WhatsAppening? Brevi note su origini, combattenti e futuro delle moderne guerre digitali

Emilio Girino
Avvocato in Milano – Managing Partner, Studio Ghidini, Girino & Associati – Docente CUOA Finance – già Membro dell'Arbitro Bancario Finanziario (Collegio di Milano e Collegio di Coordinamento)

Franco Estrangeros
Avvocato in Milano – Partner, Studio Ghidini, Girino & Associati – già Membro dell'Arbitro Bancario Finanziario (Collegio di Milano e Collegio di Coordinamento)

1. Alle origini del conflitto: per una realistica identificazione dei belligeranti

Quando, non più bambini e seduti composti sui banchi del liceo, qualche illuminato docente ci spiegò che le guerre non nascono da pretesti nazionalisti o da ribelli impeti, ma solo da bieche motivazioni pecuniarie, ebbene – riconosciamolo e riconosciamoci in quei momenti – nessuno di noi ci credeva o ci voleva credere. Nessun adolescente è pronto a credere che stragi e massacri si debbano a faccende di portafoglio invece che a credi libertari, magari non limpidi ma di certo non monetizzabili. Un mito presto sfatato nella giovinezza. Ogni guerra non ha un senso, nella testa di chi la sferra, che non sia un senso umanamente dispendioso: non tanto d'umanità (particolare considerato drammaticamente secondario) ma di denaro.

Le guerre odierne si battagliano per lo stesso fine ma, accanto ai conflitti tradizionali, s'affiancano lotte quasi invisibili e combattute con mezzi meno sanguinari ma non meno letali o, se si preferisce, diversamente letali, sotto il labaro di non meglio comprensibili libertà o, più precisamente, liberazioni (mai si è veramente capito da chi e da che cosa). Labaro da tessere con pazienza e grande scaltrezza manifatturiera e da agitarsi sullo smorto futuro

d'umanità condannate a un declino fatto di totale isolamento sociale, dunque soppressione di creatività e reattività umane, che per loro natura si cibano di socialità, sempre meno sociale e sempre più virtuale.
È questo inusuale *incipit* essenziale per affrontare un tema che, con minima preveggenza, riassume il senso della belligeranza attuale e futura in nome del benessere virtuale, della presunta purificazione esistenziale, della pace sociale, del mondo come posto migliore.
Nessuno potrebbe anche solo debolmente dubitare che la principale fonte di profitto sia oggi l'informazione. "*I showed you how the system works… the value of information!*" rinfaccia Gordon Gekko all'arrivista broker Buddy Fox nel *Wall Street* degli anni '80, quando il secondo, dopo essersi ben cibato dei criminali insegnamenti del primo, gli si rivolta contro, travolto da un improvviso impeto di legalità (complici un padre degno e infartato e la spinta di una Sec alle costole). Ma si parlava di *insider trading*, faccende per eletti inafferrabili o ingenui affaristi di borsa, roba da ricchi colletti bianchi.
Le vere informazioni che oggi rendono non sono notizie segrete trafugate e consumate da topi di *trading venues*, bensì notizie che miliardi di individui, dal più eccelso al più modesto, spontaneamente generano. Non già informazioni privilegiate per il mercato borsistico, ma informazioni su se stessi, quelle banalissime notizie su cosa uno fa, cosa mangia, cosa compra, cosa legge, cosa guarda, dove va in vacanza, dove e come si veste[1].
È su questo terreno d'umana e incosciente fragilità che i tessitori dei social network costruiscono le loro fortune, fabbricate con pixel ma profumatamente pagate. Non dagli utenti (almeno in apparenza) ma da chi li può raggiungere con réclame mirate su cui le reti sociali lucrano smisurati profitti[2].

[1] Ne abbiamo ampiamente trattato in Privacy e PCS: dal caso Facebook allo sgretolamento del concetto di gratuità del dato personale, in questa Rivista, 1-2020, p. 49, cui ci permettiamo di rinviare.

[2] Analoga meccanica è riprodotta, "in miniatura" e in forme meno aggressive, nell'universo del commercio elettronico proprietario. Tuttavia, per magnitudo e per funzionalità specifica, il metodo di raccolta e l'impiego dei dati hanno rispettivamente un tratto meno invasivo e uno spettro di diffusione del dato più ristretto per non dire inesistente. Il sito di vendita normalmente cerca di fidelizzare il cliente, la cui profilazione mira a spingere quest'ultimo ad effettuare ulteriori acquisti. In genere, il sito è geloso dei dati del proprio cliente e ben difficilmente ospiterà banner di concorrenti, al limite chiedendo un consenso alla diffusione del dato verso operatori terzi del gruppo di appartenenza. E la differenza ha una precisa ragion d'essere: si accede ad un sito per comprare merci o servizi di un dato produttore e le si paga, dunque non si usufruisce di un servizio gratuito né si offrono dati personali ulteriori e diversi dai propri estremi e dalla tipologia di acquisto effettuato. Completamente diversa – ed esattamente equiparabile a quella delle reti sociali – è l'attitudine appropriativa dei siti di commercio elettronico distributivo e pluri-marca, specie di grandi dimensioni, dove lo scopo è profilare il cliente per sottoporgli una pletora di prodotti anche completamente diversi, con un livello

Non è servita una precisa strategia, risultando sufficiente invece una rapida tattica, tanto semplice quanto straordinariamente efficiente, come il leggendario uovo colombiano: 1) illudere l'utenza della gratuita libertà di parola, espressione, (auto)esposizione; 2) consolidare quella libertà gravida di informazioni; 3) a dipendenza raggiunta, appropriarsi di quei dati per rivenderli a mercanti settorialmente interessati. Questo terzo stadio oggi è ormai abbondantemente completato e per le nuove reclute non sono neppure più necessarie le fasi di cattura, addestramento e assuefazione. La macchina gira da sé.

La susseguente, ovvia domanda è: chi sono i combattenti, dove e quali sono gli eserciti schierati in campo, quali le loro divise e le loro bandiere?

Nuovamente la globalizzazione digitale impone uno sforzo di revisione delle schematizzazioni belliche cui la storia ci ha abituati. Se è relativamente facile intuire il valore commerciale dei dati personali dell'utenza e dunque individuare i nuovi bottini, meno agevole è comprendere chi siano i veri contendenti.

Il paradigma storico vuole che una guerra scoppi fra nazioni o dentro le nazioni, fra realtà sovrane o politico-territoriali in entrambi i casi protese ad acquisire un potere di gestione, governativa ed economica, di un dato territorio e delle sue risorse industriali, tecnologiche, naturali o umane. Questo concetto può ancora, debolmente, valere per le cc.dd. guerre doganali, per l'imposizione di dazi aggressivi o ritorsivi, ma una guerra digitale non conosce confini e, per questa sola ragione, lo scontro nazionalistico o intestino si rivela un modello inadeguato.

Neppure lo scontro si consuma fra le reti sociali o, se ciò avviene, riguarda una minima parte del milieu. Il sistema è attualmente contrassegnato da una marcata impronta oligopolistica e gli oligopolisti hanno una duplice ragione per non veramente combattere fra di loro: da un lato, evitare la costituzione di un monopolio che ineluttabilmente porterebbe alla reazione delle autorità antitrust mondiali e al suo spezzettamento e, dall'altro lato, creare un fronte comune per conservare il dominio di mercato e ostacolarne l'ingresso ai *new comers* i quali, se comunque riusciranno a sfondare, per sopravvivere dovranno adeguarsi allo schema dei leader di mercato.

di estrazione di dati crescente ed esponenziale. Stesso fenomeno si registra, sia pur in scala più ridotta e con effetti decisamente minori per i cc.dd. "siti-schermo", siti cioè che "regalano" attività ludiche in cambio dell'assoggettamento forzato al ricevimento di pubblicità o banner di terzi della più disparata natura, i quali alimentano tali siti proprio pagando i dati dei clienti che utilizzano gratuitamente i servizi (come nel noto caso Planet49, su cui rinviamo al nostro Per un consenso (veramente) informato: la Corte di giustizia UE inizia l'inversione di rotta, in questa Rivista, 4-2020, 53). Per rapidità espositiva, il riferimento nel testo alle reti sociali deve intendersi esteso anche alle realtà equiparabili nel senso qui chiarito.

Nemmeno può dirsi che la guerra sia ingaggiata verso gli utenti che semmai ne sono le vittime o, più tecnicamente, le prede, insostituibili produttori di quella messe di dati che anima il conflitto.
La guerra allora fra chi è combattuta? Chi è l'avversario delle reti? Dobbiamo prendere atto di una realtà tanto singolare quanto sconvolgente: la lotta vede contrapposte le reti ai regolatori. I secondi, istituzionalmente votati a proteggere le masse da sé stesse, dalle loro inconsapevolezze e dalle loro narcotiche cedevolezze alle blandizie delle reti, diventano gli unici, veri antagonisti dei social. Più le maglie normative sul trattamento dei dati si stringono, più le reti tentano percorsi di fuga. Non diversamente, si dirà, da quanto accade in ogni ambito economico, quello fiscale per primo, dove ad ogni giro di vite corrisponde una controspinta eguale e contraria dell'apparato produttivo e contributivo. Tuttavia, mentre in questi casi sono interi sistemi o parti di sistemi a tentar di reagire, nella guerra fra regolatori e reti, lo scontro, pur dovendo teoricamente interessare la globalità degli individui, si consuma solo a questo livello superiore.
Sicché la guerra, in definitiva, si gioca essenzialmente su questo tavolo, dove all'un capo si collocano le reti e il loro incessante bisogno di continuare a non perdere la più ampia signoria possibile dei dati dell'utente e, all'altro capo, siede un regolatore sempre più vigile e dedito a contenere ogni degenerazione di tale signoria in uno sfrenato uso dei dati delle persone fisiche.
Del resto è questo il crescente problema immanente alla dialettica fra tecnologia e diritto: la volontà della prima d'imporsi sul secondo, in nome di un non meglio chiarito naturale privilegio evoluzionistico, e l'opposizione del secondo che giustamente non può permettere alla novità digitale di violare le regole del mondo reale.

2. WhatsAppening? Se una vicenda oscura diviene una profezia illuminante

Una sintomatica epifania di questo nuova tipologia di conflitto è la recente, obiettivamente esasperata e per taluni versi travisata *querelle* sulla modifica dei termini di servizio e dell'informativa privacy di WhatsApp.
Tutto accade all'inizio dello scorso gennaio, quando si sparge la voce che il più celebre e diffuso *instant messenger*, è in procinto di cambiare policy e di imporre all'utenza, pena l'inutilizzabilità del servizio, la concessione del diritto di trasmettere i dati dei clienti alla sua casa madre (Facebook). Il panico si diffonde, alimentato anche da autorevoli, o come tali ritenuti, *influencer* che invitano a lasciare WhatsApp per passare ad altri e più onesti sistemi di comunicazione istantanea (per primo Signal, gestito da un'organizzazione

non lucrativa finanziata da Brian Acton, fondatore di WhatsApp – nel frattempo ceduta a Facebook – che aveva da tempo lasciato l'azienda per contrasto di vedute con la leadership di quest'ultima[3]). Per fatale nemesi, le notizie, vere o false che siano, corrono sul web al millisecondo, anche attraverso video catastrofici o spesso tagliati ad arte, e milioni di utenti fuggono come topi dalla nave che pare affondare.

Il Garante italiano non tarda a reagire e con un comunicato del 14 gennaio 2021 annuncia battaglia: vuole vedere chiaro in un'informativa che chiara non pare[4].

Se la memoria umana di per sé è corta, sul web diventa virale nello stretto e dimensionale senso di nanometrica: WhatsApp ci aveva già provato quasi cinque anni prima, il 25 agosto 2016, in epoca anteriore all'entrata in vigore del GDPR. Stesso stilema: una modifica della privacy policy, accordata dalla facoltà contrattuale del social di modifica unilaterale delle condizioni di servizio, grazie alla quale i dati dell'utenza di WhatsApp avrebbero potuto essere trasferiti ad altre società del gruppo Facebook. Nelle circostanze, all'esito dell'istruttoria avviata a carico della rete di messaggistica il Garante osservò[5] che "*il flusso di dati personali riferiti degli utenti italiani di WhatsApp nell'ambito del gruppo di società facente capo a Facebook si configura come comunicazione a terzi, operazione che è possibile effettuare lecitamente solo ove, prima di attivare il flusso di dati tra le società, il titolare (WhatsApp) abbia acquisito il consenso informato dei singoli interessati (artt. 13 e 23 del Codice) o si sia in presenza di uno dei presupposti di esonero del consenso previsti dall'art. 24 del Codice*[6]".

[3] Il passaggio a tale messenger sembrerebbe essere stato consigliato, tra gli altri, anche dall'Unione Europea ai propri funzionari più di un anno fa: cfr. L. Cerulus, EU Commission to staff: Switch to Signal messaging app, 27.2.2020 in politico.eu.

[4] Così recita il comunicato leggibile sul sito del Garante (doc-web 9519943): "Il messaggio con il quale WhatsApp ha avvertito i propri utenti degli aggiornamenti che verranno apportati, dall'8 febbraio, nei termini di servizio – in particolare riguardo alla condivisione dei dati con altre società del gruppo – e la stessa informativa sul trattamento che verrà fatto dei loro dati personali, sono poco chiari e intelligibili e devono essere valutati attentamente alla luce della disciplina in materia di privacy. / Per questo motivo il Garante per la protezione dei dati personali ha portato la questione all'attenzione dell'Edpb, il Board che riunisce le Autorità privacy europee. / Il Garante ritiene che dai termini di servizio e dalla nuova informativa non sia possibile, per gli utenti, evincere quali siano le modifiche introdotte, né comprendere chiaramente quali trattamenti di dati saranno in concreto effettuati dal servizio di messaggistica dopo l'8 febbraio. / Tale informativa non appare pertanto idonea a consentire agli utenti di Whatsapp la manifestazione di una volontà libera e consapevole. / Il Garante si riserva comunque di intervenire, in via d'urgenza, per tutelare gli utenti italiani e far rispettare la disciplina in materia di protezione dei dati personali".

[5] Provvedimento n. 462 del 4 ottobre 2018, leggibile sul sito istituzionale del Garante Privacy italiano (doc-web 9058572).

[6] Ovviamente il riferimento normativo era al codice privacy anteriore al GDPR.

Interessante lo snodo argomentativo lungo il quale il Garante emanò un chiaro divieto a dar corso alla pratica contestata. Sul piano dell'informativa ai fini del rilascio di un consenso informato, l'Autorità italiana osservò: "a) *l'informativa relativa alla condivisione non rispetta il principio di correttezza e, soprattutto, appare inidonea in quanto non contiene tutti gli elementi tassativamente previsti dall'art. 13 del Codice*[7]*, con riferimento ai seguenti tre profili: i. nel messaggio di notifica viene solo comunicato un generico cambiamento della cd. privacy notice, non evidenziandosi in alcun modo l'elemento sostanziale che ha reso necessario modificare le informazioni agli interessati (vale a dire la condivisione con Facebook dei dati relativi all'account WhatsApp); ii. non è di agevole comprensibilità, anche nell'informativa integrale, quali siano i dati oggetto di comunicazione a Facebook; iii. le finalità perseguite dal trattamento in questione risultano vaghe, specie laddove fanno riferimento a un preteso "miglioramento delle esperienze con le inserzioni e i prodotti di Facebook", mentre si tratta di consentire, tra le altre, a operazioni di carattere pubblicitario effettuate, evidentemente, nell'interesse di Facebook*".

Quanto al consenso, il Garante ritenne che lo stesso non potesse "ritenersi espressamente, specificamente e liberamente manifestato, poiché risulta[va] essere stato richiesto: i. mediante un modello imperniato sul principio dell'opt-out (casella di spunta già "flaggata")[8]; ii. prospettando, in caso di mancata adesione, l'interruzione di un servizio ormai divenuto di generale utilizzo, ossia una conseguenza sproporzionata rispetto alle esigenze di funzionamento dello stesso (come peraltro confermato dal fatto che tale comunicazione di dati non ha poi avuto luogo, senza alcuna compromissione delle attività di WhatsApp)".

Al divieto dell'Autorità s'accompagnò anche un limpido avvertimento: "Ove Whatsapp intenda, nella vigenza del Regolamento [GDPR; n.d.r.], effettuare i predetti trattamenti a prescindere dal consenso e invocare, invece, le diverse basi giuridiche ora indicate, in alternativa al consenso, dall'art. 6, par. 1, lettere da b) a f), del Regolamento, l'Autorità di controllo capofila di cui agli artt. 60 e ss. del Regolamento, in cooperazione con questa Autorità dovrà valutare l'integrale rispetto della disciplina applicabile".

Tornando al presente, nel sito del social il consiglio sembra essere stato, obtorto collo, recepito. WhatsApp dichiara che la sua privacy policy è in via di cambiamento ma assicura che "oggi, Facebook non usa le informazioni

[7] V. nota precedente.

[8] Con tanto di rinvio a precedenti della stessa Autorità: provv. 4 luglio 2013, in www.gpdp.it, doc. web n. 2542348; ordinanze-ingiunzioni 1° ottobre 2015 doc. web n. 4611905, 5 marzo 2015, doc. web n. 4203055, 11 giugno 2015, doc. web n. 4243173, 18 dicembre 2014, doc. web n. 3750400 – nonché Gruppo WP29, Parere n. 15/2011.

del tuo account WhatsApp per migliorare le tue esperienze con i prodotti di Facebook o per fornirti esperienze pubblicitarie più pertinenti su Facebook. Questo è il frutto di colloqui con la commissione per la protezione dei dati irlandese o IDPC (Irish Data Protection Commission) e le altre autorità europee per la protezione dei dati"[9]. Discorso diverso vale per la clientela business, ma gli utenti privati europei, per ora, possono contare sull'applicazione delle regole anteriori. Il caso non è ancora concluso ma è più che ovvio che il social, memore di quel consiglio e a fronte dell'ulteriore richiamo del Garante, non compirà certo le mosse incaute attribuitigli, in alcuni casi in termini imprecisi e fuorvianti. E comunque, anche per gli utenti non europei, il social ha deciso il rinvio dell'aggiornamento a maggio 2021.

Quella che per il momento parrebbe la classica tempesta nel bicchier d'acqua si rivela invece, al di là del caso concreto, la miglior conferma che la vera lotta si consuma non fra reti, neppure fra reti e utenti, ma proprio fra reti e regolatori e che l'impianto protettivo istituito dal GDPR costituisce un baluardo al momento difficilmente espugnabile. Quella stessa vicenda prova, altresì, che la guerra è ben lungi dalla fine (che probabilmente mai arriverà) e che il conflitto potrebbe espandersi ben oltre il tema, pur per ora centrale, del trattamento del dato a fini pubblicitari. Qualche ulteriore riflessione, dunque, s'impone.

Il GDPR si fonda su alcuni capisaldi, fra cui spiccano, ai fini della nostra analisi, il consenso dell'interessato e il principio di minimizzazione dei dati (artt. 5 e 7 GDPR). L'infrazione di queste regole potrebbe spostare il conflitto rete – regolatore su altri piani di lettura.

3. I capisaldi del GDPR: a) il consenso informato fra nuovi terreni di scontro e ricadute civilistiche

Il consenso è il perno su cui ruota l'intero mercato pubblicitario dei social. Infatti, in assenza di esso, la rete non avrebbe titolo alcuno né per comunicare il nominativo dell'utente a terzi né per veicolare messaggi mirati all'utente

[9] Quantunque nel sito ancora si legga che "Attualmente, WhatsApp condivide solo alcuni tipi di informazioni con le aziende di Facebook. Le informazioni che condividiamo con le altre aziende di Facebook includono le informazioni di registrazione dell'account (come il numero di telefono), i dati delle transazioni (per esempio, se usi Facebook Pay o Shops in WhatsApp), informazioni relative ai servizi, informazioni su come interagisci con le aziende quando utilizzi i nostri servizi, informazioni sul tuo dispositivo mobile e sul tuo indirizzo IP. Possiamo inoltre condividere altre informazioni, indicate nella sezione "Informazioni raccolte" dell'Informativa sulla privacy o raccolte previa notifica o con il tuo consenso". Ma la politica è in corso di cambiamento e in ogni caso essa non si applica alle persone fisiche residenti nell'area europea.

stesso, il che presuppone, ovviamente, una specifica attività di profilazione per tagliare su misura il messaggio.
Quando il consenso s'innesta all'interno di un rapporto negoziale, esso diventa superfluo solo nel momento in cui sia necessario all'esecuzione del contratto (art. 6, co. 1, lett. c) GDPR). Il concetto di necessità è letto in termini estremamente restrittivi dal GDPR, che all'art. 7.4 ha cura di precisare che, ai fini della libera prestazione del consenso, "*si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto*". Sia pur in forma lievemente contorta, la norma persegue un fine molto chiaro: evitare che il più generale accordo contrattuale finisca con l'includere anche l'implicito consenso al trattamento di dati che non sarebbero necessari per l'esecuzione del contratto.
Sia qui permessa una breve ma utile parentesi. La natura sinallagmatica del "contratto di rete sociale" è stata rintracciata dalle sentenze gemelle del Tar Lazio 260-261 del 10 gennaio 2020 sulle quali ci siamo altrove già espressi[10]. Il caso riguardava il *claim* di gratuità con cui Facebook invitava i nuovi utenti alla registrazione dei profili unitamente ad un meccanismo di acquisizione del consenso (casella preselezionata di *opt-in*) all'uso per fini promozionali dei dati dell'utente con l'implicito ma inequivoco avvertimento che il rifiuto del consenso avrebbe compromesso la fruibilità del servizio: *claim* che il TAR bocciò, confermando il provvedimento dell'AGCM con cui la pratica era stata ritenuta commercialmente scorretta (ingannevole e aggressiva) ed incentrando la decisione sulla natura patrimoniale del dato personale. Negando l'accettabilità di "*una visione parziale delle potenzialità insite nello sfruttamento dei dati personali*" che ne circoscriva la tutela a "*quella rinvenibile nella sua accezione di diritto fondamentale dell'individuo*", il TAR concluse che i dati possono "*altresì costituire un "asset" disponibile in senso negoziale, suscettibile di sfruttamento economico e, quindi, idoneo ad assurgere alla funzione di "controprestazione" in senso tecnico di un contratto"*.
Tornando al punto e rientrando nel mero ambito privacy, la circostanza che un sinallagma sia rintracciabile fra la fruizione del servizio e il consenso ad un trattamento a fini di raccolta pubblicitaria potrebbe rendere tale consenso superfluo, in quanto necessario all'esecuzione del contratto? La risposta è certamente negativa, per la semplice ragione che il condivisibile costrutto del TAR non trova specifica declinazione nelle condizioni d'uso della rete. Prescindendo, qui e per ora, da ogni ulteriore implicazione circa le conse-

[10] V. nota 1.

guenze del descritto fenomeno di patrimonializzazione del dato personale, i contratti delle reti non rendono affatto chiaro ed esplicito quel sinallagma, difficilmente riconoscibile, e solo a posteriori, dall'utente (*se vuoi usare la rete, devi accettare l'uso pubblicitario dei tuoi dati*).

Secondo il cit. art. 7 GDPR (comma 2°), "*se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante*". Ora, la portata di tale precetto è tutt'altro che irrilevante poiché spesso il consenso all'utilizzazione del dato per fini promozionali o è annegato nei termini del servizio o è catturato attraverso meccanismi di condizionamento della scelta dell'utente (*pre-flag* o simili)[11]. In tali casi se "*nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante*", ciò significa che la necessità del consenso permane tale anche a voler riconoscere un sostanziale *do ut des* nel rapporto fra rete e utente. Ma non solo. A ben vedere, la norma reca in sé una potenziale e dirompente ricaduta anche sul piano civilistico. Se il consenso rilasciato in modo non libero e informato nell'ambito di una più generale dichiarazione rende non vincolante anche ogni altra parte di quella stessa dichiarazione e se quella dichiarazione coincide, come spesso accade, con i termini e le condizioni del servizio, ciò significa che il mancato valido consenso all'uso commerciale del dato rende invalida l'intera pattuizione. Quindi, difetterebbe, oltre al rilascio di un valido consenso, anche il più generale accordo che regola la fruizione del servizio, con conseguente nullità del contratto per carenza di uno dei suoi requisiti essenziali (art. 1325 c.c.).

[11] Non si trascuri in tal senso la limpida lettura data dal 32° considerando del GDPR: "Il consenso dovrebbe essere prestato mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle" (tondi nostri). Del resto il tema è già stato chiaramente affrontato e inequivocabilmente risolto (anche perché più che facilmente risolvibile) dalla Corte di Giustizia dell'Unione Europea (sent. 1° ottobre 2019, Causa C-673/17, trattato nello scritto menzionato in nota 2). Nello stesso senso si orientano anche le nuove Linee Guida sull'utilizzo dei cookie e di altri strumenti di tracciamento poste in pubblica consultazione dal Garante il 26 novembre 2020, sulle quali si rinvia a *Le nuove linee guida sull'utilizzo di cookie e di altri strumenti di tracciamento: cosa cambia e quali gli aspetti tecnici rilevanti* di V. Colarocco, E.R.M. Lazzara, G. D'Agostino, N. Giuli in questo stesso numero della Rivista.

Indubbiamente, un simile esito – a tacer qui di problemi di correttezza commerciale – potrebbe legittimare il social a chiudere il profilo dell'utente, data la nullità del titolo negoziale. Ma è altrettanto indubbio che, in un siffatto caso, la nullità del contratto originario obbligherebbe alla restituzione delle reciproche prestazioni e se ciò, per l'utente, equivale a perdere l'intero contenuto del profilo, per la rete comporterebbe un obbligo restitutorio, probabilmente esteso, totalmente o parzialmente, alle utilità ricavate dall'utilizzo illecito del profilo. Sarebbe pressoché impossibile, dunque concretamente improbabile, una pratica massiva di questa soluzione, poiché la stessa si scontrerebbe con l'esigenza vitale di ogni rete di poter mantenere e incrementare i propri utenti, il proprio "parco fornitori" di dati.
L'intersezione fra la lettura del TAR nel caso sopracitato e il tenore della norma del GDPR potrebbe spianare, come nei fatti spiana, un nuovo terreno di scontro fra reti e regolatori.
È infatti pacifico che ogni rete voglia proseguire nella politica di promozione del servizio come gratuito e nel contempo poter contare sulla pressoché libera utilizzabilità dei dati dell'utente per fini commerciali propri, cercando di tener separate le due direttrici di servizio e di utilizzo dei dati. Le reti non vogliono insomma riconoscere l'esistenza del sinallagma affermato dalla giurisprudenza amministrativa, eppure quel sinallagma esiste. Allo stato attuale, è proprio la regola del consenso libero e informato lo scudo con cui il regolatore paralizza il tentativo delle reti di proseguire nell'artificiale scissione fra apparentemente gratuita fruizione del servizio e prestazione più o meno forzata del consenso all'uso dei dati dell'utenza. Uno scudo che contiene una sorta di sanzione implicita tale da privare di ogni efficacia un'intera pattuizione con cui il consenso ad un trattamento specifico sia stato impropriamente acquisito: dunque uno strumento che determina una sorta di contaminazione di un intero impianto negoziale a motivo di una violazione della normativa privacy, per cui un mancato o illecito consenso acquisito all'uso dei dati travolge il primario consenso sotteso all'accordo contrattuale. Un salto in avanti di non poco momento e destinato ad aumentare il livello dello scontro.

4. (*Segue*): b) il principio di minimizzazione dei dati, spesso sconosciuto alle reti

Altro caposaldo del GDPR rilevante ai nostri fini è il principio di minimizzazione dei dati, i quali, sempre a norma dell'art. 5, debbono essere "*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*". La funzione del precetto è palese e intrinseca al principio stesso

della protezione del dato personale: evitare che il trattamento si estenda a dati eccedenti il necessario, rispetto alle finalità della raccolta.
Nuovamente riemerge il *driver* dello stretto necessario.
E parallelamente si ripropone il tema del se e in che misura i dati dell'utente siano necessari alla rete sociale. Lo scopo dichiarato di una rete non è fare raccolta pubblicitaria bensì consentire l'interconnessione e l'interazione fra più individui (prova ne sia che esistono reti gestite da associazioni di volontari e senza fine di lucro). Ovvio dunque che elementi minimi quali il nominativo dell'interessato, la sua collocazione geografica e il suo indirizzo fisico o elettronico siano da considerarsi indispensabili ai fini di consentire la costruzione di un profilo e renderlo innestabile nel circuito comunicativo della rete. Ma la raccolta delle reti sociali va ben oltre estendendosi anche alle interazioni, al contenuto delle comunicazioni e ad ogni connessa informazione che ne derivi con una facoltà di uso praticamente illimitata e per finalità diverse da quelle con cui gli edulcoranti e, questi sì, minimizzanti linguaggi delle reti dichiarano la finalità della raccolta ("migliorare la tua esperienza", "rendere più fruibili i nostri servizi" e così via).
Una volta di più si ricade in quella logica sinallagmatica, non dichiarata e soprattutto sproporzionata rispetto alla stessa finalità di veicolazione di pubblicità mirata. Altro terreno sul quale, a breve, le reti torneranno a scontrarsi con i regolatori, dovendo risolvere un serio problema di dimostrazione dell'esistenza di una reale, oggettiva e comprovata esigenza di acquisizione di dati "necessari".
Inevitabilmente il tema della minimizzazione s'intreccia con quello della profilazione, quest'ultima definita dall'art. 1 n. 4 del GDPR come qualsiasi forma di trattamento automatizzato di dati personali consistente nel loro utilizzo per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzarne o prevederne aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti: la base cioè di un trattamento per i più svariati scopi, primo fra tutti il marketing. Secondo il GDPR la profilazione potrebbe costituire un interesse legittimo ma solo per finalità di marketing diretto. Tuttavia, l'art. 21 è molto chiaro nell'accordare all'interessato il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.
Dunque, che cosa accade se il nuovo utente accorda il suo consenso alla profilazione estesa richiesta dal social per creare il profilo e poi decide di revocare il consenso? Può o non può la rete escluderlo? Se si affermasse

che l'esclusione sia possibile si cozzerebbe contro il chiaro divieto normativo che ne uscirebbe completamente depotenziato e snaturato, a meno che non si rientri nella logica sinallagmatica sopra descritta, nel qual caso tuttavia ritorneremmo al punto di partenza, nel senso che si dovrebbe ridefinire un perimetro di dati da considerarsi necessari allo scopo (e sempre che il consenso sia stato validamente e coscientemente espresso: v. § 5): acquisti, gusti, contenuti e immagini correlati ad esigenze di marketing diretto possono avere un senso, ma viceversa spostamenti e geolocalizzazioni – ed è solo un esempio – parrebbero eccedere il fine di una pubblicità mirata e sottendere trattamenti per finalità diverse.

Ancora, il principio di minimizzazione dei dati si pone già in fase d'avvio del rapporto fra rete e utente, quando la prima richiede al secondo di metterle a disposizione tutti i contatti presenti nel suo dispositivo. Le scelte dei social non sono uniformate al riguardo: alcuni, correttamente, si limitano a offrire questa possibilità all'utente, altre invece pongono l'apertura della rubrica quale condizione per accedere al servizio, altre ancora offrono una scelta solo apparentemente libera perché nei fatti il rifiuto pregiudica l'interazione. Ove l'utente accetti o sia costretto ad accettare, l'assuefazione dell'utenza porta quest'ultima a non riflettere e a mettere a disposizione gli estremi dei suoi contatti.

Si riapre qui l'antico tema della rubrica personale e della configurabilità di un trattamento anche di dati ad uso privato. Problema che il GDPR risolve sul versante privato o, meglio ancora, "personale e domestico" dei dati. L'art. 1 esclude l'applicabilità del regolamento ai trattamenti di dati "*effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico*": la norma va, per così dire, "decifrata" alla luce del *considerando* 18, che qualifica come attività personali e domestiche quelle "*senza una connessione con un'attività commerciale o professionale*", specifica che tali attività "*potrebbero comprendere la corrispondenza e gli indirizzari, o l'uso dei social network e attività online intraprese nel quadro di tali attività*" e, infine, si premura di precisare: "*Tuttavia, il presente regolamento si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico*".

Sul piano individuale un problema potrebbe porsi là dove un dispositivo sia utilizzato ad uso promiscuo[12]: in uno stesso computer o smartphone

[12] Come spesso accade normalmente e come è accaduto e accade nel corso della pandemia, dove non sempre i lavoratori dipendenti o autonomi costretti ad un repentino lavoro agile sono stati dotati o disponevano di dispositivi per la gestione delle attività personali separati da quelli per lo svolgimento di attività lavorative o professionali.

possono convivere ad esempio numeri telefonici e indirizzi di famigliari, parenti e amici così come indirizzi e recapiti di colleghi, clienti o fornitori, browser di mail personali e aziendali. Non appare tuttavia né realistico né ragionevolmente esigibile né tanto meno tecnicamente sorvegliabile l'imposizione del poderoso impianto di tutela al singolo individuo sul dispositivo di sua proprietà utilizzato a fini plurimi. Tranne, verrebbe da dedurre, l'impiego di adeguate misure di sicurezza che, nei limiti del ragionevole, possano essere adottate per la protezione dei dati personali di terzi, siano essi privati o soggetti professionali. Sicché, tornando al punto, non potrebbe considerarsi conforme a prudenza e a sicurezza aprire la propria rubrica al gestore di una rete.

Accantoniamo tuttavia questo antico dilemma in quanto ci porterebbe troppo in là e riprendiamo il filo del discorso.

Nel caso in cui l'utente, perché la scelta di aprire o no la rubrica gli è stata concessa o perché non gli è stata data, apra l'indirizzario, il gestore viene a conoscenza di dati (nominativi, recapiti telefonici, indirizzi di posta elettronica, magari e spesso anche fotografie nel caso in cui siano presenti nel dispositivo dell'utente e questi le abbia associate ai suoi contatti) di soggetti terzi rispetto alla rete perché deliberatamente hanno ritenuto di non aderirvi. Nondimeno i loro nominativi sono soggetti ad un pur minimo trattamento, con ogni probabilità consistente nel confronto fra i dati che, nella rubrica del nuovo utente, corrispondono a profili che utilizzano la stessa rete e i dati di coloro che invece non la utilizzano. Di quel trattamento (sempre ammesso che il dato del terzo non venga comunque trattenuto dalla rete, perché in tal caso ci si troverebbe di fronte ad una violazione plateale della normativa), il soggetto terzo dovrebbe ricevere adeguata informativa in base all'art. 14, comma 1° dello stesso GDPR, trattandosi di dati raccolti presso un terzo (ossia il neo-utente), ma tale informativa di norma non avviene, invocando l'esimente di cui al comma 5° dello stesso articolo, che esclude l'obbligo di informazione quando questa sia impossibile o richiederebbe uno sforzo sproporzionato[13] da parte del titolare del trattamento.

[13] Il che, peraltro, è assai discutibile. La potenza degli algoritmi di gestione è tale per cui non pare affatto né impossibile né sproporzionata una notifica automatica al terzo estraneo, la quale precisi che il dato è stato fornito da un utente del social e che la rete, rilevata l'estraneità dell'interessato alla rete stessa, lo ha utilizzato solo per accertare l'estraneità del terzo e lo ha già cancellato dalla memoria del sistema. A voler essere pignoli, l'esimente opererebbe prioritariamente per raccolte operate per trattamenti a fini di archiviazione di interesse pubblico, di ricerca scientifica o storica o a fini statistici, in nessuna delle quali categorie ricade l'accesso di una rete sociale a rubriche in cui possono essere (e di norma sono) presenti contatti di persone che non utilizzano quella stessa rete (cfr. art. cit. e considerando 62).

Tuttavia, è lecito domandarsi se un simile trattamento sia davvero necessario alla funzionalità del social o se non sia esso stesso una violazione del principio di minimizzazione. È così indispensabile accedere alla rubrica di un utente? Supponiamo che il Signor A decida di iscriversi al social XY, il quale gli chieda o gli imponga di aprire la sua rubrica – processo che tecnicamente si realizza permettendo all'applicazione XY di "leggere" un'altra applicazione (rubrica contatti). Nella rubrica di A, vi sono anche la Signora B, l'avvocato C, il medico specialista in malattie rare D. B e C usano già a loro volta l'applicazione XY, mentre D non la utilizza né ha intenzione di utilizzarla. L'apertura della rubrica consegna a XY (almeno) nominativo, telefono e molto probabilmente anche e-mail di B e C dei quali, essendo già suoi clienti, XY è già a conoscenza. La stessa apertura, però, consegna a XY anche i dati del medico D. L'acquisizione dei dati di B e C è del tutto superflua, quella dei dati di D del tutto estranea allo scopo dell'avvio del servizio fra la rete XY e il Signor A. Nel primo caso si chiede o si obbliga A alla comunicazione di un dato inutile, nel secondo alla comunicazione del dato di un terzo che A potrebbe benissimo non voler comunicare (nell'esempio, essendo un medico esperto in malattie rare, ne sia A affetto o meno) e che il medico D non vorrebbe fosse trasferito a terzi, men che mai a una rete sociale che egli detesta. Ma il dato, in tal senso, si "moltiplica": non solo la rete XY viene a conoscenza dei dati di D ma anche del fatto che D sia in contatto con A. In entrambi i casi, assistiamo ad una sovrabbondanza di richiesta di dati che va a toccare anche soggetti estranei al rapporto rete-utente.

Non è forse questa una violazione del principio di minimizzazione? Non assume alcun rilievo il fatto che il trattamento sia limitato (sempre che lo sia: v. § 5) ad una scrematura dei contatti che già aderiscono alla rete, in vista di facilitare il nuovo utente a rintracciarli: questa, al limite, è una funzionalità aggiuntiva, per la quale occorrerebbe una specifica informativa e un altrettanto informato specifico consenso, dunque quanto meno l'apertura della rubrica dovrebbe sempre essere una facoltà e non già una condizione di fruizione del servizio. Mentre assume rilievo il fatto che questa intrusione della rete in altra applicazione dell'utente comporti la possibilità di conoscere dati (ed inferirne collegamenti più o meno appropriati con l'utente) anche di individui terzi e senza che gli stessi ne vengano a conoscenza. Tutto ciò, non essendo strettamente necessario all'attivazione del servizio (come dimostra il fatto che alcune reti non impongono affatto questo obbligo), certamente conduce ad un'acquisizione di dati esorbitante lo scopo.

Anche questo è certamente un ulteriore terreno di battaglia fra reti e regolatori destinato a condurre ad esiti probabilmente molto sorprendenti. E lo è perché il principio di minimizzazione dei dati risulta, allo stato attuale,

molto affermato in astratto, ma non ancora completamente esplorato in tutte le sue potenzialità limitative di raccolta e trattamento[14].

5. Nuove aggressioni, estensione del conflitto, proiezioni evolutive

Il raggio espansivo del conflitto può essere ampio e palese così come oscuro e ristretto. La morsa regolativa riduce, lentamente ma senza sosta, ogni

[14] Come confermato dal fatto che l'attenzione del Garante si sta sempre più penetrantemente soffermando proprio sul tema qui discusso. Nella Relazione 2019, prendendo posizione sul delicato tema connesso al suo provvedimento 18 aprile 2019, n. 96 (doc. web n. 9105201) in materia il corretto uso dei dati relativi agli elettori da parte di partiti, movimenti politici, comitati promotori, sostenitori e singoli candidati (cfr. par. 14.5.3), e soffermandosi altresì sull'uso di messaggi politici e propagandistici inviati agli utenti, il Garante ha osservato: "anche alla luce di casi recenti di profilazione massiva degli elettori (il cd. micro-targeting), pure in quest'ambito il trattamento dei dati deve rispettare la cornice normativa esistente, sì da proteggere il processo elettorale ed evitare rischi di interferenze e turbative esterne. Le preoccupazioni di un utilizzo improprio dei dati personali per sofisticate attività di profilazione su larga scala e di invio massivo di comunicazioni o, ancora, per orientare campagne personalizzate volte a influenzare l'orientamento politico e/o la scelta di voto degli interessati sulla base degli interessi personali, dei valori, delle abitudini e dello stile di vita dei singoli rendono infatti urgente garantire la corretta applicazione delle norme in materia di protezione dei dati, soprattutto online, anche al fine di proteggere il processo elettorale da interferenze e turbative esterne. In tale quadro, va ribadito che il trattamento dei dati personali finalizzato all'invio di messaggi politici e propagandistici agli utenti di social network (come Facebook o Linkedin), in privato come pubblicamente sulla bacheca virtuale degli stessi, sono sottoposti alla disciplina in materia di protezione dei dati (artt. 5, 6, 7, 13, 24 e 25 del RGPD). La medesima disciplina è altresì applicabile ai messaggi inviati utilizzando altre piattaforme, come Skype, WhatsApp, Viber, Messenger, rispetto alle quali i rischi sopra evidenziati risultano ancor più elevati in considerazione delle peculiari condizioni di servizio imposte unilateralmente dalle piattaforme di comunicazione e social networking, anche mediante i dispositivi mobili utilizzati. Talora, infatti, esse prevedono la condivisione indifferenziata (e senza il necessario consenso specifico) di tutti o gran parte dei dati personali memorizzati negli smartphone e nei tablet (quali rubrica, contatti, sms, foto, dati della navigazione internet) o l'accesso del fornitore a tali informazioni" (Garante per la Protezione dei dati personali, Relazione 2019, 125, tondi nostri). Nello stesso senso va letta la (pur più ampia) inchiesta aperta dal Garante su Clubhouse, il nuovo social americano "elitario", dove non si postano messaggi o foto ma si parla in stanze virtuali cui si accede solo su invito. Nella sua privacy policy (disponibile sul sito clubhouse.com) si legge fra, le altre cose: "may we use your list of contacts (if you choose to provide us with access to them) to recommend other users you might want to follow and to recommend your account and content to others": in altri termini, l'apparente facoltà di scelta se condividere o meno i contatti diviene nella sostanza una condizione per poter concretamente fruire del servizio. Sulla stessa linea si colloca del resto la recentissima presa di posizione del Garante che, nelle nuove Linee Guida sull'utilizzo dei cookies (nel mentre scriviamo ancora in fase di pubblicazione), richiamando il principio di minimizzazione dati personali da applicarsi vieta la prassi, ancora largamente in uso nel web, di inibire la navigazione in assenza della prestazione del consenso allo scaricamento di cookies di profilazione. V. anche nota 19.

margine erosivo azzardato dalle reti, non di rado inclini anche a spregiare gli statuiti giurisprudenziali[15]. È questa la civiltà e libertà cui tutti ambiamo, specie in tempi d'inclusione ecosostenibile e politicamente corretta, tempi che abbattono financo blocchi di bronzo o marmo inermi, invece utili per ricordare meriti e nefandezze di chi ne è stato il calco e per giudicarli con razionale discernimento invece che con i *like* d'un *meme* ignorante e d'un eteroguidato *cry havoc*?

Vi sono molti ambiti in cui il solletico dell'ego produce effetti straordinari. Le applicazioni per calcolare lo stato di salute (battiti cardiaci, colesterolo, muscolatura, zuccheri, agrodolci e intermedi, saturazione, glicemia, calorie bruciate, stress, emozioni, postura, quantità e qualità del sonno e molto altro) sanno dare un profondo senso di esaltazione o un deprimente messaggio di esclusione secondo ciò che il *mainstream* impone. Ma chi potrebbe impossessarsi di quelle informazioni, piaccia o no al GDPR, concependo nuove applicazioni che, grazie a un frettoloso consenso, possano leggere i dati salutisti di altre? E come quelle applicazioni stesse tutelerebbero quel prezioso e sensibile patrimonio conoscitivo? "*Alzi la mano, del resto, chi ancora crede che gli stessi, legittimi collettori e padroni di dati non ne facciano uso commerciale a nostra insaputa*"[16].

Oppure: abbiamo mai pensato come potrebbero essere manipolati, contraffatti, fraintesi e strumentalizzati scritti, parole, opere, omissioni o commissioni, non necessariamente esposti in un social ma anche diffusi altrove in Internet, per profilarci non più a scopo commerciale ma per fini esclusivi (nel senso stretto di esclusione) o classificatori (profilazioni extra-commerciali utilizzabili per ricatti economici)? Oppure per fini falsificatori delle nostre persone e del nostro pensare?

A tratti sembra di tornare alle epoche post-lumi quando, accantonate le

[15] È del 17 febbraio scorso la notizia dell'irrogazione a Facebook da parte dell'AGCM della sanzione di complessivi 7 milioni di euro per non aver attuato quanto prescritto nel provvedimento emesso nei suoi confronti nel novembre 2018 e avente ad oggetto l'accertata pratica scorretta consistente nell'indurre in modo ingannevole gli utenti a registrarsi sulla piattaforma social non informandoli – durante l'attivazione dell'account – dell'attività di raccolta, con intento commerciale, dei dati da loro forniti e, più in generale, delle finalità remunerative sottese al servizio, enfatizzandone viceversa la gratuità. Constatata la mancata pubblicazione a rettifica e la mancata cessazione della pratica scorretta accertata, l'Autorità ha nuovamente sanzionato il Social con la misura sopra descritta. È invece del giugno 2019 l'applicazione a Facebook di una sanzione di 1 milione di euro per gli illeciti compiuti nell'ambito del ben noto caso "Cambridge Analytica", la società che attraverso un'app per test psicologici aveva avuto accesso ai dati di 87 milioni di utenti e li aveva usati per tentare di influenzare le elezioni presidenziali americane del 2016.

[16] Così si legge in G. Ghidini – D. Manca – A. Massolo, *La nuova civiltà digitale*, Milano, 2020, p. 113 ss.

credenze religiose, gli umani si votarono all'occultismo, alla negromanzia, alle divinazioni da interiora. Roba di cui (forse) oggi ridiamo ma che proprio oggi si riproduce, in altra forma e con sembianze meno rivoltanti, con la stessa imperiosità d'un credo religioso o d'una superstizione. Dopo essersi ripresi ogni genere di libertà, gli individui ora incappano in nuove forme di asservimento: e lo fanno da soli, per incoscienza o per bisogno di essere in una realtà virtuale, specie se quella reale li confini nell'anonimato.
WhatsAppening, whatsfacebooking, whatstwittering, whatsinstagramming, whatstiktokening, whatspinteresting, whatsyoutubening, whatsnapchattening, whatsclubehousing, whatsgoogling and so on socializing. La domanda "che succede" potrebbe essere rivolta a questi e ad altri collettori privati di dati. Potremmo continuare all'infinito, certi di tornare sempre al punto di partenza, come nel nostalgico Monopoli quando si riparte da una casella per arrivare ad un'altra senza passare dal "via", il tutto in balia d'un lancio di dadi – in questo caso di qualche click di troppo, troppo carpito o troppo distratto.
La guerra non cesserà, perché le prede sono troppo golose per chi le cerca, troppo assuefatte per chi le impersona e ormai troppo dipendenti ed esauste per reagire. Restano solo i regolatori, spesso pachidermici e paludati secondo la narrazione corrente, nei fatti assai più occhiuti e rapidi di quanto non lo siano le (deboli) reazioni dei (pochi) singoli. Pur nel sacrosanto rispetto di ogni più lecita critica, i regolatori oggi dovrebbero essere lodati. Siamo inclini ad ignorarli o anche a disprezzarli per il loro puntiglio leguleio o per il loro fastidioso intromettersi nei nostri mondi paralleli. Peccato, diremmo meglio: per fortuna, che siano i più – licenza "poetica" – resilienti fortilizi di protezione.