

LA PRIVACY AI TEMPI DEL CORONAVIRUS

Secondo un giovane Ludwig Beck, oppositore di Hitler e congiurato, *“Tempi straordinari richiedono misure straordinarie”*.

La celebre citazione è stata recentissimamente ripresa da Christine Lagarde, Presidente della Banca Centrale Europea, per parlare delle misure economiche e valutarie che verranno adottate dall'Unione Europea per affrontare la crisi causata dal diffondersi del Coronavirus.

Misure straordinarie vengono oggi adottate non solo in materia economica, ma anche in tutti gli altri settori della nostra vita quotidiana: assistiamo così quotidianamente ad un clamoroso -e spesso autoimposto- ridimensionamento delle nostre libertà individuali e collettive e ad una graduale smaterializzazione dei rapporti interpersonali, professionali e non, che si sono repentinamente trasformati in contatti a distanza (tra call-conferenze lavorative ed aperitivi in video-chat).

Ad essere oggetto di una fortissima compressione è anche il ns. diritto alla privacy, o meglio il diritto alla protezione dei nostri dati personali.

Come noto, infatti, alcune delle strategie dimostrate più efficaci nel combattere la diffusione del Coronavirus sono basate proprio sulla quasi completa eliminazione di libertà individuali e collettive ed un controllo capillare e totale delle attività dei cittadini, complice anche una concezione già in partenza più limitata di tali diritti.

Le cronache riportano che in Cina i cittadini delle zone colpite dal virus (in particolare la provincia di Hubei) sono stati sostanzialmente “tumultuati” nelle proprie abitazioni, costantemente controllati da esercito e forze dell'ordine; i contagiati, poi, erano immediatamente analizzati e trasportati presso centri statali, ove venivano ricoverati fino alla completa guarigione.

In Corea del Sud si è fatto invece ampio uso delle più moderne tecnologie, al fine di controllare meticolosamente tutti i cittadini: sono stati anzitutto effettuati accertamenti a tappeto tramite tamponi (con *“stazioni mobili per il test, visite nelle abitazioni e punti di controllo in strada agli automobilisti”* - fonte Agi) e si è poi provveduto a tracciare gli spostamenti dei positivi mediante i GPS degli smartphone, mettendo questi dati *“a disposizione dei cittadini per far sì che ognuno di loro potesse sapere immediatamente se e quando aveva incrociato la strada di un possibile contagiato.”* (fonte Corriere della Sera). Addirittura, i dati degli spostamenti dei contagiati sono stati utilizzati per creare mappe, verificare il rispetto della quarantena ed allertare (e controllare) i soggetti negativi che erano venuti a contatto con i positivi.

Questi modelli hanno così comportato la totale perdita della privacy dei comuni cittadini (sani e contagiati).

Anche in Italia sono stati imposti (dal virus e dalle misure governative) importanti cambiamenti nel nostro concetto di privacy e protezione dei dati personali, pur senza raggiungere gli estremi a cui abbiamo accennato.

Molte delle misure straordinarie adottate nel nostro Paese (controllo con tamponi, verifica della temperatura sui luoghi di lavoro, smart-working, autocertificazioni per poter circolare, utilizzo di applicazioni per la geolocalizzazione ed il tracciamento degli spostamenti e paventato utilizzo di

droni) comportano infatti palesi e rilevanti conseguenze sotto il profilo del trattamento dei dati personali.

I giuristi che si occupano della materia devono pertanto porsi quotidianamente alcune faticose domande: cosa è lecito? fino a dove si possono spingere il datore di lavoro, la forza pubblica, il governo, nella limitazione del diritto alla privacy? come possono essere inquadrare giuridicamente (e, talvolta, giustificate *ex post*), tali misure? quali cautele e strumenti occorre adottare nel trattamento dei dati personali conseguente alle misure?

In una recentissima intervista (La Stampa del 25/03/2020), il Garante per la Protezione dei Dati Personali Antonello Soro si è espresso su alcune delle questioni poste sopra, chiarendo che in un momento drammatico come quello attuale anche il diritto alla privacy può “*soggiacere a delle limitazioni a fronte di un interesse collettivo*”, ed ha di conseguenza aperto persino alla possibilità di “*tracciamento precoce dei positivi e delle persone che sono venute a contatto con loro, oltre che un controllo sul rispetto della quarantena*” sul modello coreano, pur rappresentando l’assoluta necessità di cautele e termini temporali nel trattamento.

Possiamo qui brevemente accennare al trattamento giuridico -in applicazione della normativa comunitaria e nazionale sul diritto della protezione dei dati personali- di alcuni istituti particolarmente interessanti al tempo del Coronavirus.

L’obiettivo generale deve essere naturalmente quello di cercare di rispettare le norme (seppur “stressandole”) pur in un momento straordinario.

A necessitare un approfondimento è anzitutto la legittimità delle operazioni di trattamento dei dati personali svolte dalla Pubblica Amministrazione, dal personale sanitario e dalle forze dell’ordine.

Sul punto, l’art. 14 del D.L. 14/2020 -rubricato “*Disposizioni sul trattamento dei dati personali nel contesto emergenziale*” ha concesso rilevanti poteri ai soggetti impegnati nella lotta al Coronavirus, permettendo “*Fino al termine dello stato di emergenza ... per motivi di interesse pubblico nel settore della sanità pubblica ... i soggetti operanti nel Servizio nazionale di protezione civile, ..., nonché gli uffici del Ministero della salute e dell’Istituto Superiore di Sanità, le strutture pubbliche e private che operano nell’ambito del Servizio sanitario nazionale e i soggetti deputati a monitorare e a garantire l’esecuzione delle misure disposte ai sensi dell’articolo 3 del decreto-legge 23 febbraio 2020, n. 6 ... possono effettuare trattamenti, ivi inclusa la comunicazione tra loro, dei dati personali, anche relativi agli articoli 9 e 10 del regolamento (UE) 2016/679, che risultino necessari all’espletamento delle funzioni attribuitegli nell’ambito dell’emergenza determinata dal diffondersi del COVID-19.*”

In ogni caso, secondo il comma 3 del medesimo articolo, tali trattamenti dovranno essere “*effettuati nel rispetto dei principi di cui all’articolo 5 del citato regolamento (UE) 2016/679, adottando misure appropriate a tutela dei diritti e delle libertà degli interessati.*”

Di conseguenza, ad esempio, le forze dell’ordine sono legittimate a richiedere l’autocertificazione necessaria per la circolazione (contenente anche dati personali particolari ex art. 9 GDPR, riferiti alla salute del cittadino) e con la nota del 18/03/2020 la Polizia di Stato ha imposto di utilizzare moduli cartacei, escludendo la possibilità di usare app telematiche di soggetti terzi perché metterebbero -anche- a rischio la privacy dei cittadini.

Altri elementi di interesse della nostra breve analisi riguardano il trattamento dei dati personali nell’ambito lavorativo e professionale.

Particolare rilevanza, ad esempio, assume il controllo della temperatura effettuato dal datore di lavoro al momento dell'accesso agli stabilimenti aziendali, che deve considerarsi un dato personale rientrante nella categoria dei dati particolari di cui all'art. 9 Regolamento Europeo 679/2016 (GDPR), per cui è normalmente previsto un divieto generale di trattamento.

Tuttavia, lo stesso art. 9 comma 2 dispone che *“il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale”*, sempre se autorizzato dal diritto dell'Unione o dello Stato membro.

Non vi è dubbio che verificare l'eventuale rischio di presenza di sintomi del Coronavirus (febbre sopra 37,5 gradi) rientri nei diritti del titolare del trattamento (il datore di lavoro) al fine di evitare rischi, ad esempio, per gli altri operatori dell'azienda.

Inoltre, l'art. 1 n. 7 lett. d) del DPCM 11/03/2020 fornisce una base normativa al trattamento, disponendo che i datori di lavoro *“assumano protocolli di sicurezza anti-contagio e, laddove non fosse possibile rispettare la distanza interpersonale di un metro come principale misura di contenimento, con adozione di strumenti di protezione individuale;”*.

La possibilità di attuare il trattamento non esclude, naturalmente, che debbano essere rispettati tutti i principi e gli oneri in capo al titolare.

Dovranno quindi essere individuati *ex ante* i soggetti preposti al rilevamento della temperatura, che dovranno essere specificamente autorizzati ed istruiti; dovrà essere conservato il dato registrato solo nel caso in cui lo stesso sia utile per la finalità perseguita (e quindi in caso sia superiore a 37,5 gradi e determini l'esclusione dallo stabilimento; dovrà essere fornita all'interessato un'ideonea informativa ex art. 13 GDPR, che indichi le finalità del trattamento (prevenzione da contagio da Coronavirus), la base giuridica (art. 9 lett. b) GDPR ed art. 1 n. 7 lett. d) DPCM 11/03/2020), dovranno essere conservati per il solo tempo strettamente necessario (ad esempio fino al termine dello stato di emergenza).

Analoghe considerazioni possono applicarsi anche alla richiesta -molto diffusa- da parte del datore di lavoro di fare firmare una dichiarazione ai visitatori dello stabilimento, che escludano di essere risultati positivi al Coronavirus o di essere venuti a contatto con soggetti positivi.

Per gli stessi motivi di cui sopra, tali dichiarazioni possono essere richieste, ma dovranno essere rispettati i principi previsti dal GDPR e dalla normativa nazionale.

Altro elemento di rilievo attinente al mondo del lavoro è la necessità di ricorrere allo smart-working, ossia il lavoro da casa, consentendo al lavoratore di trattare fisicamente al di fuori dell'ambiente aziendale -anche- dati personali.

Ciò comporta rilevanti conseguenze sulla gestione dei dati personali, atteso che la normativa impone di adottare misure *“tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio”* (art. 32 GDPR), cercando in particolare di evitare il c.d. Data Breach (artt. 33-34 GDPR); è chiaro pertanto che -pur nelle difficoltà attuali- anche presso il luogo di "lavoro domestico" il dipendente dovrebbe essere debitamente istruito ed incaricato e dovrebbero essere valutati ed adottati strumenti finalizzati a ridurre tali rischi (password alfanumerica, firewall, antivirus, ecc.).

Cambiando completamente settore, il Garante della Privacy ha poi approvato la possibilità di inviare in via telematica (mediante email, SMS e portali della pubblica amministrazione) le ricette mediche, al fine di evitare assembramenti presso gli studi medici e snellire le procedure.

E' invece in discussione l'utilizzo di droni da parte delle pubbliche amministrazioni, per cui l'ENAC ha recentemente fornito l'autorizzazione e di cui il Comune di Torino intende presto fare uso, pur

garantendo che *“Vorremmo evitare di usare i droni per controllare direttamente i cittadini”* (fonte La Stampa 24/03/2020).

A valle della ns. breve esposizione, ci sembra di poter sostenere che, almeno nel ns. Paese, si sta attualmente tentando -pur con grande difficoltà- di individuare un punto d'incontro tra la tutela della privacy di ogni cittadino e le primarie necessità di salute e sanità pubblica, limitando i diritti di ciascuno ma tenendo fermi i principi basilari e le garanzie poste a tutela del singolo individuo.

Anche per questo aspetto della nostra vita, auspichiamo dunque di poter presto ritornare alle nostre consuete abitudini.

Avv. Lorenzo Casavecchia