TeLex Anie
NOVITÀ LEGISLATIVE E GIURISPRUDENZIALI

Segnalazioni giuridiche a cura del Servizio Centrale Legale

N. 4 Anno XXV
Aprile 2020

INDICE:

negli accordi fra imprese ma può essere impiegata tra le imprese e i privati (o i liberi professionisti);

b) non è previsto un obbligo di riconoscimento dei documenti firmati con SPID al di fuori dell'Italia. Pertanto i documenti così sottoscritti saranno oggetto di autonoma valutazione da parte degli Stati Membri in cui si vuole usare il documento informatico firmato con questa soluzione SPID.

Avv. Gian Marco Rinaldi
Studio Legale Bird & Bird

PRIVACY

LA GESTIONE DEI BIG DATA IN TEMPO DI PANDEMIA

In tempi di emergenza appare inevitabile per tutti percepire un notevole mutamento dei valori primari e delle esigenze quotidiane: beni e diritti che prima apparivano scontati ora non lo sono più. La salute, la sicurezza e la salubrità degli ambienti (art. 32 Cost.), i medicinali, il cibo, la libertà personale (art. 13 Cost.) e la libertà di spostarsi (art. 16 Cost.), sono ritornati ad essere qualcosa da raggiungere.

A ben pensarci, però, tutti questi valori sono da sempre stati costituzionalmente garantiti e, solo con l'avvento del COVID-19, sono stati rimessi in discussione.

Un punto su cui si sta discutendo parecchio in questi giorni e che riguarda in modo inscindibile i valori costituzionali di cui sopra e la privacy, è la possibilità di utilizzare delle soluzioni tecnologiche *data driven* per affrontare l'emergenza sanitaria, sociale ed economica legata alla diffusione del virus sul territorio italiano.

Nel dettaglio, è stato attivato un gruppo di esperti scelti in collaborazione con il Ministero della Salute, l'Istituto Superiore della Sanità e l'Organizzazione Mondiale della Sanità, alcuni dei quali sono stati direttamente designati dall'AGCM, AGCOM e dal Garante per la protezione dei dati personali.

Il tema dell'organizzazione dei processi di raccolta ed elaborazione di una grossa mole di dati anche attraverso la stretta collaborazione da parte di queste autorità negli anni scorsi non era passato inosservato e, data l'emergenza che si sta sviluppando, si sta rafforzando sempre più.

Già il 30 maggio 2017, infatti, AGCOM, AGCM e il Garante Privacy hanno avviato un'indagine conoscitiva sui big data volta ad approfondire la conoscenza degli effetti prodotti dal fenomeno dei Big Data e ad analizzarne le conseguenze in relazione all'attuale contesto economico- politico-sociale e al quadro di regole in vigore.

Lo scorso mese di febbraio, poi, a chiusura della predetta indagine, le tre Autorità coinvolte hanno riportato i risultati e le conclusioni della stessa.

Di seguito, partendo dalle considerazioni effettuate dal Garante Privacy nell'elaborato in questione, un breve focus su quanto emerso: la materia della protezione dei dati personali si pone, infatti, per la trasversalità che la caratterizza, come punto di incrocio necessario rispetto a tutti gli ambiti interessati da questo fenomeno.

Le attività legate all'utilizzo dei *Big Data* possono evidenziare chiari profili di contrasto con aspetti fondamentali della disciplina di protezione dei dati con riferimento ai principi di liceità e correttezza nel trattamento, aspetto quest'ultimo che rinvia ad una effettiva (e compiuta) consapevolezza degli interessati (e correlativa trasparenza dei titolari del trattamento) circa le operazioni connesse all'utilizzo dei dati personali che li potrà riguardare, al rispetto del principio di finalità e alla corretta individuazione della base giuridica posta a fondamento di tali operazioni di trattamento.

Le informazioni rese agli interessati, del resto, vanno ad integrare esse stesse una componente "concorrenziale" rispetto al trattamento posto in essere dai singoli titolari del trattamento, ben potendo orientare le scelte di quanti vedono le informazioni a sé riferite coinvolte nel trattamento (così dando attuazione al diritto all'autodeterminazione informativa), non diversamente dalle informazioni contenute sulle etichette e dai documenti informativi che i consumatori consultano prima di procedere all'acquisto di beni di consumo.

Fornire una corretta informativa è il pre-requisito per un valido consenso al trattamento dei dati (che, per l'appunto, si vuole informato), ove lo stesso sia necessario. Consenso al trattamento che non comporta alcuna "cessione" di dati personali, neanche quando acceda alla fruizione di servizi "gratuiti"; il diritto alla protezione dei dati personali, infatti, consiste anzitutto nel potere dell'interessato di controllare l'uso che dei dati personali a sé riferiti viene fatto in relazione alle finalità per le quali i dati sono (legittimamente) trattati.

Un altro tema su cui si è concentrato il Garante è la necessità da parte di chi tratta *Big Data* di adottare misure preventive e processi interni volti a commisurare il rischio sui diritti degli interessati (che possono determinare anche l'adozione di decisioni individuali sulla base di analisi "predittive").

In questa prospettiva ha considerato necessario svolgere una valutazione d'impatto sulla protezione dei dati, così come prevista dall'art. 35 GDPR, cui, con alta probabilità, devono essere sottoposti i trattamenti di dati

posti in essere con la tecnica dei *Big Data*, in particolare con riguardo ai casi in cui il trattamento comporti "*una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche*" (cfr. art. 35, par. 3, lett. a).

Le conclusioni tratte a seguito dell'analisi del fenomeno dal punto di vista della privacy sono le seguenti:

- per regolamentare il tutto risulta necessaria la cooperazione rafforzata e l'interlocuzione con altri soggetti istituzionali, ad iniziare dalle autorità indipendenti di settore cui sono rimessi poteri di vigilanza e regolatori (si pensi già solo ai settori assicurativo, bancario, finanziario, energetico ecc.);
- la necessità di profili professionali (cd. *data scientist*) che possano operare nel contesto dei *Big Data*, anche presso le autorità di controllo, per assicurare la qualità dell'attività di ricerca svolta;
- le competenze di tali figure professionali non possono prescindere da un'adeguata considerazione dei profili etici e giuridici (anzitutto con riguardo alle discipline di protezione dei dati personali) che tali trattamenti implicano.

Adottando le soluzioni finali proposte, quindi, la finalità ultima degli articolati processi sottesi all'utilizzo di Big Data vuole essere, in termini generali, quella di accrescere l'efficienza dei processi produttivi, migliorare la capacità decisionale dei soggetti che ne usufruiscono e prevedere più accuratamente le tendenze comportamentali degli individui oggetto di analisi sia in campo economico, medico, scientifico o, come nel caso attuale, emergenziale.

Avv. Vittoria Piretti
Studio Legale Stefanelli

PRIVACY&AI AI TEMPI DEL CORONAVIRUS: RIFLESSIONI SU GEOLOCALIZZAZIONE E SISTEMI PREDITTIVI

L'epidemia Covid-19 ha puntato ancora di più i riflettori su i due temi più caldi del 2020: Intelligenza Artificiale e privacy.

Ad un mese di distanza dal lancio della politica europea sull'Intelligenza Artificiale, l'Europa si trova ad affrontare una sfida cruciale, che definirà senza dubbio le politiche future.

In un battito di ciglia abbiamo visto fiorire articoli ed interviste in cui "la privacy" viene trattata come un concetto totalmente astratto, da dover sacrificare in modo assoluto per permettere il raggiungimento di un obiettivo comune. Siamo costantemente bombardati da notizie dove viene chiesto di scegliere tra privacy e tecnologia, privacy e salute, privacy e sicurezza, come se una escludesse per forza l'altra. Allo stesso tempo, si susseguono notizie sulla creazione di applicazioni e altri sistemi informatici basati sull'Intelligenza Artificiale dedicati al monitoraggio dei contagi.

Il diritto alla privacy altro non è che il diritto alla riservatezza, un diritto fondamentale collegato alla nozione della dignità umana: comporta il diritto di ognuno ad avere una vita privata, senza interferenze illecite. È distinto, seppur collegato, dal diritto alla protezione dei dati, che ha come obiettivo assicurare che le informazioni relative ad un soggetto vengano trattate correttamente. Il GDPR rappresenta il cuore della disciplina europea relativa al trattamento dei dati personali.

Ciò posto, come per altri diritti e libertà, è possibile che in situazioni determinate i diritti individuali alla **privacy** e alla **data protection** vengano "limitati" come risultato di un bilanciamento con altri diritti aventi portata pubblica, come nel caso della salute. Tuttavia, qualsiasi deroga di questo tipo deve trovare la sua base in una fonte legittima, che preveda i limiti e la proporzionalità della deroga allo scopo perseguito.

In questo senso si è anche espresso il Garante Italiano, Antonello Soro:

Non è vero che la privacy è il lusso che non possiamo permetterci in questo tempo difficile, perché essa consente tutto ciò che è ragionevole, opportuno e consigliabile fare per sconfiggere il coronavirus. La chiave è nella proporzionalità, lungimiranza e ragionevolezza dell'intervento. Oltre che nella sua temporaneità.

In questo articolo quindi cercheremo di fare un po' di chiarezza sugli aspetti di **data protection** più rilevanti relativi all'applicazione di un sistema di IA in questo particolare periodo storico.

In particolare, ci occuperemo dello sviluppo di sistemi di IA per effettuare attività di screening, **contact tracing** e di valutazione del rischio di infezione. Riassumeremo anche gli ultimissimi criteri emanati dal Garante relativamente alla geolocalizzazione dei contagiati da coronavirus.

Possiamo individuare due aspetti chiave relativi all'applicazione di AI per combattere l'epidemia da Corona virus:

1. trasparenza sulle modalità di trattamento e corretta informazione degli interessati.
2. temporaneità, proporzionalità e accuratezza del trattamento dei dati;

Trasparenza sulle modalità di trattamento e corretta informazione degli interessati: le norme del GDPR relative all'IA

Nel caso in cui il trattamento sia il risultato di un processo decisionale automatizzato (all'interno del quale rientrano i trattamenti effettuati tramite l'utilizzo tecnologie di Intelligenza Artificiale) il GDPR impone requisiti obblighi informativi e di trasparenza ulteriori che devono essere necessariamente rispettati.

In particolare, l'art. 13 (2) lett. f) prevede che l'interessato debba essere informato circa

*"l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo […] e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato***".**

Inoltre, secondo l'articolo 15 (1) lett. h) GDPR l'Utente ha il diritto di ottenere dal Titolare le informazioni contenute all'art. 13 (2) lett. f) di cui sopra.

Infine, l'articolo 22 GDPR prevede che:

1. *L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.*
2. *Il paragrafo 1 non si applica nel caso in cui la decisione:*
   a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
   b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
   c) si basi sul consenso esplicito dell'interessato.
3. *Nei casi di cui al paragrafo 2, lettere a) e c),il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.*

L'interessato, pertanto, deve essere in grado di esprimere il proprio consenso al trattamento dei dati in modo consapevole, il linguaggio utilizzato deve essere immediato e chiaro, in particolar modo poiché si tratta nella maggior parte di casi di raccolta di dati tramite app installate su smartphone personali.

L'informativa deve sempre essere il risultato di un bilanciamento da parte di colui che diffonderà al pubblico il software: da un lato vi è il diritto dell'interessato a ricevere informazioni più accurate possibili e dall'altro l'esigenza di semplificare concetti complessi e di costruire la fiducia degli interessati nella tecnologia, visto l'impatto che potrebbe avere sul loro benessere psicofisico.

Temporaneità, proporzionalità e accuratezza del trattamento dei dati: i criteri da seguire per la geolocalizzazione dei contagiati dal coronavirus previsti dal Garante italiano

In un'intervista ad Agenda Digitale del 29 Marzo 2020 il Garante italiano ha delineato i criteri che devono essere seguiti da parte di governi per poter utilizzare un software per la geolocalizzazione di soggetti positivi al fine di analizzare l'andamento epidemiologico del Covid-19 o per ricostruire la catena dei contagi.

- Gradualità: il governo deve innanzitutto valutare se soluzioni meno invasive possano essere sufficienti a fini di prevenzione;
- Viene permessa l'acquisizione di trend anonimi di mobilità;
- Se il governo invece intende acquisire dati identificativi è necessario innanzitutto che venga **emanata una previsione normativa ad efficacia temporalmente limitata, dotata di adeguate garanzie.** In particolare viene evidenziata la necessità che questa normativa sia conforme al principio di proporzionalità, analizzando in particolare lo scopo della raccolta dei dati;
- Il Governo deve poi condurre **un'analisi preliminare dell'effettiva idoneità della soluzione tecnologica scelta** a conseguire risultati utili nell'azione di contrasto, in ordine proporzionale alle esigenze perseguite e sempre che misure meno invasive non debbano ritenersi idonee a conseguire i risultati sperati
- Il Garante poi **ha stabilito che l'elaborazione dei dati relativi alla geolocalizzazione degli individui debba essere per forza essere collegata** al dato sanitario relativo alla positività o meno dei soggetti tracciati**.**

Per quanto attiene ai soggetti privati che elaboreranno il software, il Garante ha stabilito che**:**

- I soggetti privati gestori delle infrastrutture tecnologiche dovrebbero essere in grado di **porre il patrimonio informativo di cui dispongono a disposizione dell'autorità pubblica;**
- All'autorità pubblica dovrebbe essere riservata la fase dell'analisi dei dati (e dell'eventuale reidentificazione di questi). Questo è dettato dal maggiore rischio che quest'attività comporta, che può trovare garanzie adeguate negli organi statali.

- **Le società coinvolte nel progetto devono possedere idonei requisiti di affidabilità e trasparenza di azione**.

L'intervento del Consiglio d'Europa

In data 30 marzo 2020 il Chair of the Committee of Convention 108 e il Data Protection Commissioner del Consiglio d'Europa sono intervenuti i con una dichiarazione congiunta relative al trattamento dei dati nell'ambito del contrasto alla diffusione del COVID-19.

Per quanto riguarda nello specifico l'utilizzo di software di IA, nello statement vengono indicate i seguenti punti chiave da tenere in considerazione nella fase di sviluppo di sistemi predittivi:

- Trasparenza e "**explainability**" dell'analisi tecnica svolta dall'IA;
- Approccio precauzionale e una strategia di gestione del rischio (compreso il rischio di ri-identificazione nel caso di dati anonimi)
- Qualità e minimizzazione dei dati;
- Il ruolo della supervisione umana.

Conclusione

È assolutamente possibile lo sviluppo di tecnologie avanzate senza che vengano erosi inevitabilmente i diritti degli individui alla data protection e alla riservatezza. Anzi, è necessario - in una situazione di emergenza come questa - che tali tecnologie vengano utilizzate per il bene comune.

L'intervento umano è fondamentale: è tramite questo che vengono infatti delineate le caratteristiche del software che poi opereranno di default il software stesso verrà utilizzato dagli interessati.

Per questo motivo è necessario che gli operatori del mercato sappiano come orientarsi all'interno della normativa sulla privacy e sulla data protection in un momento delicato come questo.

Fonti:

- Coronavirus is forcing a trade-off between privacy and public health, Karen Hao, MIT Technology Review
- The Public Interest and Personal Privacy in a Time of Crisis, Hu Yung

Avv. Silvia Stefanelli, Avv. Alice Giannini
Studio Legale Stefanelli

DIRETTORE RESPONSABILE
Maria Antonietta Portaluri

REDAZIONE
Alessandra Toncelli – Mirella Cignoni

LA REDAZIONE RINGRAZIA PER LA COLLABORAZIONE

Avv. Gian Marco Rinaldi, Studio Legale Bird & Bird - Avv. Mariaelena Giorcelli, BBM Partners, Buffa, Bortolotti & Mathis - Avv. Riccardo G. Cajola, Cajola & Associati - Avv. Dario Paschetta e Avv. Mariagrazia Berardo, Studio Legale Frignani Virano e Associati - Avv. Alessandra Boiano, Avv. Michele Franzosi, Avv. Alice Garlisi, Avv. Mirko Maggioni, Avv. Alessandro Raffaelli e Avv. Elisa Teti, Studio Legale Rucellai & Raffaelli (Milano – Roma – Bologna)- Avv. Silvia Stefanelli, Avv. Alice Giannini e Avv. Vittoria Piretti, Studio Legale Stefanelli.

Proprietario ed editore:
Federazione ANIE
Viale Lancetti 43, 20158, MI
Telefono (02) 3264.1
Direttore Responsabile
Maria Antonietta Portaluri
Registrazione del Tribunale
di Milano al n° 116 del
19/2/1996

TeLex Anie

FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE
CONFINDUSTRIA

Pubblicazione a cura di:
Servizio Centrale Legale
Viale Lancetti 43, 20158, MI
Telefono (02) 3264.246
e-mail legale@anie.it
Diffusione via web www.anie.it