Covid-19, la società affidata alla rete avvia nuovi modelli completando la rivoluzione digitale

Covid-19, web society and digital revolution. The new challenges of emergency, security and individual rights

Fulvio Berghella, Oasi-Gruppo Cedacri

Keywords
Covid-19, lavoro a distanza, Intelligenza artificiale

Jel codes
I18, M15, O33

L'emergenza provocata dalla pandemia e la necessità di isolare le persone evitando i contatti hanno permesso l'avvio immediato del telelavoro e lo svolgimento a distanza di tutte le attività che non richiedono la presenza fisica. La gestione della crisi, lo sviluppo di sistemi basati sull'intelligenza artificiale e l'affidamento globale alla rete comportano vantaggi e rischi che richiedono equilibrio tra sicurezza, globalizzazione dei dati e privacy.

The emergency caused by Covid-19 disease pandemic and the need to isolate people allowed the immediate start of teleworking and the development of all activities that do not require physical presence. Crisis management, systems based on artificial intelligence and global reliance on the network entail advantages and risks that require a balance between security, data globalization and privacy.

1. Niente sarà come prima

Niente sarà come prima! È questa l'esclamazione ricorrente che caratterizza la crisi generata dalla pandemia del Coronavirus disease 2019 (Covid-19). La stessa espressione accompagnò l'avvento di Internet, il crollo delle twin tower e la crisi economica conseguente le vicende Lehman Brothers. Ma questa volta è diverso perché tutti, indipendentemente dai ruoli e dalla condizione sociale, hanno dovuto confrontarsi con la fragilità della propria esistenza, la precarietà delle attività economiche, il limite della sicurezza sociale. La scala dei bisogni umani è regredita a quelli primari di salute e sicurezza, declassando quelli superiori di socializzazione, prestigio e autorealizzazione.

L'emergenza sanitaria e la crisi sistemica hanno costretto i governi a scelte difficili e conflittuali: sul piano nazionale interno la necessità di decidere se adottare sistemi di sorveglianza totalitari o affidarsi alla responsabilizzazione dei cittadini; su quello dei rapporti internazionali il dover riflettere tra l'isolamento del proprio Paese o sperare nella solidarietà internazionale. Le decisioni hanno comunque richiesto rapidità. Così in pochi giorni sono stati avviati processi di nuovi funzionamenti delle attività sociali e produttive, in ambito pubblico e privato che, in tempi normali, avrebbero richiesto anni di dibattito.

L'isolamento domiciliare e l'impossibilità degli spostamenti hanno generato la proliferazione di tutte le attività eseguibili a distanza. Il virus, in un certo senso, ha costretto milioni di persone all'alfabetizzazione informatica e rimosso le ultime resistenze alla rivoluzione digitale avviata con l'avvento di Internet.

I primi tangibili cambiamenti, incoraggiati dalla normativa sull'emergenza dai Dpcm del 4 e 11 marzo 2020, e che in parte sono destinati a permanere nel tempo, riguardano il

lavoro agile per le attività che possono essere svolte al proprio domicilio o in modalità a distanza. Un'indagine svolta da Bva Doxa nei primi di marzo su un campione di 301 aziende operanti in Italia ha evidenziato: un uso massivo dello smartwork esteso al maggior numero di persone nel 73% degli intervistati, un utilizzo contenuto circoscritto ad alcune aree/funzioni nel 17% e marginale riservato a specifiche figure nel 10%. Maggiore è l'adesione delle aziende multinazionali (90%). Altissima l'efficienza percepita nella gestione dell'attività lavorativa (90%). Nel 39% dei casi si ritiene che i cambiamenti organizzativi permarranno anche dopo il termine della crisi.

Il telelavoro in tutte le sue forme (smartworking, remote working, home working), la teledidattica, la telemedicina, la teleassistenza, il supporto psicoterapeutico, i rapporti con pubblica amministrazione, gli acquisti, le operazioni bancarie online, i tele-contatti sociali, nel loro insieme, hanno provocato un incremento della domanda di Internet stimata nel 40% in più rispetto alle precedenti medie di normale utilizzo, con punte del 60% nei periodi di accesso degli studenti alle videolezioni.

2. Regole per il telelavoro sicuro

L'affidamento di gran parte delle attività sociali alle comunicazioni via Internet comporta notevoli vantaggi, ma anche nuove vulnerabilità e rischi da mitigare, compresa la capacità della rete di sopportare il traffico eccessivo, tant'è che il Decreto legge 17 marzo 2020, n. 18, cosiddetto «Cura Italia», all'art. 82 con rubrica «Misure destinate agli operatori che forniscono reti e servizi di comunicazioni elettroniche» prescrive che fino al 30 giugno 2020, al fine di far fronte alla crescita dei consumi dei servizi e del traffico sulle reti di comunicazioni elettroniche, le imprese che svolgono attività di fornitura di reti e servizi di comunicazioni elettroniche intraprendono misure e svolgono ogni utile iniziativa atta a potenziare le infrastrutture e a garantire il funzionamento delle reti e l'operatività e continuità dei servizi.

Con l'aumento delle connessioni crescono contemporaneamente i rischi dei cybercrime. Il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (Cnaipc), attraverso la Polizia postale, ha diffuso note di allertamento su alcune nuove minacce informatiche che sfruttano la tematica del Coronavirus. In particolare due malware diffusi via e-mail attraverso campagne massive di spam, in grado di assumere il controllo remoto del pc in cui è stato eseguito.

Le criticità hanno indotto l'Agenzia europea per la sicurezza informatica a emanare, il 24 marzo, alcune raccomandazioni per i datori di lavoro e per il personale, al fine di migliorare la sicurezza in tempi di Covid-19[1]. Tra le disposizioni, ai datori di lavoro è raccomandato di: assicurarsi che le soluzioni Vpn aziendali siano in grado di supportare un gran numero di connessioni simultanee; fornire videoconferenze audio/video sicure; accedere alle applicazioni aziendali solo tramite canali di comunicazione crittografati; consentire l'accesso ai portali delle applicazioni mediante meccanismi di autenticazione a più fattori; assicurarsi che i computer e altri dispositivi aziendali usati dispongano di software e patch di sicurezza aggiornati e ricordare agli utenti di verificare gli avvenuti aggiornamenti; garantire che siano disponibili adeguate risorse It per supportare il personale in caso di problemi tecnici durante il telelavoro; garantire l'esistenza di policy per la gestione degli incidenti di sicurezza e le violazioni dei dati personali; assicurare che il trattamento dei dati del personale da parte del datore di lavoro nel contesto del telelavoro sia conforme al quadro giuridico dell'Ue in materia di protezione dei dati.

Al personale in telelavoro sono indirizzate raccomandazioni simmetriche, ma anche di: non usare lo stesso dispositivo per le attività di lavoro e per quelle svolte nel tempo libero; connettersi a Internet tramite reti sicure non utilizzando quelle aperte, per evitare che le persone nelle vicinanze possano fare intrusioni; non scambiare informazioni aziendali sensibili attraverso connessioni potenzialmente insicure; utilizzare, per quanto possibile, le risorse Intranet aziendali per la condivisione dei file di lavoro; prestare particolare attenzione alle e-mail che fanno riferimento al Coronavirus, poiché potrebbero nascondere tentativi di phishing o truffe; crittografare i dati inattivi per proteggerli dal furto o dallo

[1] Le complete raccomandazioni di Enisa sullo smartworking sono consultabili all'indirizzo: https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home.

smarrimento; utilizzare antivirus e antimalware sempre aggiornati; attivare il blocco schermo nel caso di lavoro in uno spazio condiviso; non condividere gli Url delle riunioni virtuali sui social media o altri canali pubblici.

3. Prevenzione tecnologica e privacy

Le tecnologie possono fornire un grande contributo ad arginare la pandemia, migliorare l'assistenza ai pazienti domestici, monitorare nel continuo il livello di esposizione al rischio di contagio. La ricerca delle migliori soluzioni digitali è stata già avviata con un programma interministeriale di concerto con le autorità scientifiche. In alcuni paesi è stato attivato, con buoni risultati, il «contact tracing» finalizzato al tracciamento degli spostamenti delle persone potenzialmente portatrici di infezione, ricorrendo ad applicazioni per la localizzazione mediante dispositivi mobili. E, nel contesto emergenziale, nel quale è richiesto un trattamento planetario di dati sensibili, non mancano i sostenitori della sospensione del diritto alla privacy a vantaggio della sicurezza collettiva. Ma qual è l'equilibrio tra le due esigenze? La prudenza richiede riflessioni attente, anche per evitare che, terminata l'emergenza, le decisioni eventualmente assunte nella condizione di crisi possano permanere causando la regressione dei diritti fondamentali acquisiti in tempi normali. Nella disamina delle normative si evince che privacy e sicurezza non solo sono conciliabili, ma la protezione dei dati personali è garanzia di ogni forma di sicurezza.

Il regolamento europeo (Gdpr) è stato redatto anche tenendo conto di circostanze epidemiche sanitarie, come risulta dal Considerando 46: «Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione (…)». Ed è previsto all'art.9.2.c una deroga al divieto di trattamenti di dati sanitari quando il trattamento è necessario per tutelare un interesse vitale dell'interessato, e l'applicabilità può ritenersi necessaria anche nel contesto lavorativo.

Al riguardo, nell'ambito delle iniziative inerenti all'epidemia di Covid-19, il Comitato europeo per la protezione dei dati, il 19 marzo 2020, ha adottato una dichiarazione. In essa si afferma che l'emergenza è una condizione giuridica che può legittimare limitazioni delle libertà, a condizione che tali limitazioni siano proporzionate e confinate al periodo di emergenza. La dichiarazione conferma i principi fondamentali da applicare, riassumibili[2] in alcuni fondamenti:

- la liceità del trattamento deve essere comunque garantita. Il regolamento generale sulla protezione dei dati si applica anche al trattamento dei dati personali in un contesto pandemico e consente alle competenti autorità sanitarie pubbliche e ai datori di lavoro di trattare dati personali nel contesto di un'epidemia, conformemente al diritto nazionale. Gli esimenti previsti consentono la gestione dell'emergenze, ad esempio se il trattamento è necessario per motivi di interesse pubblico rilevante nel settore della sanità pubblica, non è necessario il consenso dei singoli interessati;
- nel settore delle telecomunicazioni, di rilevante importanza nella gestione dell'emergenza, anche in relazione alle norme di controllo e del lavoro, sono in vigore le leggi nazionali di attuazione delle regole europee (direttiva e-privacy), basate sul principio che i dati relativi all'ubicazione possono essere utilizzati dall'operatore solo se resi anonimi o con il consenso dei singoli e le restrizioni non si applicano ai dati anonimizzati. È anche previsto che i singoli Stati possano introdurre ulteriori misure legislative finalizzate alla tutela della sicurezza pubblica, a condizione che le misure adottate siano necessarie, adeguate e proporzionate senza rinunciare ai fondamenti che distinguono una società democratica. I provvedimenti dovrebbero, perciò, rispettare i contenuti della Carta dei diritti fondamentali e della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Pertanto, le misure adottate dovranno cessare al termine dell'emergenza;
- per la salvaguardia dei diritti, le persone interessate dovrebbero ricevere chiare informazioni sulle attività di trattamento straordinario e il periodo di conservazione dei dati trattati per l'evento straordinario;

2 Il documento (9295504) è consultabile sul sito: www.garanteprivacy.it.

- tutte le altre norme che interessano il contesto lavorativo e le informazioni sanitarie specifiche relative al Covid-19 devono agire in conformità al diritto nazionale, comprese le norme vigenti in materia di lavoro e di salute e sicurezza;
- inoltre, per quanto riguarda il monitoraggio degli spostamento delle persone diagnosticate come positive, mediante app per la localizzazione con telefoni cellulari è da considerare che queste soluzioni, comportando la geolocalizzazione, richiedono un approccio particolare. Il Comitato europeo suggerisce che le autorità pubbliche dovrebbero cercare di trattare i dati relativi all'ubicazione in modo anonimo, in forma aggregata e tale da non consentire la successiva re-identificazione delle persone. In tal modo permettendo lo svolgimento di analisi sulla concentrazione di dispositivi mobili in un determinato luogo (cartografia). Seguendo il principio di proporzionalità le misure decisamente invasive, come il tracciamento di localizzazione non anonimizzata, possono essere considerate proporzionate in circostanze eccezionali, ma tali misure dovrebbero essere soggette a maggiori controlli e tempi minori di conservazione dei dati (principio di limitazione della finalità).

Le attività formative a distanza (teledidattica), previste dai decreti per l'emergenza Covid-19, comportano potenziali rischi derivati da un uso scorretto e inconsapevole degli strumenti utilizzati. Con un provvedimento del 26 marzo[3], il Garante privacy ha emanato gli indirizzi da seguire. Tra essi, in applicazione dei principi di privacy by design e by default è indicato che: gli strumenti utilizzati da scuole e università devono possedere fin dalla progettazione e per impostazioni predefinite misure a protezione dei dati; le piattaforme informatiche utilizzate devono fornire solo i servizi richiesti per la didattica online e minimizzare i dati trattati evitando funzionalità non pertinenti (ad esempio, la geolocalizzazione); i soggetti interessati (alunni, studenti, genitori e docenti) dovranno essere informati sulle caratteristiche del trattamento; le informazioni rese dovranno risultare comprensibili ai minori, cui sono riservate anche particolari garanzie di protezione sull'utilizzo dei loro dati.

4. Analisi dei dati e algoritmi antropocentrici

L'uso sistemico delle tecnologie emergenti di data analytics e d'intelligenza artificiale (Ia) per monitorare e contenere il contagio da Coronavirus è stato già sperimentato con successo in alcuni paesi. In Cina molti ospedali sono stati dotati di sistemi Ia in grado di diagnosticare con rapidità la presenza del Covid-19 in pazienti sospetti. Il software consente l'analisi di scansioni termografiche praticate sui petti dei soggetti esaminati distinguendo, con un margine di errore modesto, la tipologia di polmonite. Altre nazioni sperimentano soluzioni che incrociano, mediante algoritmi Ia, dati di questionari compilati dalla popolazione con app, big data territoriali, cartografie e spostamenti, cercando di prevedere le zone in cui si svilupperanno contagi. Ulteriori iniziative avviate da scienziati e ricercatori di centri universitari hanno avviato un forum globale di condivisione dei dati per favorire la comprensione comune e la ricerca di soluzioni. Scienza e ricerca superano i confini nazionali condividendo in rete dati, informazioni e ipotesi di soluzioni.
Anche su questi aspetti il virus ha rimosso molti dei pregiudizi esistenti e accelerato l'uso dell'Ia. Terminata l'emergenza, molte delle innovazioni acquisite durante la crisi faranno parte della vita normale. Nel frattempo, nel Web, sarà stata scambiata e memorizzata un'enorme quantità di dati, con relativi vantaggi e nuovi rischi di abusi. I dati dello scenario digitale mondiale attestano su Internet, prima della crisi, circa 4,5 miliardi di utenti, ma evidenziano anche che solo la metà del traffico è generato da essere umani, la restante metà proviene da bot. E questo aspetto richiede ulteriori considerazioni.
Il rapporto dell'indagine conoscitiva sui big data, condotto congiuntamente dall'Autorità per le garanzie nelle comunicazioni (Agcom), dall'Autorità garante della concorrenza e del mercato (Agcm) e dal Garante per la protezione dei dati personali, pubblicato il 10 febbraio 2020 (quindi prima dello sviluppo nazionale dell'epidemia e del conseguente super utilizzo della rete), evidenzia la crescita esponenziale della produzione di dati. Nell'anno 2018 il volume totale

3 Il provvedimento è consultabile sul sito www.garanteprivacy.it (doc. web n. 9300784).

di dati creati nel mondo è stato di 28 zettabyte, (uno Zb è pari a un trilione di gigabyte) con una previsione che entro il 2025 il volume complessivo dei dati arriverà fino a 163 Zb. Il processo viene convenzionalmente articolato in tre fasi, ciascuna comprendente operazioni di trattamento quali:

1. raccolta (generazione, acquisizione, memorizzazione);

2. elaborazione (estrazione, integrazione, analisi);

3. interpretazione e decisione.

Per ciascuna fase, ai fini regolamentari delle normative applicabili, è necessario definire se i dati oggetto di trattamento hanno natura personale o non personale. Con riguardo al trattamento dei dati di natura personale il rapporto ricorda che è stato previsto uno specifico regime di protezione nell'ambito del quadro normativo definito a livello europeo, a cui concorrono sia il Gdpr, sia regole speciali per le attività online, individuate nella direttiva 2002/58/Ce sul trattamento dei dati personali e la tutela della vita privata nel settore delle comunicazioni elettroniche[4].

Il tracciamento, la geolocalizzazione, i controlli, il monitoraggio delle attività e dei consumi richiedono lo sviluppo di software basati su algoritmi di cosiddetta intelligenza artificiale. Ed anche su questi aspetti è necessario effettuare valutazioni sulla liceità delle soluzioni adottate, tenendo conto degli indirizzi normativi esistenti, a partire dalle «Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679[5]». Il 19 febbraio 2020 la Commissione europea ha pubblicato il documento *White paper. On Artificial Intelligence - A European approach to excellence and trust*, nel quale viene precisato che nei piani della Commissione è previsto un approccio coordinato sulle implicazioni umane ed etiche dell'intelligenza artificiale, nonché una riflessione sull'uso migliore dei big data per l'innovazione, nel rispetto del principio che l'intelligenza artificiale europea sia fondata sui valori e diritti fondamentali come la dignità umana e la protezione della privacy, riassumile nel concetto di un approccio umanocentrico.

5. Toolkit del Consiglio d'Europa

Il Consiglio d'Europa, il 7 aprile, ha indirizzato ai governi dei 47 Stati membri un toolkit sul rispetto dei diritti umani, della democrazia e dello Stato di diritto durante la crisi del Covid-19.

Il documento si propone di contribuire a garantire che le misure adottate nell'emergenza siano proporzionate alla minaccia di diffusione del virus e limitate nel tempo, affinché, oltre alle vite umane, non vadano distrutti i valori fondamentali delle società libere. Il documento tratta quattro aree principali:

- deroga alla Convenzione europea dei diritti dell'uomo in situazioni di emergenza;
- rispetto dello Stato di diritto e dei principi democratici in situazioni di emergenza, compresa la fissazione di limiti alla portata e durata delle misure di emergenza;
- norme fondamentali in materia di diritti umani, compresa la libertà di espressione, la protezione della vita privata e dei dati personali, la protezione dei gruppi vulnerabili dalla discriminazione e il diritto all'istruzione;
- protezione dalla criminalità e tutela della vittime di reato, in particolare per quanto riguarda la violenza di genere.

Il Consiglio precisa, tra l'altro, che l'entità delle misure adottate e il modo in cui vengono applicate variano in ragione della gravità della crisi e avendo natura eccezionale possono richiedere deroghe agli obblighi degli Stati previsti dalla Convenzione. Spetta a ogni Stato valutarle, ma alcuni diritti non sono alienabili, tra essi: il diritto alla vita, il divieto di tortura e il trattamento o la punizione disumani o degradanti, il divieto di schiavitù e servitù e la regola del «nessuna punizione senza legge». Deve comunque prevalere il principio di legalità. L'azione dello Stato deve restare conforme alla legge e conservare la base costituzionale in ogni atto.

In merito alla tutela della privacy e protezione dei dati, il Consiglio ricorda che le nuove tecnologie hanno la capacità potenziale per contenere e porre rimedio alla pandemia, dati di geolocalizzazione, intelligenza artificiale, riconoscimento facciale, applicazioni sui social media, potrebbero facilitare la sorveglianza pandemica. I principi di protezione

4 Direttiva 2009/136/Ce del Parlamento europeo e del Consiglio del 25 novembre 2009.

5 Versione emendata e adottata in data 6 febbraio 2018.

dei dati e la Convenzione 108 del Consiglio d'Europa consentono un bilanciamento tra protezione e interessi pubblici, compresa la salute pubblica, anche con eccezioni alle normali regole di protezione dei dati, per un periodo di tempo limitato, con garanzie adeguate e un efficace quadro di controllo per garantire che questi dati siano raccolti, analizzati, archiviati e condivisi in modi legittimi e responsabili. Il trattamento su larga scala di dati personali mediante l'intelligenza artificiale dovrebbe essere eseguito solo quando l'evidenza scientifica dimostra che i potenziali benefici per la salute pubblica prevalgono sui benefici di soluzioni alternative e meno invasive.

6. Conclusioni

La crisi sistemica ha prodotto situazioni asimmetriche. Da un lato l'isolamento geografico dei popoli con il ripristino dei confini non solo nazionali ma anche locali; dall'altro l'affidamento straordinario delle attività, della condivisione dei dati scientifici, della ricerca di soluzioni, dei dialoghi decisori internazionali al Web che opera in uno spazio senza confini e senza tempo. Internet esprime il paradosso di garantire la continuità dei contatti planetari di una società che oggi, per sopravvivere, è priva di contatti reali (contactless). La pandemia ha dimostrato la possibilità di organizzare diversamente il lavoro in tutti i settori che non richiedono la presenza fisica, con notevoli vantaggi diretti e indiretti sulle economie di scala delle imprese e della società nel suo complesso, sulla qualità della vita, sugli impatti ambientali, sull'organizzazione delle famiglie e sui rapporti con la burocrazia. Terminata l'emergenza, per valutare, selezionare e stabilizzare i veri vantaggi ottenibili, sarà necessario un deciso impegno nell'adeguamento delle normative, degli assetti organizzativi aziendali e nel cambio del modo di percepire i propri ruoli nei rapporti di lavoro e con le altre attività sociali. ▮