportamento di quanti si trovino in Europa.

In questo senso, la protezione dati può rappresentare un requisito di tutela del consumatore e "***antitrust by design***" in quanto consente il governo dell'elemento fondativo dell' "economia del prezzo-zero": il dato personale.

Regolarne le condizioni di utilizzo, l'ambito di circolazione, le garanzie per l'identità che riflette, significa dunque armonizzare economia e persona, tecnologia e umanità, sicurezza e libertà.

Di qui anche la curvatura pubblicistica di questa disciplina: presidio di dignità del singolo ma anche presupposto di correttezza ed equità dell'economia "dei *like*", strumento di governo del mercato in funzione di tutela della persona.

Non sarebbe democraticamente sostenibile un regime in cui i grandi gestori delle piattaforme tecnologiche, attraverso protocolli informatici o condizioni generali di contratto, stabiliscano il codice normativo su cui fondare diritti e doveri nella dimensione digitale: contesto in cui più di ogni altro si dispiega la nostra esistenza. Da questa consapevolezza nasce il nuovo quadro giuridico, attraverso il quale l'Europa può ritrovare un ruolo di protagonista nello scenario globale, altrimenti egemonizzato dal nuovo bipolarismo sino-americano.

Con il passaggio a una disciplina di unificazione, la norma interpreta questo disegno sovranazionale e l'aspirazione universalistica al riconoscimento della protezione dati in una dimensione che supera i limiti imposti dal principio di territorialità.

Muta la stessa natura delle nostre Autorità, proiettate, ancor più nettamente rispetto al passato, in ambito europeo, ove grazie alle procedure di cooperazione e coerenza potranno rivolgersi davvero, con una voce sola, a interlocutori, come

le grandi piattaforme, attratte in altri e ben diversi ordinamenti. In questa prospettiva, sarà sempre più determinante l'azione di *enforcement,* per verificare che il principio di responsabilizzazione sia interpretato davvero nel segno dell'incremento delle garanzie.

Sul piano interno, il rango del Regolamento rafforza la centralità della disci- plina europea e l'efficacia della tutela multilivello dei diritti, delineando con le sue norme un limite per lo stesso legislatore nazionale.

Il parere obbligatorio del Garante sulla normativa primaria si è dimostrato, in questo primo anno di applicazione, un passaggio essenziale per delineare il miglior

equilibrio possibile tra la protezione dati e gli altri diritti e interessi di rilevanza costituzionale, nel rispetto del canone di proporzionalità, valorizzato di recente dalla stessa Consulta in relazione alla trasparenza.

Il dialogo tra Garante e legislatore ha spesso consentito apprezzabili migliora- menti dei testi, come nel caso del reddito di cittadinanza.

Maggiori resistenze si sono invece riscontrate, ad esempio, rispetto all'intro- duzione generalizzata dei controlli biometrici per i dipendenti pubblici.

È auspicabile che la sottovalutazione dei principi di proporzionalità e mini- mizzazione dei dati, riscontrata rispetto a tali provvedimenti, lasci spazio in futuro a un supplemento di riflessione, sottraendo temi così rilevanti all'enfasi della politica di parte e al conseguente rischio di norme meramente simboliche.

Uno degli eventi più significativi del contesto in cui si è svolto il mandato di questo Collegio è stato il Datagate, che ha avuto, anche in Europa, profonde implicazioni sul rapporto tra libertà e sicurezza, protezione dati e prevenzione.

La presa di coscienza collettiva che ne è derivata ha indotto, dapprima e con più forza nelle Corti europee, la revisione della disciplina delle misure limitative della libertà per fini di sicurezza, nel segno del canone di proporzionalità.

La giurisprudenza della Corte di giustizia sulla *data retention*, giunta sino all'annullamento di un atto normativo europeo, ha in questo senso contribuito non soltanto alla generale invalidazione degli strumenti di sorveglianza massiva, ma anche al consolidamento della dimensione 'costituzionale' della protezione dati, quale parametro valutativo delle politiche pubbliche, tanto dell'Unione quanto degli Stati membri. Sotto il profilo della *data retention* il legislatore italiano, nonostante i nostri reiterati richiami, non sembra aver colto sino in fondo le implicazioni di questi principi. La norma – senza eguali in Europa – che consente la conservazione generalizzata e indifferenziata, per sei anni, dei dati di traffico telefonico e telematico, costituisce una miope sfida al principio di proporzionalità ed espone il nostro Paese al rischio di censura in sede di controllo giurisdizionale di legittimità.

Tuttavia in altri campi si sono registrate innovazioni di rilievo.

Anzitutto, sul fronte dell'attività di prevenzione, proprio all'indomani del Datagate abbiamo promosso un rilevante rafforzamento del ruolo di controllo attribuito al Garante dal Codice.

Esso si è espresso attraverso nuove forme di esercizio del potere di vigilanza, disciplinate con il protocollo d'intenti siglato con il **Dis** nel novembre 2013 e due mesi fa ulteriormente potenziato, ma anche mediante una significativa attività consultiva che ha consentito di modulare la disciplina di settore nel segno dell'equilibrio tra prevenzione e riservatezza.

In ordine all’attività giudiziaria e, in particolare, allo strumento delle intercettazioni, sin dal 2013 abbiamo promosso l’adozione di alcune garanzie essenziali, omogenee per tutti gli uffici giudiziari, per impedire, in fase d’indagini, fughe di notizie pregiudizievoli sia di queste che della riservatezza individuale.

Dopo un’iniziale sottovalutazione del problema, si è registrato un adeguamento sostanzialmente uniforme agli standard richiesti, con beneficio non soltanto per i cittadini ma anche per la stessa attività investigativa.

Il Garante ha anche più volte, in questi anni, sollecitato Governo e Parlamento all’adozione di modifiche legislative volte a evitare il fenomeno del giornalismo di trascrizione, che si alimenta della produzione in giudizio di conversazioni irrilevanti ai fini investigativi, ma spesso gravemente lesive della riservatezza delle parti e dei terzi, coinvolti nelle indagini.

Alle iniziative assunte autonomamente da alcune Procure e poi promosse dal CSM in questa direzione, ha fatto seguito una riforma che – almeno sotto

questo profilo – tentava di limitare la trascrizione di contenuti irrilevanti, bilanciando (in maniera forse perfettibile) esigenze probatorie, diritto di difesa e privacy.

La sospensione dell’efficacia della riforma lascia sostanzialmente invariato, in tutte le sue criticità, il quadro normativo e la disomogeneità nelle garanzie derivante dalle diverse prassi adottate da ciascuna Procura, con un fenomeno di federalismo giudiziario che in tema di libertà suscita inevitabilmente preoccupazioni.

In assenza di riforme effettive, mai come in quest’ambito occorre un impe- gno comune.

Giustizia e informazione si caratterizzano principalmente per la loro indipendenza e, quindi, per la responsabilità nell'esercizio delle rispettive funzioni.

Responsabilità tanto più necessaria rispetto al potenziale distorsivo del pro- cesso mediatico, in cui logica dell'audience e populismo penale rischiano di ren- dere la presunzione di colpevolezza il vero criterio di giudizio.

Per altro verso, il ricorso ai **trojan** a fini intercettativi – la cui disciplina non ha introdotto molte delle garanzie da noi suggerite per impedire possibili violazioni – si è rivelato estremamente pericoloso. Soprattutto nel caso di utilizzo di captatori connessi ad app e quindi posti su piattaforme accessibili a tutti, suscettibili di degenerare, anche solo per errori gestionali, in strumenti di sorveglianza massiva. Violazioni simili a quelle recentemente verificatesi vanno impedite, non potendosi tollerare errori in un campo così sensibile, perché incrocia la potestà investigativa e il potere, non meno forte, della tecnologia.

Alcune innovazioni positive si sono invece riscontrate rispetto alla disciplina della gestione di dati personali per fini di polizia, che a seguito delle modifiche legislative del 2015 si è articolata in una più compiuta ricognizione dei trattamenti e dei principi del Codice applicabili in materia, conferendo così maggiore certezza e organicità al quadro giuridico di riferimento.

In sede di recepimento della **direttiva (UE) 2016/680**, si sono poi introdotte alcune importanti garanzie ulteriori, tanto in ordine ai limiti del potere di tratta- mento attribuito agli organi inquirenti, quanto in ordine ai diritti riconosciuti all'interessato.

È significativa, ad esempio, la previsione del diritto della persona (a prescindere dalla posizione processuale, includendovi anche il terzo estraneo alle indagini) di

richiedere, con una procedura particolarmente agile, la cancellazione o rettifica dei propri dati illegittimamente trattati in ambito giudiziario penale. Norma, questa, che potrebbe risultare particolarmente utile anche rispetto alle conversazioni intercettate.

Le tutele introdotte in sede di recepimento della direttiva si sono rivelate par- ticolarmente preziose nella valutazione della legittimità dei nuovi sistemi d'indagine fondati, soprattutto, su *web scraping* e *social media intelligence*, ovvero sul "rastrella- mento" delle fonti aperte per la raccolta di elementi utili in chiave investigativa.

Cardine di queste strategie deve essere un uso accorto della tecnologia, che non può certo offrire un vantaggio competitivo al reo rispetto agli inquirenti, solo per la difficoltà del diritto di stare al passo dell'evoluzione tecnologica. Ma che deve rispettare le libertà individuali, evitando gli eccessi deterministici della polizia predittiva, non potendo – in uno Stato di diritto – la ragion di Stato annullare le garanzie.

In ordine alla tutela dei dati personali dei minori, si è registrata dal punto di vista normativo una maggiore attenzione, espressa anche dal contributo richiesto al Garante e spesso recepito nell'ambito del procedimento legislativo.

Significativa, in tal senso, la legge sul cyberbullismo, che ha valorizzato l'esigenza di tutela in forma specifica dell'immagine e dell'identità del minore, attribuendo all'Autorità il compito di ordinare la rimozione di contenuti lesivi in caso di inerzia o rifiuto illegittimo del gestore, nei tempi celeri richiesti dalla realtà della rete.

Un equilibrio condivisibile tra tutela del minore, riservatezza e diritti dei lavoratori si era poi raggiunto, anche seguendo le nostre indicazioni, in relazione al tema della videosorveglianza negli asili per prevenire gli abusi e consentirne una più efficace ricostruzione probatoria.

La seconda lettura ha, tuttavia, alterato profondamente quest'equilibrio, introducendo misure – nella loro astratta rigidità – di dubbia compatibilità con il principio di proporzionalità.

Sul versante applicativo, invece, abbiamo avuto modo di affermare come – soprattutto ove sia in gioco la riservatezza del minore – il carattere "chiuso" del profilo di un social network non possa legittimare l'inapplicabilità delle norme di protezione dati, in ragione dell'agevole elusione dei sistemi di "chiusura" degli account e dell'intrinseca diffusività della pubblicazione in rete.

Caratteristica, questa, che deve indurre alla massima cautela nell'affidare al web i propri frammenti di vita, soprattutto se intima, di cui chiunque può appropriarsi quale strumento d'intimidazione o più in generale di coartazione della libertà, come purtroppo insegnano drammatici casi di cronaca.

Importante è stata l'evoluzione che ha caratterizzato il diritto all'oblio, riconosciuto dalla Corte di giustizia nel 2014 ma già da tempo tutelato dal Garante nella forma della deindicizzazione e valorizzato dagli istituti complementari della rettifica e dell'aggiornamento dei dati non più rispondenti alla realtà attuale.

La rettifica è stata peraltro da noi estesa allo "*snippet*" ed ha inciso anche sulla funzione di completamento automatico dei motori di ricerca, con la prescrizione della dis-associazione tra il nome dell interessato e termini pregiudizievoli, tali da ingenerare la convinzione di un suo coinvolgimento in attività illecite.

A seguito della sentenza **Costeja**, abbiamo delineato una specifica proce- dura per la tutela dell'identità nel suo progressivo costruirsi e per non cristallizzare, schiacciandola, la complessità di una biografia su un momento superato, quando non addirittura fuorviante: troppa memoria,

si è detto, a volte uccide la storia.

Sul terreno della cronaca giudiziaria, attraverso la deindicizzazione si sono garantite anche – ad esempio nei casi di concessione del beneficio della non menzione della condanna nel casellario – le esigenze di reinserimento sociale del soggetto, altrimenti pregiudicato dall'essere eternamente marchiato come reo.

E la stessa giurisprudenza ha confermato come, rispetto a notizie inesatte, le tutele accordate dalla disciplina di protezione dati possano garantire, ad un tempo, la correttezza dell'informazione.

Quest'ultimo parametro, unitamente a quello dell'essenzialità, abbiamo più volte dovuto invocare, a fronte della diffusione di un eccesso di dettagli inerenti la vita privata, anche sessuale, di soggetti, persino minorenni, coinvolti in indagini giudiziarie, anche in qualità di persone offese: con il rischio di un accanimento informativo non utile ai cittadini e lesivo della dignità degli interessati, persino indulgendo al sensazionalismo o confondendo il pubblico interesse con ciò che è di interesse del pubblico.

È stato anche necessario ricordare, rispetto a un episodio di *revenge porn* in danno di un'esponente politica, il dovere del giornalista di astenersi dal diffondere dati espressivi della sfera intima individuale, privi di alcun rilievo sul ruolo e sulla vita pubblica dell'interessata.

Rispetto ad alcuni eccessi riscontrati in una nota trasmissione radiofonica, abbiamo peraltro escluso la possibilità di ricorrere ad artifici o raggiri, per raccogliere notizie acquisibili con gli strumenti propri dell'inchiesta giornalistica e di legittimare qualunque raccolta, anche illecita, di dati, in nome del solo interesse pubblico della notizia.

Non vi sarebbe, altrimenti, più alcun limite nella correttezza

dell’acquisizione delle notizie e qualsiasi metodo di raccolta verrebbe giustificato in ragione del fine da perseguire.

La rilevanza assunta dalle regole deontologiche in ambito giornalistico ha indotto il legislatore a confermarne la vigenza anche nel nuovo quadro giuridico, raf- forzandola peraltro con la previsione della sanzione amministrativa per i casi di violazione.

Ma al di là e prima della responsabilità in termini sanzionatori, è necessario che il giornalismo sia oggi all’altezza di un compito ben più oneroso e nobile del passato: perché lo straordinario potere di cui dispone, accresciuto dalla rete, richiede un dovere di lealtà e correttezza ancora maggiore.

La digitalizzazione dell’attività amministrativa è una componente essenziale della competitività nazionale, che va realizzata nel rispetto dei diritti dei cittadini.

In questa chiave vanno letti i nostri numerosi interventi, volti a rendere il pro- cesso d’informatizzazione – prezioso per lo sviluppo del Paese – pienamente compatibile con i principi di proporzionalità e minimizzazione, tali da circoscrivere al necessario l’espansione del patrimonio informativo pubblico, così da rendere, al con- tempo, esso stesso più sicuro e più efficiente l’azione amministrativa.

A fronte dell’imponente moltiplicazione e interconnessione delle banche dati pubbliche, abbiamo costantemente indicato misure per la loro razionalizzazione e messa in sicurezza.

Si pensi alle indicazioni fornite rispetto al trattamento di dati personali su larga scala che era stato previsto, dall’**Agenzia delle entrate**, per la fatturazione elettronica, con riguardo potenzialmente a ogni aspetto della vita quotidiana dell’intera popolazione, ritenuto sproporzionato rispetto al pur legittimo obiettivo perseguito.

Nella consapevolezza della necessità di responsabilizzare i soggetti a vario titolo coinvolti nella complessa catena della sicurezza dei sistemi e delle reti, abbiamo svolto un'importante attività ispettiva rispetto ai nodi di interscambio internet (ixp), gestiti da privati non sempre in modo adeguato e dalla cui sicurezza dipendono, tra l'altro, la sicurezza nazionale, l'efficacia delle indagini, l'incolumità dei singoli.

La parcellizzazione dei centri di responsabilità comporta, del resto, rischi cui è necessario ovviare centralizzando le competenze all'interno di una strategia unitaria, nazionale ed europea insieme, per proteggere non tanto e non solo il punto terminale ma l'"ecosistema digitale" nel suo complesso.

Altrimenti avremmo soltanto monadi protette, immerse però in un reticolo di vulnerabilità, peraltro sempre crescenti. E questo, tanto più a fronte del ricorso sempre più imponente al cloud e dello sviluppo del **5G,** con cui la superficie di attacco cresce in progressione geometrica, perché i rischi si estendono a tutti i nodi della rete.

Il 2018 è stato definito, dal **Clusit**, l'anno peggiore relativamente alla sicurezza cibernetica, così costantemente esposta a minacce da configurare una sorta di cyber-guerriglia permanente.

E se nel settore pubblico in generale gli attacchi sono cresciuti nell'ultimo anno del 41%, in ambito sanitario l'incremento ha toccato l'acme del 99% rispetto all'anno precedente, con effetti tanto più gravi che in altri settori perché l'alterazione dei dati sanitari può determinare – come abbiamo sottolineato anche rispetto al fascicolo sanitario elettronico – errori diagnostici o terapeutici.

La carente sicurezza dei dati e dei sistemi che li ospitano può rappresentare, in altri termini, una causa di malasanità.

O, come nel caso di cui ci siamo occupati, degli embrioni

scambiati, la violazione delle regole essenziali di protezione dati può avere effetti deleteri nei processi medici, tanto più gravi ove quei processi incidano su aspetti qualificanti l'esistenza individuale: la nascita, la morte, la genitorialità.

Specularmente, la protezione dei dati è un fattore determinante di efficienza sanitaria, funzionale anche alla correttezza del processo analitico fondato su big data.

Dall'esattezza dei dati utilizzati nel processo algoritmico dipende, infatti, l'"intelligenza" delle loro scelte, che tanto più in ambito diagnostico non possono tollerare errori.

Innovazioni rilevanti hanno interessato la disciplina della trasparenza, con il compiuto superamento della segretezza quale forma di esercizio del potere e la mutazione del rapporto tra autorità e singolo: da autoritativo, burocratico e insindacabile a paritetico, partecipato e "controllabile"; della concezione dell'amministrazione, come servizio prima che potere; della stessa idea del cittadino, partecipe attivo della funzione di controllo democratico sull'attività pubblica.

Tuttavia, il carattere indifferenziato degli obblighi di pubblicità, unitamente all'introduzione degli accessi civico e generalizzato – che prescindono dall' interesse qualificato del richiedente – hanno reso tanto complessa, quanto necessaria, la definizione puntuale dei limiti posti alla trasparenza per esigenze di tutela della riservatezza. Attraverso le linee guida adottate dal Garante, l'intesa su quelle dell'**Anac** e i numerosissimi pareri resi in materia di accesso civico, abbiamo applicato in concreto il canone di proporzionalità, su cui si misura la natura davvero democratica di questa concezione dell'amministrazione "aperta".

L'irragionevolezza dell'estensione indifferenziata dei

medesimi, rilevanti obblighi di pubblicità a categorie di dipendenti pubblici del tutto eterogenee, da noi più volte rilevata, è stata del resto censurata anche dalla Corte costituzionale.

Essa ha peraltro sottolineato il rischio che l'eccesso informativo determini, con una singolare eterogenesi dei fini, opacità per confusione, ostacolando con la raccolta massiva di dati personali non tutti egualmente utili, la ricerca delle informazioni realmente rilevanti per consentire, invece, quel governo del potere visibile su cui si fonda la democrazia.

Alla crescita del patrimonio informativo pubblico si è affiancato, parallela- mente, un altrettanto rilevante aumento delle banche dati e dei sistemi di profilazione gestiti da privati.

Sono innumerevoli, infatti, le classificazioni e schedature cui ciascuno di noi è soggetto per il semplice fatto di essere o di essere stato parte di un rapporto commerciale, con la conseguente moltiplicazione esponenziale dei profili che ci riguardano.

Tanto più di fronte alla rapidissima diffusione di oggetti intelligenti – dagli elettrodomestici agli assistenti vocali fino agli *smart speaker* – che stanno entrando progressivamente nelle nostre case e i cui potenziali rischi per la riservatezza di abitudini e scelte ci sono spesso ignoti.

I nostri dati, così raccolti per i fini più vari, concorrono a ridefinire le nostre identità: quelle "transattive" derivanti dalla ricostruzione del profilo di consumatore di ciascuno e quelle "predittive" che anticipano comportamenti, scelte e persino responsabilità.

Sono, del resto, ricorrenti i tentativi – di cui ci siamo occupati – di immet- tere nel mercato servizi fondati su banche dati per la misurazione del *rating* reputazionale.

In gioco vi è, certamente, l'inadeguatezza di un algoritmo a svolgere valuta- zioni necessariamente discrezionali e complesse, quali quelle relative all'affidabilità professionale ed economica, con il rischio di errori e false attribuzioni.

Ma soprattutto vi è la sfida, culturale e antropologica, di non ridurre la com- plessità di una biografia al r*anking* attribuitole dall'algoritmo, sostituendo dunque i 'numeri agli uomini', per citare **Federico Caffè.**

Sempre più declinata al futuro nel cono d'ombra del passato, valutata per le sue propensioni desunte meccanicamente dai comportamenti pregressi, la persona finisce con il perdere il diritto al presente, schiacciata da un passato che si proietta sul futuro, assorbendo ogni altra dimensione.

All'idea della responsabilizzazione dei protagonisti del trattamento, su cui si fonda il Regolamento, si ispira poi la recente riforma della disciplina del telemar-

keting, volta a contrastare tale fenomeno, in particolare, con la prevista responsabilità solidale di titolare e responsabile, l'ambiguità dei cui ruoli ha rappresentato sinora una delle maggiori criticità.

L'efficacia di tale riforma è stata, tuttavia, depotenziata dal ritardo nell'ado- zione della normativa di attuazione.

Rilevante è stata anche la riforma dello Statuto dei lavoratori che, quasi cin- quant'anni fa, aveva introdotto nel nostro ordinamento le prime norme a tutela della riservatezza, all'interno di un rapporto tipicamente asimmetrico quale quello di lavoro.

Tentando di adeguare norme pensate per l'organizzazione fordista del lavoro alla realtà dei sistemi satellitari e della biometria, il **Jobs Act** ha apportato significative innovazioni.

Con diversi provvedimenti, abbiamo cercato di offrirne puntuali interpreta- zioni alla luce dei principi di necessità e proporzionalità, per impedire l'abuso del potere datoriale di controllo.

La tutela accordata dalla disciplina di protezione dati, in quanto ancorata non alla forma contrattuale ma all'elemento – il dato personale, appunto – su cui si basano i controlli datoriali e la stessa gestione algoritmica del rapporto di lavoro (si pensi ai riders), diviene così un prezioso strumento di garanzia.

Significativo, in questo senso, un provvedimento nel quale abbiamo dichiarato illecita la prassi, adottata da una cooperativa, di affiggere, nella bacheca aziendale, non solo contestazioni disciplinari ma anche cartelli conte- nenti la valutazione professionale di ciascun dipendente, espressa mediante *emoticon.*

Una simile forma di gogna è, infatti, incompatibile con la dignità e il diritto alla riservatezza dei lavoratori.

La disciplina di protezione dati rappresenta, del resto, un presidio di tutela del lavoratore tanto più importante, quanto più le nuove tipologie di impiego sfuggano alle forme e quindi anche alle garanzie pensate per il rapporto di lavoro tradizionale, come nel caso dello *smart work.*

Il diritto alla privacy è uno di quei diritti inviolabili protetti anche in ambito endoassociativo e per la tutela del quale siamo intervenuti, più volte, a valutare – pur nel rispetto dell'autonomia statutaria – la correttezza dei trattamenti svolti, anche riguardo all'associazionismo politico.

Oltre a prescrivere misure volte a garantire il corretto trattamento dei dati (peraltro sensibili) di iscritti ed esterni, soprattutto in relazione alla propaganda elettorale, abbiamo recentemente avuto modo di approfondire le

implicazioni – illustrate anche dal Consiglio d'Europa – che la digitalizzazione degli strumenti di partecipazione politica ha sulle libertà individuali.

Da un lato, infatti, rientra nell'autonomia dell'associazione la scelta del voto elettronico quale metodo di espressione, da parte degli iscritti, della propria volontà.

Dall'altro lato, tale scelta non esime l'associazione dal rispetto dei principi essenziali di protezione dati, volti a garantire anche la libera espressione, da parte dell'iscritto, del proprio orientamento politico, al riparo da rischi di violazione, profilazione, manipolazione.

Tali garanzie sono tanto più necessarie quanto più le scelte espresse in ambito associativo si traducano poi, più o meno direttamente, in posizioni assunte dal partito o dai suoi esponenti, nelle sedi istituzionali.

Si traccia infatti, così, un *continuum* tra base, partito e luoghi della rappresentanza che, a maggior ragione, deve rispettare anzitutto le libertà fondamentali.

La centralità della persona è stata la "cifra" caratterizzante il mandato che a breve concluderemo, nel tentativo quotidiano di riequilibrare i rapporti tra libertà dell'uomo e determinismo della tecnica, promuovendo quella fiducia nel digitale, indispensabile per il suo sviluppo e per la sua stessa sostenibilità.

Nella progressiva affermazione universale del diritto alla protezione dati e nella sua tenuta sociale, nella sua capacità di divenire cioè forma e regola dell'agire individuale e collettivo, si giocherà una delle partite più importanti della democrazia e dello stesso ordinamento internazionale, per governare l'innovazione nel rispetto dei diritti e della dignità.

A quest'obiettivo nessuno può sentirsi estraneo: perché

involge il senso stesso del nostro essere persona e la natura della società in cui viviamo.

Alla scrittura di questo fondamentale diritto di libertà dobbiamo dunque tutti partecipare, per scommettere ancora una volta tanto sulla persona quanto sul progresso.

Nel presentare la nostra prima relazione, affermavamo come, a partire dall'impostazione personalista su cui si fonda la Costituzione, sia possibile ambire a ricomporre le crescenti fratture sociali, attorno a una nuova idea di cittadinanza.

Questa è stata la nostra bussola nel percorso di questi anni, vissuti sempre con la consapevolezza del limite e, insieme, con l'ambizione di far crescere nel nostro Paese la cultura di uno straordinario diritto di libertà.

Abbiamo cercato di assolvere con tutto il nostro impegno, la nostra passione e la nostra lealtà il mandato affidatoci dal Parlamento, nel rispetto della Costituzione e con indipendenza di giudizio.

Consentitemi di ringraziare le Colleghe e il Segretario generale che hanno condiviso questa esperienza in un clima di unità e armonia, nonché i dipendenti del Garante per il loro prezioso lavoro.

Ringrazio tutte le Autorità che mi hanno onorato del loro sostegno e della loro fiducia, nonché la **Guardia di Finanza** per l'importante, consolidata collaborazione.

Al prossimo Collegio consegniamo un'Autorità potenziata sotto il profilo non solo delle funzioni, ma anche delle risorse umane e finanziarie.

La sfida che la attende, nel prossimo futuro, attiene all'effettività di questo diritto, che le norme hanno delineato nella massima compiutezza.

Ma la dimensione più autentica della protezione dati vive

nella realizzazione quotidiana, per la quale è indispensabile il contributo di ciascuno.

Se il diritto è “un’opera collettiva”, questo fondamentale diritto di libertà – che sempre più governerà il futuro nella sua complessità – lo è ancora di più.

Per approfondire:

Cambridge Analytica, GDPR, eFattura, Rousseau e reddito di cittadinanza. L’attività del Garante Privacy nel 2018

https://www.key4biz.it/relazione-annuale-garante-privacy-il-discorso-integrale-di-antonello-soro/256906/

5G Conference Warns on Security as Huawei Controversy Rages

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/TJYdJyrskA8/5g-conference-warns-security-huawei-controversy-rages

---

Come cambiano (e perché

cambiano) Facebook e Instagram

Rubrica settimanale **SosTech**, frutto della collaborazione tra **Key4biz** e **SosTariffe**. Per consultare gli articoli precedenti, **clicca qui**.
«**Il futuro è privato**»: parole che potrebbero sembrare una sottile presa in giro (e forse lo sono) quando vengono pronunciate dall'uomo a cui, a torto o ragione, pensiamo subito tutti quando si parla di "violazione della privacy". Ma **Mark Zuckerberg** è serissimo quando, dal palco della conferenza per gli sviluppatori F8, indica la direzione che **Facebook** seguirà per i prossimi anni, con cambiamenti che si preannunciano radicali sia dal punto di vista della grafica e dell'interfaccia che di quello che sta sotto il cofano.

Sottile povocazione, perché meno di dieci anni fa, nel 2010 – un'era geologica nel mondo digitale – lo stesso CEO di Facebook, intervistato dal fondatore di **TechCrunch Michael Arrington**, dichiarava con la massima disinvoltura: «*La gente ora si sente molto più a suo agio non solo nel condividere più informazioni e di diverso tipo, ma in modo più aperto e con ancora più persone. Le norme sociali sono un qualcosa che evolve nel tempo*». E se è vero che questi ultimi anni rappresentano, per molti versi, un'esitazione – quando non una vera e propria marcia indietro – rispetto a molte cose che si davano per scontate, allora non ci si deve stupire più di tanto quando Zuck discetta di **messaggi criptati** e di social «*non solo come piazza, ma come salotto digitale*».

Fonte: Statista

Sempre più privati

In questi dieci anni sono successe parecchie cose – dall'acquisizione di **Instagram**, oggi il social network d'elezione per i giovanissimi, agli scandali riguardanti l'uso decisamente disinvolto dei dati degli utenti, vedasi **Cambridge Analytica**. Facebook oggi non è più consultato dal computer, ma, con la complicità dei prezzi sempre più bassi delle connessioni via **Internet mobile** (su **SosTariffe.it** potete confrontare ogni giorno le più convenienti), dagli smartphone, e proprio la fruizione mobile ha ispirato le interfacce dei social più apprezzati dai consumatori del futuro (non solo Instagram ma anche **Snapchat** e **Tik Tok**).

Il **ripiegamento sul privato**, in altre parole – e questa forse è un'attenuante per Zuckerberg – non riguarda soltanto la nostra esperienza digitale, ma è un fenomeno più ad ampio raggio, che tocca tanti aspetti della nostra vita. I social sono solo un riflesso di questa mutazione; oggi preferiamo guardare e commentare le **Storie** della propria ristretta cerchia di amici (più qualche superstar e influencer che ci tiene a dirci "sono come voi") rispetto a quando pensavamo di dire la nostra al mondo con i **blog** (non a caso l'esempio utilizzato dallo stesso Zuckerberg nel 2010).

Dalla piazza al salotto

Se il mondo, almeno parzialmente, **si chiude**, anche Facebook lo asseconda. Ma come? Il **cambiamento grafico e di interfaccia** è sicuramente il più radicale dal 2011, quando per la prima volta venne introdotta la timeline. «*Non è nemmeno blu*», ha scherzato – ma solo fino a un certo punto – il giovanissimo CEO durante il suo intervento, riferendosi a un look che pare

aver rinunciato in massima parte al suo colore iconico in favore di **un bianco** più leggibile, più neutro, e soprattutto "diverso": come dire, **Facebook non è più quello di prima**. Cambierà l'icona ("più vivace e moderna") e la navigazione sarà facilitata, grazie a un design più semplice e immediato. In più, codice del sito e dell'app verrà riscritto da zero per renderli più veloci.

Ma i cambiamenti più radicali riguarderanno i **gruppi**, la *feature* che più di ogni altra tiene a galla la piattaforma: saranno più accessibili e immediati per chi è alla ricerca di contesti più intimi, e allo stesso tempo **più controllati** per evitare abusi e comunità che incitano alla violenza.

La scialuppa di salvataggio? Instagram

Ma le novità di Zuckerberg non riguardano solo Facebook. Non si butta via niente, e allora perché rinunciare a tante funzioni meticolosamente introdotte nel corso degli anni e inutilizzate perché, diciamocelo, ormai sono sempre meno gli under 40 che accedono a Facebook? Sempre in base ai cambiamenti annunciati alla F8, **la "facebookizzazione" di Instagram** sembra ormai inevitabile. **Adam Mosseri**, a capo del più popolare social network del momento, ha mostrato il "**Create mode**", ovvero un nuovo formato delle Storie dedicato a testi, quiz e sondaggi non legati direttamente a dei contenuti fotografici o video, un po' come i "color block status" introdotti da Facebook nel 2017. Una caratteristica che tra l'altro per la prima volta spezza ufficialmente il legame tra **fruizione visiva e non testuale** che ha portato al successo di Instagram, ma che ormai gli utenti stanno abbandonando in favore di Storie dove si scrivono righe su righe di testo.

Fonte: Statista

Il rischio dell’effetto televendita

Dietro a tutto, rimane il problema della **monetizzazione**. Il fatturato dei social arriva dalla pubblicità, ma anche dalla gestione dei dati degli utenti secondo modelli che oggi non sono più sostenibili, alla luce degli scandali e delle manipolazioni. Bisogna quindi puntare altrove, e se le novità per Instagram sono anche “no profit” (come i “**Donation stickers**”, che permetteranno di raccogliere fondi per cause benefiche con le Storie) la parte più ghiotta per **Menlo Park** riguarda ancora la possibilità di acquistare i prodotti pubblicizzati dall’influencer di turno direttamente dall’app: è stata infatti annunciata la possibilità di aggiungere degli speciali tag ai post che conducono direttamente al link per l’acquisto del prodotto; per evitare che tutto si riduca a un’immensa **televendita**, i portavoce di Instagram si sono affrettati a specificare che gli influencer non riceveranno una percentuale di quanto venduto grazie ai loro link. E nessuno si stupirebbe se anche i gruppi, in tempi più o meno brevi, arrivassero sulla piattaforma-sorella.

Insomma, Instagram è la perfetta scialuppa di salvataggio per il social network che fino a tre o quattro anni fa appariva una corazzata impossibile da fermare e che adesso invece è sempre più sul punto di affondare, a causa degli scandali e del cambiamento delle abitudini degli utenti, in particolare nell’ambitissima fascia **tra i 12 e i 34 anni**. Instagram fa soldi, è popolare, non genera (troppe) polemiche e quando qualcosa va storto si può ancora intervenire, ad esempio con ciò di cui si è molto parlato in queste settimane ma che ancora attende il suo debutto ufficiale, cioè la possibilità di **nascondere i like di un post**. L’obiettivo è far sì che i contenuti vengano apprezzati di per sé e non in base a quante altre persone in precedenza hanno messo un “cuore” (dinamica che è patita particolarmente dai teenager e che ha dato

origine a casi di vero e proprio “**bullismo digitale**” soprattutto negli Stati Uniti, ma anche da noi). Resta da vedere **se tutto questo basterà**.

Fonti:

https://www.key4biz.it/come-cambiano-e-perche-cambiano-facebook-e-instagram/256522/

Google unveils auto-delete for location, Web activity, and app usage data

Enlarge / Mountain View, Calif.—May 21, 2018: Exterior view of a Googleplex building, the corporate headquarters of Google and parent company Alphabet.
Getty Images | zphotos

reader comments

63 with 50 posters participating

Share this story

Google will soon let users automatically delete location history and other private data in rolling intervals of either three months or 18 months.

“Choose a time limit for how long you want your activity data to be saved—3- or 18-months—and any data older than that will be automatically deleted from your account on an ongoing

basis," Google announced yesterday. "These controls are coming first to Location History and Web & App Activity and will roll out in the coming weeks."

Google location history saves locations reported from mobile devices that are logged into your Google account, while saved Web and app activity includes "searches and other things you do on Google products and services, like Maps; your location, language, IP address, referrer, and whether you use a browser or an app; Ads you click, or things you buy on an advertiser's site; [and] Information on your device like recent apps or contact names you searched for."

You can already go into your Google activity control settings to completely turn off the features that save your location history and Web and app activity. But the new auto-delete option will provide a middle ground in which users who are concerned about the data storage can save activity data for a non-forever period of time without having to manually delete it once in a while.

Chrome browser history as well as "activity from sites, apps, and devices that use Google services" are currently listed as a subset of Web and app activity in Google's activity controls settings, and the saving of this data can be disabled. The new auto-delete function doesn't appear to cover Chrome history in a preview provided by Google, however. Note how Chrome history is listed separately at the end of this short video showing how you'll be able to enable the auto-delete functionality when it rolls out:

What's the advantage of saving the data at all? Google's announcement said that saving the data "can make Google products more useful for you—like recommending a restaurant that you might enjoy, or helping you pick up where you left off on a previous search."

But Google's disclosures about how it saves data history

haven’t always been accurate. Last year, the Associated Press found that “several Google apps and websites store user location even if users have turned off Location History.” In response, Google changed a help page that erroneously claimed, “With Location History off, the places you go are no longer stored.” The page now says, “Some location data may continue to be saved in other settings, like Web & App Activity, as part of your use of other services, like Search and Maps, even after you turn off Location History.”

Google has been facing scrutiny from Congress as lawmakers consider proposals for a new data privacy law.

“We work to keep your data private and secure, and we’ve heard your feedback that we need to provide simpler ways for you to manage or delete it,” Google said in its announcement yesterday.

No word on auto-deleting other data

Google seemed to indicate that the auto-delete function will come to other data when it said, “These controls are coming first to Location History and Web & App Activity.” But Google didn’t say whether or when its new auto-delete function will be available for any other specific categories of data, such as YouTube search and watch history, or voice recordings from Google Assistant requests. Like location history, Web history, and app activity, you can disable saving of this other data completely in your account settings.

Google says that “Device information“—another category that can be turned off completely but isn’t included in the new auto-delete function—includes “things like contact lists, calendars, alarms, apps, and music, and can help Google give you more accurate results and suggestions.”

In its privacy policy, Google says, “We use various technologies to collect and store information, including

cookies, pixel tags, local storage, such as browser web storage or application data caches, databases, and server logs.”

Deleting your data from your Google account should erase it from Google’s data centers, except when it’s stored in a way that doesn’t identify you.

“When you delete data, we follow a deletion policy to make sure that your data is safely and completely removed from our servers or retained only in anonymized form,” Google says. “Complete deletion of data from our servers… generally takes around two months from the time of deletion” and “often includes up to a month-long recovery period in case the data was removed unintentionally,” Google also says. Google also uses encrypted backup storage “to help recover from potential disasters” and says that “[d]ata can remain on these systems for up to six months.”

https://arstechnica.com/?p=1499235