Lecce, 25 marzo 2020

Egregio Presidente del Consiglio dei Ministri, Giuseppe Conte
On. Ministro per l'Innovazione tecnologica e la digitalizzazione, Paola Pisano
On. Ministro dello Sviluppo Economico, Stefano Patuanelli
On. Ministro dell'Università e Ricerca Gaetano Manfredi
Ill.mo Garante per la protezione dei dati personali, Antonello Soro
Ill.mo Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica COVID-19, Domenico Arcuri
Spett.le Agenzia nazionale per lo sviluppo, Invitalia

Si discute in queste ore dell'opportunità di tracciare gli spostamenti dei cittadini tramite l'introduzione, in ambito nazionale, di soluzioni informatiche, in analogia con l'esperienza sudcoreana. In qualità di giuristi che da anni si occupano concretamente delle delicate materie afferenti alla protezione dei dati personali, percepiamo un significativo rischio di derive e utilizzi gratuiti.

Ci permettiamo sommessamente di richiamare, in questa lettera, alcuni principi fondamentali,

Il bilanciamento tra diritto alla salute e diritto alla protezione dei dati personali

È stato già correttamente evidenziato sia a livello istituzionale (es. EDPB, *Statement* del 19 marzo 2020) sia in dottrina (cfr. *Pizzetti, Bolognini, Lisi, Sarzana, Nicotra, Iaselli e altri*) che il "GDPR" (Regolamento UE 2016/679) così come la Direttiva cd. "ePrivacy" (Direttiva 2002/58/CE) consentono di costruire il *bilanciamento* tra diritto alla salute e diritto alla protezione dei dati personali in modo da assicurare la prevalenza del primo sul secondo. Diciamolo in termini ancora più diretti: **la protezione dei dati personali non si pone come un ostacolo** alle iniziative necessarie per la tutela dalla salute pubblica.

Digital & Law Department S.r.l.
Segreteria Organizzativa
Via Vito Mario Stampacchia n°21 – 73100 Lecce
Tel. e fax: 0832-256065
E-mail: info@digitalaw.it – P.E.C.: digitalaw@pec.it
C.F. e P.IVA: 04372810756

Tuttavia, questo non implica **"dare carta bianca" a qualsiasi soluzione di tracciamento informatico dei cittadini** purché connessa con il contenimento dell'emergenza sanitaria in corso.

Il coordinamento tra politica di contrasto e raccolta di informazioni su scala nazionale

È importante anzitutto chiarire **i benefici reali e gli obiettivi sanitari attesi**. Nel *case study* asiatico coesistono una pluralità di applicazioni informatiche, alcune con **finalità di prevenzione, nei confronti di chi si sposta, altre di repressione, nei confronti di chi è in quarantena**.
Concentriamoci sulle prime, che sono coordinate in maniera strutturale e necessaria con la politica di contrasto del virus attuata in Sud Corea, che differisce attualmente dalla nostra. Quel sistema si basa infatti su una strategia di **tamponi a tappeto** e su una quarantena **limitata ai soli soggetti risultati positivi**, non già estesa all'intera popolazione, il che incidentalmente ha enorme significato sia in termini di libertà individuale, non completamente compressa da misure draconiane, sia in termini di economia, non del tutto paralizzata, e dunque di sostenibilità nel tempo. Non si bloccano cioè milioni di persone a casa (come in Cina).

In mancanza di questi due elementi cruciali (tamponi a tappeto e circolazione non del tutto ristretta dei soggetti negativi) non si comprende il senso dell'introduzione di un'applicazione informatica per la prevenzione di nuovi contagi. Il soggetto negativo al tampone, relativamente libero di circolare, potrebbe infatti positivizzarsi attraverso il contatto casuale con persone risultate positive o con luoghi da queste frequentati di recente (il virus ha un tempo limitato di sussistenza su oggetti, (cfr. per es. AA.VV., *Aerosol and Surface Stability of SARS-CoV-2 as Compared with SARS-CoV-1*, in *The New England Journal of Medicine*, 17.3.2020).

Di qui la ragione che rende *necessaria* un'applicazione informatica che permetta di ricostruire retrospettivamente lo storico recente degli spostamenti dei soggetti positivi, avvertendo tempestivamente i frequentatori delle stesse aree. Senza una campagna di tamponi a larghissimo raggio e comunque in presenza di un *lockdown* completo, come quello a cui l'Italia sempre di più tende, l'app perde cioè di significato. **La soluzione informatica sudcoreana si basa dunque su un contesto e un concetto completamente diversi da quelli attualmente praticati in Italia**.

Ci chiediamo pertanto, alla luce di tali considerazioni, quale potrà invece mai essere il senso di ricostruire retrospettivamente il percorso di milioni di persone, se poi la conoscenza di tale informazione è resa inutile dalla mancanza del dato relativo ai test. Verrebbe svolta cioè una

raccolta di informazioni altamente personali e sensibili su scala nazionale in modo assolutamente *ultroneo*.

[Pur nella difficoltà di ricostruire i dettagli esatti delle politiche attuate, l'analisi della situazione sudcoreana si basa su una serie di fonti giornalistiche, compreso le seguenti: *Max Fisher*, *How South Korea Flattened the Curve*, in *New York Times*, 23.3.2020; Will Bedingfield, *What the world can learn from South Korea's coronavirus strategy*, in *Wired Magazine* (ediz. UK), 21.3.2020, Max S. Kim, *South Korea is watching quarantined citizens with a smartphone app*, in *MIT Technology Review*, 6.3.2020].

Altre finalità di trattamento diverse da quella di prevenzione

Tornando alle funzionalità di un'applicazione informatica, si noti che perfino ove lo scopo fosse uno studio *a posteriori* – ma, attenzione, è finalità diversa da quella precedentemente analizzata e tutta da bilanciare –, sarebbe corretto circoscriverlo a campioni e aree delimitate, anziché all'intera popolazione nazionale.

Se invece l'applicazione italiana fosse progettata solo con l'intento di svolgere attività di polizia/repressiva, dunque per finalità solo *indirettamente* sanitaria, corrispondente alla seconda tipologia impiegata in Corea (ma a quanto pare, comunque installata su *base volontaria*, cfr. ult. art. cit.), ci pare che il trattamento non superi criteri di gradualità e proporzionalità.
Si tratta di un'attività che è già egregiamente svolta dalle forze dell'ordine, senza avvertire l'esigenza di un "Grande Fratello" orwelliano.
Il disallineamento individuale rispetto alle prescrizioni, non ha assunto dimensioni tali da renderlo incontrollabile con strumenti tradizionali. Più esattamente, come del resto correttamente evidenziato dal Presidente Soro, **sussistono fondati e validi motivi di legge che rendono perfettamente lecita la mobilità di migliaia di italiani**: dall'attività motoria consentita (nonostante la *vulgata* popolare), allo spostamento per ragioni di lavoro, a quello per ragioni sanitarie o alimentari.
Dunque, il mero dato del movimento da un luogo a un altro non è di per sé significativo, mentre il suo incrocio con il contenuto delle autocertificazioni (pur possibile) non siamo sicuri che rappresenti il modo migliore di assicurare l'osservanza delle prescrizioni.

È stato ampiamente osservato dalle parti sociali che il punto critico della situazione **non va ravvisato tanto nello spostamento in sé quanto nelle modalità con cui è svolto**, così come per l'organizzazione dell'attività lavorativa. Le doglianze riguardano spazi che non sempre assicurano distanziamento, insufficienza di DPI, carenza di tamponi regolari che possano escludere la presenza di positivi asintomatici, a tutela dei colleghi e di terzi.

Infine, si è parlato perfino di un utilizzo dell'applicazione per segnalare gli orari di minor affollamento di supermercati e mezzi pubblici: non comprendiamo come tutto ciò richieda un

tracciamento individuale, infatti gli stessi obiettivi possono essere raggiunti altrimenti e in modo non invasivo. **I principi di gradualità e proporzionalità – va notato – prima ancora di essere regole di diritto appaiono esigenze di buonsenso**.

Un'esperienza inedita nelle democrazie occidentali

Ci piacerebbe dunque, secondo l'ordine logico delle cose, conoscere, prima ancora della notizia relativa allo sviluppo applicazioni informatiche, **quali siano le esatte finalità** per cui vengono progettate e quale sia il rapporto con il programma di contrasto all'epidemia, punto quest'ultimo che nel caso di scuola sudcoreano appare assai chiaro, nostro malgrado.
Si ritiene fondamentale evitare iniziative che, pur lastricate da ottime intenzioni, si traducano in attività di monitoraggio gratuite rispetto a una platea di interessati corrispondente addirittura all'intera popolazione nazionale e peraltro prive di precedenti – leciti – nell'esperienza delle democrazie occidentali.
È appena il caso di notare la profondità del tracciamento sulle vite individuali, le infinite possibilità di incrocio dei dati, il potenziale stigma sociale collegato alla raccolta, gli effetti duraturi sulla psicologia dei monitorati, le conseguenze nel caso di *personal data breach*, il pericolo rappresentato anche, e non da ultimo, dalla **normalizzazione sociale di un monitoraggio di Stato condotto a tale livello di pervasività**.
Rischiamo cioè di coltivare quello che domani sarà un frutto avvelenato.

La valutazione d'impatto e il rispetto delle esigenze di trasparenza, buona fede e correttezza

Le considerazioni appena esposte non intendono sminuire il peso derivato da circostanze *estreme*, ma rispetto alle relative misure di contrasto ci piacerebbe poter consultare quantomeno un **DPIA**, ossia una **valutazione d'impatto**. Si tratta di un adempimento obbligatorio e riteniamo peraltro corretto che il documento di analisi venga reso pubblico in ragione di esigenze di trasparenza, buona fede e correttezza.
La valutazione d'impatto dovrebbe chiarire punti essenziali quali il perimetro di accessi e di circolazione dei dati, la durata della conservazione, la localizzazione per area geografica dei *data center*, le policy di sicurezza applicate (almeno per *estremi essenziali*, per evitare compromissioni di sicurezza), le linee guida dell'ENISA applicate e soprattutto se e quali tecniche di anonimizzazione su base matematico-statistica tra quelle enunciate nella opinione 5/2014 dell'*ex* Gruppo di lavoro 29 (es. *k-anonymity*) siano state seguite.

Ci ha colpito, non positivamente, il fatto che tutte queste questioni abbiamo trovato scarsa evidenza non solo nel dibattito pubblico, ma soprattutto in quello istituzionale.

Inoltre, ci piacerebbe essere rassicurati sul fatto che il team che sta lavorando in queste ore all'applicazione (di cui si ignora la composizione e forse sarebbe preferibile garantire trasparenza in tal senso) stia seguendo, come per legge, un rigoroso approccio di *privacy-by-design*, che cioè stia costruendo il prodotto informatico integrando fin dalla progettazione la massima tutela per i dati personali **e non si ponga invece solo a prodotto ultimato il problema del dialogo con i diritti fondamentali coinvolti**. Sarebbe anche estremamente opportuno, per ragioni di trasparenza, che il codice fosse *open source* e che si facesse uso, se del caso, di librerie ugualmente *open source*. Le librerie informatiche utilizzate andrebbero inoltre verificate per escludere che non comportino flussi di dati a soggetti terzi non autorizzati (non sarebbe la prima volta).

In conclusione, gli scriventi caldeggiano che l'introduzione di un'applicazione informatica di tracciamento dell'intera popolazione si incastri in modo necessario e logico, non casuale e periferico, con il programma sanitario da attuare. L'applicazione deve cioè costituire un'***extrema ratio*** e tradursi in un esercizio di autorità.

Ci piacerebbe dunque, questo è il senso della presente lettera aperta, conoscere il dettaglio dei punti sopra accennati, in modo che l'iniziativa informatica in programma sia il più possibile pubblica e condivisa, supportata da una precisa e trasparente dichiarazione delle finalità.

Rispettosamente

Avv. Andrea Lisi e Avv. Enrico Pelino

Digital & Law Department S.r.l.
Segreteria Organizzativa
Via Vito Mario Stampacchia n°21 – 73100 Lecce
Tel. e fax: 0832-256065
E-mail: info@digitalaw.it – P.E.C.: digitalaw@pec.it
C.F. e P.IVA: 04372810756

Condividono e sottoscrivono il presente documento

Luca Bolognini, *avvocato - Presidente dell'Istituto Italiano per la Privacy e la Valorizzazione dei Dati*
Franco Cardin, *esperto privacy - Presidente Commissione di Valutazione di ANORC Professioni*
Giovanni Crea, Componente del Comitato tecnico-scientifico di ANORC Professioni
Luigi Foglia, *avvocato – Segretario generale ad interim di ANORC*
Diego Fulco, *avvocato - Direttore del Comitato Scientifico d'istituto italiano privacy*
Luciana Grieco, *avvocato esperto in protezione dei dati personali*
Michele Iaselli, *avvocato - Presidente dell'Associazione Nazionale per la Difesa della Privacy (ANDIP)*
Donato A. Limone, *Professore Ordinario di Informatica Giuridica e docente di Scienza dell'Amministrazione digitale presso Unitelma Sapienza*
Daniele Minotti, *avvocato - esperto in diritto penale delle nuove tecnologie*
Massimiliano Nicotra, *avvocato, Docente presso Università di Roma Tor Vergata*
Gianni Penzo Doria, *Direttore dell'Archivio di Stato di Venezia*
Roberto Scano, *esperto per la normazione e diffusione delle competenze digitali - Presidente IWA Italy - International Web Association Italia*
Sarah Ungaro, *avvocato e Vicepresidente di ANORC Professioni*