La *data protection* ai tempi del Coronavirus tra prevenzione dei reati e repressione del contagio

Massimo Farina
Massimo Farina PhD, Ricercatore dell'Università degli Studi di Cagliari, docente di "Diritto dell'Informatica e delle Nuove Tecnologie" e di "Informatica Forense" – Coordinatore del laboratorio ICT4Law&Forensics – DIEE/UdR CNIT, University of Cagliari.
Mail: m.farina@unica.it.

1. L'impiego della tecnologia per la prevenzione dei contagi e il controllo dei diritti

La recente e virulenta epidemia che ha gradualmente conquistato lo scenario nazionale, europeo ed internazionale rivela tutta la delicatezza degli interessi individuali e collettivi posti in gioco. Riecheggia prepotentemente, nelle difficoltà interne tese ad apprestare idonee garanzie ai contrapposti interessi, l'insegnamento dell'Alexy sul bilanciamento tra principi costituzionali e sulla teoria dei diritti fondamentali[1]. Tali insegnamenti, tuttavia, risultano di più ardua e critica applicazione alla luce del dinamismo ordinamentale, implicando necessariamente un confronto dialogico con le fonti del diritto sovranazionale e con le più recenti generazioni di diritti fondamentali. Nel corso degli ultimi anni, invero, è stata riposta a livello europeo un'attenzione crescente alla protezione dei dati personali relativi alle persone fisiche: in effetti, tanto l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, quanto l'articolo 16, paragrafo 1, del Trattato sul funzionamento dell'Unione europea stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
Ciononostante, il riconoscimento giuridico non impedisce la verificazione di nuove sfide per la protezione dei dati personali, provocate dalla rapidità dell'evoluzione tecnologica e dalla globalizzazione: in tali casi, è posto nelle mani delle istituzioni pubbliche il delicato compito del contemperamento, attraverso il sugello impresso da atti politici a contenuto variamente normativo.
Tale scenario si riespande nell'attuale momento storico, ove la tecnologia si dimostra idoneo strumento – oltre che per la tutela dei diritti fondamentali – per il controllo della popolazione[2]. Si tratta di una prassi già a lungo invalsa in diversi paesi orientali, come ad esempio la Cina, tesa a garantire l'ordine pubblico e la sicurezza. In tal caso, la peculiare forma di stato cinese ha da sempre costituito un valido supporto istituzionale per l'impiego di sistemi di videosorveglianza (ad esempio, attraverso l'impiego dei droni), di riconoscimento biometrico e geolocalizzazione, tesi ad una sorveglianza capillare e continuativa sui cittadini. Non sorprende, pertanto, la riconversione di simili strumenti per il controllo epidemiologico ed il monitoraggio delle condotte umane in questo periodo di emergenza sanitaria: si è così proceduto, ad esempio, all'impiego dei sistemi di videosorveglianza per intercettare le persone che non indossavano una mascherina, ovvero per effettuare una scansione termica contactless, così da individuare eventuali stati di alterazione febbrile.
Lo *smartphone* rappresenta lo strumento tecnologico privilegiato per l'implementazione di tali politiche pubbliche: sono state infatti create,

[1] R. ALEXY, *Teoria dell'argomentazione giuridica. La teoria del discorso razionale come teoria della motivazione giuridica*, Milano, 1998.
[2] Cfr. C. FARALLI, *Diritti e nuove tecnologie*, in *Rivista di scienze della comunicazione e di argomentazione giuridica* , 2, 2019, 43 ss; C. CASONATO, *La scienza come parametro interposto di costituzionalità*, in *Rivista AIC*, II, 2016.

d'intesa con il governo cinese, apposite applicazioni per il monitoraggio e l'attuazione delle politiche per il contenimento dell'epidemia. Tali app, in particolare, utilizzando i *big data* in possesso della sanità cinese, procedevano attraverso strumenti di Intelligenza artificiale all'identificazione dei potenziali portatori di virus, che venivano così assoggettati all'obbligo di quarantena coatta.

Il ricorso a simili misure, ed in particolare quelle relative alla geolocalizzazione, per quanto riscontratesi efficaci per la riduzione dei contagi, è attualmente oggetto di acceso dibattito a livello europeo. Nonostante le recenti posizioni adottate dall'*European Data Protection Board* sembrerebbero sopire l'acredine[3], si scorgono ulteriori criticità qualora il trattamento dei dati personali raccolti venga effettuato per finalità di prevenzione del crimine. La prospettiva non risulta invero utopica: come è noto, a seguito delle recenti misure normative nazionali sull'obbligo di quarantena, si è affermato che il mancato rispetto di tali prescrizioni possa configurare i delitti di epidemia (di cui agli artt.438 e 452 c.p., a seconda che il reato sia stato compiuto, rispettivamente, con dolo o colpa) e del più mite reato contravvenzionale di cui all'art. 650 c.p.

Lo scarso rispetto di tali misure, inoltre, sta progressivamente inducendo i vari Stati membri dell'Unione al ricorso a strumenti di controllo e monitoraggio degli spostamenti dei propri cittadini. Tale opzione, tuttavia, non si traduce esclusivamente nel trattamento di dati personali per la tutela di interessi vitali degli interessati, considerato lecito ai sensi dell'articolo 6, paragrafo 1, del Regolamento 2016/679/Ue: piuttosto, tali attività di trattamento potrebbero essere sorrette da ulteriori e differenti ragioni di ordine pubblico, da finalità di prevenzione, indagine, accertamento e perseguimento dei reati sopra citati. Simili finalità, in altri termini, legittimerebbero l'attività di monitoraggio delle competenti autorità di controllo, ai sensi della Direttiva 2016/680/Ue. Tale Direttiva, che compone assieme al coevo Regolamento n. 679 (il cd. GDPR) e alla Direttiva n. 681 (sul trattamento dei dati del codice di prenotazione delle prenotazioni aeree) le misure predisposte dal legislatore dell'Unione per assicurare una completa protezione dei dati personali, potrebbe trovare in questo particolare momento storico piena applicazione, sollevando molteplici criticità ed osservazioni, che si tenterà qui di sintetizzare.

2. La prevenzione dei reati secondo la Direttiva 2016/680/Ue

La Direttiva 2016/680/Ue inaugura un nuovo versante per l'applicazione della *data protection* nel settore della cooperazione giudiziaria e di polizia in materia penale[4]. In passato, invero, la disciplina era affidata alla competenza del Consiglio ed era sprovvista di uno strumento giuridico di portata generale nel settore in esame: per tali ragioni, a seguito delle esigenze già evidenziate nel 2005 dalla Commissione, il Consiglio emanò la Decisione quadro 2008/977/GAI: ciononostante, la Decisione quadro non ha registrato alcun significativo progresso nella realizzazione di standard e regole comuni in materia di *data*

[3] Dapprima, con lo *Statement on the processing of personal data in the context of the COVID-19 outbreak,* del 20 marzo 2020, in seguito, con le Guidelines 03/2020 *on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*, adottate il 21 aprile 2020.

[4] Per approfondimenti, cfr. G. RUGANI, *La protezione dei dati nel settore della cooperazione giudiziaria e di polizia in materia penale alla luce della direttiva (UE) 2016/680: frammentazione ed incertezze applicative*, in *Freedom, Security & Justice: European Legal Studies,*1, 2019, 75-92.

ISSN 2284-4503

protection, rivolgendosi agli Stati membri con un approccio minimalista, escludente dal proprio ambito di applicazione il trattamento dei dati svolti all'interno dei confini nazionali. Alla luce del flebile contesto normativo, pertanto, la Direttiva 2016/680/Ue apporta un notevole miglioramento, dimostrando tutto l'intento del legislatore dell'Unione di armonizzare un settore così delicato[5]. Con essa, infatti, si è proceduto all'abrogazione della Decisione quadro 2008/977/ AI e all'obbligo di recepimento, per tutti gli Stati membri, entro il 6 maggio 2018. L'Italia ha provveduto al recepimento della Direttiva attraverso il d.lgs. del 18 maggio 2018, n. 51, limitandosi ad una mera riproduzione del testo normativo di rango europeo. In ogni caso, tale scelta non esautora l'efficacia della Direttiva ed il contenuto delle sue disposizioni, che, alla luce del contesto attuale, assumono nuova colorazione.

Preliminarmente, si osserva che la Direttiva n. 680 consente il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali. Sul punto, l'art. 3 fornisce una definizione alquanto ampia di «autorità competente»,, dovendosi con ciò intendersi: «qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, salvaguardia e prevenzione di minacce alla sicurezza pubblica» ovvero «qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica». Ne discende, pertanto, che il trattamento possa esser svolto dalle autorità di pubblica sicurezza (come ad esempio dalla Polizia di Stato, ovvero dalla Polizia Postale), oltre che dalla magistratura inquirente, nonché da qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici[6].

Procedendo con la disamina della Direttiva, inoltre, si scorgono molteplici similitudini con le disposizioni contenute nel Regolamento n. 679, per quanto concerne i principi sul trattamento dei dati personali, sul rapporto tra titolare del trattamento e soggetto interessato, nonché dei diritti che quest'ultimo può far valere nei confronti del titolare per garantire la piena protezione dei propri dati. In effetti, l'articolo 12 della Direttiva corrisponde, specularmente, all'articolo 12 del Regolamento, che imprime regole di condotta per il trattamento dei dati personali, basato su canoni di trasparenza, liceità e correttezza: il titolare del trattamento, pertanto, dovrebbe comunicare al soggetto interessato tutte le informazioni relative al trattamento, in forma concisa, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Sul punto, tuttavia, la Direttiva introduce un regime derogatorio rispetto agli oneri informativi che il Regolamento attribuisce categoricamente in capo al titolare del trattamento. Viene in rilievo, in particolare,

[5] Cfr. Garante Europeo per la Protezione dei Dati, *Opinion 6/2015*, *A Further Step Towards Comprehensive EU Data Protection, EDPS recommendations on the Directive for data protection in the police and justice sectors*, del 28 ottobre 2015.

[6] Il Considerando n. 11 menziona gli istituti finanziari: questi, a fini di indagine, accertamento o perseguimento di reati, «conservano determinati dati personali da essi trattati, e li trasmettono solo alle autorità nazionali competenti in casi specifici e conformemente al diritto dello Stato membro». Sul punto cfr. M.M. CARUANA, *The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement*, in *International Review of Law, Computers & Technology*, 2017.

l'articolo 13, paragrafo 3, della Direttiva: tale disposizione, infatti, stabilisce che gli Stati membri possano adottare misure legislative intese a ritardare, limitare o escludere la comunicazione di informazioni all'interessato, ogniqualvolta ciò comprometta le indagini, la prevenzione o il perseguimento dei reati, ovvero la sicurezza pubblica e, nondimeno, i diritti e le libertà fondamentali altrui. La norma, pertanto, non solo consente il differimento, ma legittima qualsiasi forma di manifestazione preventiva di comunicazione.

Tutto ciò premesso ben si potrebbe tradurre, nell'attuale contesto empirico di riferimento, nella possibilità, per le autorità di pubblica sicurezza, di geolocalizzare i soggetti sottoposti a quarantena obbligatoria, per monitorare gli eventuali spostamenti non concessi, condotta che potrebbe assumere rilevanza ai sensi dell'art. 438 c.p.; in tal senso, l'attività di trattamento potrebbe risultare preordinata a prevenire il reato di epidemia, garantendo al contempo la sicurezza pubblica e la tutela dei diritti fondamentali altrui alla salute e, alla luce del particolare fenomeno pandemico, alla vita stessa.

Le attività di trattamento condotte *inaudita altera parte*, inoltre, potrebbero essere volte a verificare la veridicità delle dichiarazioni contenute all'interno delle autodichiarazioni che ogni cittadino deve compilare per legittimare i propri spostamenti: si ricorda, al riguardo, che l'art. 483 c.p. punisce chiunque attesti falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità. In tal caso, l'autorità pubblica potrebbe monitorare gli spostamenti del soggetto, al fine di constatarne la corrispondenza rispetto ai tragitti dichiarati nell'autodichiarazione; inoltre – e questo potrebbe costituire un punto molto critico –, attraverso l'incrocio dei dati relativi alla dislocazione dei contagiati presenti in un predeterminato raggio d'azione, si potrebbe verificare se l'interessato sia entrato più o meno volontariamente in contatto con un altro soggetto positivo al virus.

Quanto appena affermato non risulta contraddetto dalle recenti posizioni adottate dal Comitato europeo per la protezione dati, giacché queste risultano circoscritte all'enucleazione di condizioni di liceità, correttezza e trasparenza del trattamento dati secondo le forme del Regolamento 2016/679/Ue.

Ne consegue, pertanto, che tali indicazioni non comprimono la *vis* applicativa della Direttiva in esame. Al contrario, il regime derogatorio introdotto all'articolo 13, paragrafo 3, risulta più rigoroso rispetto alle tutele che sono invece predisposte dal Regolamento n. 679: più precisamente, ai sensi della Direttiva, l'autorità pubblica potrà omettere ogni comunicazione all'interessato avente ad oggetto il periodo di conservazione dei dati personali, la base giuridica per il trattamento, le categorie di destinatari dei dati personali, anche in paesi terzi o in seno a organizzazioni internazionali, ma soprattutto ulteriori informazioni, in particolare nel caso in cui i dati personali siano raccolti all'insaputa dell'interessato. Il riferimento a "ulteriori informazioni" risulta alquanto vago e ambiguo, potendo costituire un parametro di incertezza definitoria che potrà essere colmato, in misura eterogenea e variabile, da ciascun Stato membro.

L'esame della Direttiva evidenzia forti e numerose potenzialità applicative, ma disvela molteplici incertezze circa la corretta normativa da applicare, che saranno oggetti di una breve analisi conclusiva nel successivo paragrafo.

3. Brevi considerazioni conclusive

Le evidenze empiriche più recenti confermano che l'impiego della tecnologia possa apportare significativi benefici per la tutela della salute. Al

contempo, occorre riflettere sul rapporto tra utilitarismo e tutela della collettività, al fine di scorgere il grado massimo di compressione dei diritti del singolo necessario per apportare benefici generalizzati all'intera collettività.

Tale riflessione è tanto più necessaria alla luce delle disposizioni contenute nella Direttiva 2016/680/Ue, confinata fino ad ora nel dimenticatoio, all'ombra del Regolamento 2016/679/Ue (il cd. GDPR), che fino ad ora ha ricevuto maggiore clamore mediatico. L'incertezza applicativa della Direttiva opacizza i confini con il GDPR, generando problemi di coordinamento tra i due strumenti: le definizioni ampie di "autorità pubblica", come si è osservato in precedenza, non chiarificano il rapporto tra le due fonti normative; del pari, le norme di recepimento nazionale costituiscono piuttosto un'occasione persa per apprestare i livelli essenziali di certezza giuridica.

I tempi particolari, tuttavia, potrebbero in realtà costituire la prima vera e utile occasione per rivitalizzare la valenza applicativa della Direttiva, che costituisce fino ad ora un obliato fondamento giuridico che giustificherebbe il ricorso alla tecnologia per il contrasto al contagio. Ciò implica, d'altra parte, una nuova rimeditazione dell'intera disciplina della *data protection* nella più ampia cornice della cooperazione giudiziaria e di polizia in materia penale, che risulta ancora contraddistinta da grande frammentazione.

(23 aprile 2020)