Privacy e segreti: è possibile estendere ai *big data* le tutele dell'*habeas corpus*?[*]

Di Elena Falletti

Università Carlo Cattaneo-LIUC

Abstracts:

Il concetto di privacy e quello del segreto hanno in comune la volontà di escludere sguardi di terzi da materiali ritenuti importanti o pericolosi per essere svelati e cadere in mani di estranei. Si può dire che il segreto, strumentale a mantenere il potere di una parte politica, sia un elemento di sicurezza nazionale. Infatti, il segreto è un elemento importante della vita di uno Stato, inteso come comunità politicamente organizzata, necessario alla sua sopravvivenza, specie se esso coinvolge elementi non corrispondenti al rispetto della democrazia e dei diritti umani. Quale chiaro esempio si pensi alle c.d. *extraordinary renditions* o alle intercettazioni collettive realizzate dalla NSA americana o ancora alla raccolta e gestione dei big data da parte di enti pubblici o privati.

Di fronte a siffatta invasione della vita delle persone ci si appella alla privacy quale diritto al rispetto del proprio spazio di garanzia nei confronti del potere dell'autorità più forte, tradizionalmente lo Stato, affiancato in tempi più recenti dalle grandi aziende che dei big data, hanno fatto il fulcro delle loro attività commerciali ovvero istituzionali.

Come si ricorderà, sotto il profilo della tutela della persona fisica nel XVIII secolo è stato sviluppato il concetto di habeas corpus contro l'ingiusta detenzione, recentemente esteso in alcuni ordinamenti anche nei confronti della protezione della sfera digitale dove la persona si trova a vivere. Tuttavia finora si è sempre fatto riferimento ad uno sbilanciamento tra entità nazionale o sovranazionale e individuo in un rapporto verticalmente inteso, e si rivendicava l'habeas corpus contro l'entità statale, ma lo sviluppo della tecnologia digitale attraverso device sempre più pervasivi, perché indossabili o in grado di individuare in qualsiasi momento attività e localizzazione del loro possessore, può trasformare questo concetto applicandolo anche tra pari?

In questo senso si nota una trasformazione del rapporto tra 1) ente forte, cioè il fornitore della tecnologia che ottiene i maggiori vantaggi in termini di raccolta di dati personali altrui volontariamente o involontariamente ceduti; 2) chi la indossa, cioè chi attivamente la utilizza traendone un qualche beneficio, e 3) chi invece si trova a subirne involontariamente gli effetti,

* Relazione presentata al Seminario Italo-Spagnolo: IV Congreso Internacional "Perpectivas del constitucionalismo contemporáneo", 28-30 novembre 2018, Facultad de Derecho, Universitad de Murcia".

cioè la persona che interagisce con il precedente soggetto e suo malgrado si vede spogliata di informazioni. Infine, 4) il ruolo dell' ente pubblico, statale o sovranazionale, che dovrebbe monitorare tali dati e garantirne il corretto utilizzo.

Il rapporto tra questi soggetti è di natura eminentemente privatistica, tuttavia esso presenta dei profili indubbiamente costituzionalistici. Lo scopo di questo abstract è verificare se il concetto di habeas corpus possa essere applicato non solo verso le entità pubbliche, quali lo Stato, ma possa essere esteso in senso orizzontale, soprattutto nei confronti degli attori privati, che operano la raccolta di massa dei dati personali traendone linfa e giustificazione ai fini della loro stessa esistenza.

Privacy and secrets: Is it possible to extend the "habeas corpus" protection to the big data?

In the XVIII century the "habeas corpus" concept was developed for limiting the illegal invasion of people's lives by public authorities and for guaranteeing the respect of individual integrity and freedom against the unjust detention. It has been recently extended in some jurisdictions, as in Germany, also towards the protection of the digital environment where individuals live their virtual life, such as computer and smartphones.

Now, it could be investigated if the development of digital technology through the use of these technologies could transform the concept of habeas corpus among peers, especially individuals in an horizontal sense. In fact there is a strong transformation of the relationship between the body and the technology: on the one side the provider of the technology reaps the greatest benefits in terms of collection of personal data voluntarily or involuntarily transferred from the technology wearer. It could use the collected data for profiling users and their life environment. On the other side both the wearer who uses some benefit from the technology and the person who interacts with the wearer could be stripped of information against their will or without knowing.

The aim of this abstract is to understand whether and how the concept of habeas corpus can be applied horizontally, between users of this type of technology.

Intimidad y secretos: ¿Es posible extender al big data la protección "habeas corpus"?

En el siglo XVIII, el concepto de "habeas corpus" se desarrolló para limitar la invasión illegal de la vida de las personas por parte de las autoridades pùblicas y garantizar el respeto de la

integridad individual y la libertad contra la detención injusta. Recientemente se ha extendido en alguna jurisdicciones, como en Alemania, también hacia la protección del entorno digital donde las personas viven su vida virutal, como ordenadores y smartphones. Ahora, se podrìa investigar si el desarrollo de la tecnologìa digital a través del uso de estas tecnologias podrìa transformar el concepto de habeas corpus entre pares, especialmente los individuos en un sentido horizontal. De hecho, existe una fuerte transformación de la relación entre el cuerpo y la tecnologia: por un lado, el proveeedor de la tecnologìa obtiene los mayores beneficios en términos de recopilación de datos personales que se transfieres voluntariamente o involuntariamente del usuario de la tecnologìa. Podrìa utilizar lo dato recopilados para perfilar a los usuarios y su entorno de vida. Por otro lado, tanto el usuario que usa algún beneficio de la tecnologìa como la persona que interactúa con el usuario podría ser despojados de información contra su voluntad o sín saberlo. El objectivo de este resum es analizar cómo el concepto de habeas corpus se puede aplicar horizontalmente, entre los usuarìos de este tipo de tecnologìa.

Sommario: *1. Introduzione: di cosa parliamo quando parliamo di privacy? 2. Le intercettazioni abusive di massa in Common Law; 3. Il "salto di qualità" di Cambridge Analytica; 4. Davvero non abbiamo niente da nascondere? 5. È possibile adeguare le garanzie dell'Habeas Corpus al trattamento dei Big Data?*

1. Introduzione: di cosa parliamo quando parliamo di privacy?

La privacy è strettamente connessa con l'espressione della personalità individuale, poichè riguarda le modalità di svelamento delle convinzioni personali, anche le più intime. L'utilizzo estensivo della c.d. information technology, connessa con la diffusione dei social media e delle tecnologie traccianti, hanno provocato una imprevista, nelle conseguenze, esplosione di tale tema.

La questione che rimane sullo sfondo concerne se la privacy debba essere considerata un diritto fondamentale (R. Post, 2018, 1002) ovvero un servizio che può essere gestito a pagamento, in quanto le informazioni personali possono essere oggetto di trasferimenti proprietari dietro retribuzione monetaria (V. Mayer Schonberger, 2010, 1861). Entrambi gli approcci però svelano il ruolo che la conoscenza di dati privati ovvero riservati può avere nella vita pubblica. Si tratta di una specie di dicotomia che riguarderebbe la contrapposizione

tra “conoscenza e trasparenza” verso “privacy e riservatezza”. Qual è il rapporto tra questi concetti che sembrano essere in contrapposizione: quando sono presenti gli uni, è impossibile la compresenza degli altri? In altri termini, cosa possiamo far sapere di noi? E cosa invece è meglio che venga tenuto riservato, celato, nascosto? Sia in rapporto con gli altri privati (esempio aziende di marketing, ovvero compagnie assicurative, ovvero protezione di segreti industriali) sia in rapporto con l’ente pubblico (protezione della riservatezza dalle intrusioni come intercettazioni, geolocalizzazioni, raccolta di dati a scopi di “sicurezza”).

Il rischio di ridurre la privacy a bene di consumo non è più remoto, ma diventa più o meno concreto a seconda di come si intende il concetto stesso di privacy. Secondo la prospettiva statunitense, la privacy è riconducibile a una semplice libertà negativa. Infatti, si tratta di una visione ove si intende escludere altri dalla propria sfera personale e dalle informazioni inerenti a questa, mantenendo un confine tra se stessi e il resto del mondo. Dal punto di vista europeo la privacy consiste in un diritto fondamentale, espressione della dignità umana, assoluta, personale e inalienabile. La distinzione tra i due modi di vedere evidenzia che la concezione statunitense della privacy è meno forte di quella europea, infatti tende a considerare le informazioni personali, anche sensibili, come oggetto di proprietà (*propertization*) e quindi bene cedibile a terzi senza significative garanzie (V. Schonberger, 2010, cit.).

Pertanto, è essenziale analizzare, seppur sommariamente, la giurisprudenza americana in tema di privacy. Sia perché, da un lato, la privacy negli Stati Uniti non riesce a far da scudo all’invadenza delle pubbliche autorità nelle vite dei singoli per ragioni di sicurezza; dall’altro lato, sia perché le compagnie principali nel “*market capitalization ranking*” sono principalmente statunitensi[1]. Esse, prima di norme giuridiche, applicano al loro business un approccio culturale diverso da quello europeo, che non si può ignorare e che se non opera propriamente da “modello”, consente di anticipare le strategie rispetto alle quale gli altri operatori si devono confrontare, sia sotto un profilo giuridico (stesura dei contratti di adesione alle piattaforme online, tattiche processuali nel contenzioso giudiziario e così via), sia extragiuridico (piani operativi aziendali, di marketing e così via). Tuttavia, va segnalata la recente apertura del CEO di Apple (D. Goldman, 2018), l’azienda con maggiore capitalizzazione mondiale, secondo il quale la privacy è un diritto umano e il modello europeo rappresentato dal GDPR dovrebbe ispirare la normativa federale americana che invece, al momento, è orientata in senso contrario.

1 In particolare Apple, Amazon.com, Alphabet (cioè, Google), Microsoft, Facebook (visitato il 31 ottobre 2018) (https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-value/).

2. Le intercettazioni abusive di massa in Common Law

L'approccio americano sembra dimostrarci che all'invasività della raccolta intrusiva di massa dei dati personali ci si possa fare l'abitudine, se non addirittura all'assuefazione, e possa portare alla trappola dell'argomentazione del "tanto non ho niente da nascondere". Prima di affrontare questo argomento pare utile analizzare come abbia avuto origine la legittimazione, almeno sociale, di siffatta intrusività.

Negli Stati Uniti, la sorveglianza per ragioni di sicurezza è legittimata da quasi cent'anni, cioè a partire dalla sentenza Olmstead v. United States del 1928, dove si affermò che il *Amendment VI*[2]della Costituzione non deve essere applicato alle registrazioni perché non vi è attività di ricerca o di sequestro, ma di solo ascolto (Solove, 2011, p. 6 ss.). Tuttavia la ragione di fondo risiede nella necessità di tutelare la sicurezza nazionale, pertanto nel corso del tempo vennero adottate nuove norme e creata una agenzia federale apposita, la *National Security Agency*[3].

Questa analisi vuole partire dall'introduzione delle norme antiterrorismo del c.d. Patriot Act del 2001 (*Uniting and Strenghtening America by Provided Apporpriate Tools Required to Intercept and Obstruct Terrorism*), a seguito degli attacchi terroristici sul suolo americano dell'11 settembre 2001. Il primo caso rilevante di sorveglianza di massa e conseguente raccolta di dati personali emerse con la decisione ACLU vs NSA[4]. Il Patriot Act ha garantito alla *National Security Agency* di intercettare in via elettronica centinaia di migliaia di comunicazioni (specie email e telefonate) cittadini statunitensi, senza l'autorizzazione giudiziaria ma con la sola autorizzazione presidenziale, illegittima per eccesso di potere, in violazione altresì degli I e del IV *Amendment* i quali tutelano rispettivamente la libertà di manifestazione del pensiero, di associazione[5] e la riservatezza. La NSA aveva opposto il *State*

2 Esso recita: "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*".

3 Seppure nella sommarietà dello spazio che è possibile dedicare allo sviluppo di questo approccio, divenuto successivamente modello per altri ordinamenti, si evidenzia come la National Security Agency sia stata creata da Truman nel 1952 con lo scopo di decrittare messaggi in codice stranieri (D. J. Solove, op. cit., 11). Ruoli altrettanto rilevanti sono stati rivestiti dalle conseguenze della scomparsa di J. E. Hoover quale capo dell'F.B.I, dopo cinquant'anni e dello scandalo del Watergate, dal quale scaturì la promulgazione del FISA (Foreign Intelligence Sourveillance Act) del 1978. Lo scopo di quest'ultima norma è di predisporre un quadro normativo all'interno del quale fosse possibile condurre sorveglianza elettronica nel contesto degli impegni della Nazione nel rispetto della privacy e dei diritti individuali (D. Solove, op. cit.).

4 American Civil Liberties Union v. National Security Agency, 493 F.3d 644.

5 Il testo dell'*Amendment I* recita: "*Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the*

Secrets Privilege, affermando che rendere pubbliche di fronte ad un giudice le ragioni che avevano dato origine al programma segreto di intercettazioni avrebbe messo in grave pericolo la sicurezza nazionale. Il giudice distrettuale di Detroit rilevò come le libertà fondamentali garantite dal *Bill of Rights* fossero le prime vittime a soffrire dello sbilanciamento dell'equilibro tra i poteri dello Stato. Tuttavia, tale rilevante e condivisibile argomentazione venne travolta in appello e la *United States Court of Appeals for the Sixth Circuit* negò che ACLU potesse agire in giudizio contro NSA in quanto le prove prodotte da parte attrice non vennero ritenute sufficienti a dimostrare che ACLU stessa fosse tra gli obiettivi del "*Terrorist Surveillance Program*". Pertanto, l'attività di raccolta massificata di dati promossa dalla NSA non cessò e affrontò altre censure giudiziarie, a volte con successo, come avvenuto nel caso *Klayman v. Obama*, deciso dalla *United States District Court for the District of Columbia*[6]. Detto giudice stabilì l'incostituzionalità dell'intero programma di intercettazioni di massa poiché violativo della ragionevole aspettativa di privacy garantita dal Quarto Emendamento della Costituzione degli Stati Uniti per via dell'indiscriminata, arbitraria e sistematica violazione della riservatezza dei dati personali che virtualmente avrebbe potuto colpire ogni singolo cittadino senza la previa autorizzazione giudiziaria. Il *Justice* Leon riconobbe che l'utilizzo estensivo dei *device* elettronici e telematici che tracciano i movimenti e le azioni dei cittadini provocano una ragionevole maggiore aspettativa nella tutela della privacy, non minore, a causa dei cambiamenti culturali che hanno accompagnato siffatta trasformazione tecnologica[7].

---

people peaceably to assemble, and to petition the government for a redress of grievances".

6 United States District Court for the District of Columbia, Klayman v. Obama, 16.12.13

7 Tuttavia, il formante giurisprudenziale statunitense presentava delle contraddizioni, infatti i parere opposto la United States District Court for the Southern District of New York (United States District Court for the Southern District of New York, ACLU v. Clapper, 27.12.13), secondo cui siffatto programma è conforme alla Section 215 dell'USA PATRIOT Act e del Quarto Emendamento della Costituzione in quanto esso pone un concreto ed effettivo argine alle attività terroristiche negli Stati Uniti, seppure esso sia di proporzioni sconosciute in precedenza, il suo scopo è profondamente differente rispetto alle mere indagini criminali, poiché le minacce natura terroristica sono senza precedenti. In ogni caso, la Foreign Intelligence Surveillance Court (FISC) (Foreign Intelligence Surveillance Court, 3.1.14), la Corte che autorizza le operazioni e i programmi della National Security Agency, ha ribadito la legittimità dei programmi di intercettazione globale della NSA autorizzandone la prosecuzione. Si segnala altresì un altro contenzioso in corso di fronte alla corte federale del *Northern District of California* in tema di raccolta dati e violazione della privacy di fronte alle corti federali. Si tratta del caso *First Unitarian Church of Los Angeles v. NSA*, dove si contesta l'autorizzazione concessa nel giugno 2013 sempre ai sensi della Section 215 dell'USA PATRIOT Act da parte della *Foreign Intelligence Surveillance Court* di tutte le chiamate, della localizzazione del telefono, della durata e dell'ora della chiamata e di ogni altra "informazione identificativa" di tutti i clienti Verizon per un periodo di tre mesi. Con questa causa si afferma che tale raccolta informativa viola tanto la libertà di pensiero, soprattutto la manifestazione di opinioni politiche, quanto quella di associazione protette del Primo Emendamento.

Nel frattempo venne svelata la vicenda politico-internazionale di Edward Snowden, il quale ottenne l'asilo politico in Russia dopo aver rivelato l'esistenza del "PRISM" (*"Planning Tool for Resource Integration, Synchronization, and Management"),* cioè un di programma di intercettazioni di comunicazioni telefoniche e telematiche di massa. Rispetto al "*Terrorist Program Surveillance*" esso rappresentò una modifica nell'approccio globale nella intercettazione delle comunicazioni, coinvolgendo anche importanti provider di servizi web, email, chat, video, archiviazione dati, comunicazioni VoIP, trasferimento di files e videoconferenze, così realizzando una raccolta sistematica dei dati personali e delle comunicazioni dei cittadini americani senza mandato giudiziario.

In merito a PRISM, il contenzioso giudiziario si estese al di fuori dei confini degli Stati Uniti per approdare in Inghilterra, e l'aspetto più interessante riguardò la discontinuità dei giudici anglosassoni rispetto a quelli americani nel valutare la legittimità di siffatto programma di sorveglianza di massa. Sul punto infatti si sono contrapposte la statunitense Corte federale distrettuale di San Francisco e la britannica *Investigatory Powers Tribunal*.

La causa Jewel v. NSA[8], celebrata negli Stati Uniti**,** riguarda un contenzioso che nelle sue varie fasi dura dal 2008 su istanza di alcuni cittadini statunitensi a seguito delle rivelazioni di un tecnico della compagnia AT&T, il quale ha svelato l'intercettazione delle comunicazioni da parte di NSA "raccolte a monte", attraverso l'infrastruttura della compagnia stessa. L'ultima istanza per bloccare tale raccolta a causa della violazione del Quarto Emendamento è stata rigettata dalla Corte californiana che invece ha accolto l'eccezione difensiva relativa al segreto di stato, il quale permette ai giudici di non utilizzare una prova che metta in pericolo la sicurezza nazionale, qualora essa venga svelata pubblicamente. A questo proposito, si osserva che l'amministrazione governativa NSA ha depositato in giudizio dichiarazioni segrete dei suoi funzionari, fruibili solo dal giudice ma non alla controparte o al pubblico e su tali dichiarazioni si è basata la Corte per rigettare l'istanza dei ricorrenti. Tuttavia va osservato che la Corte ha espresso il suo disagio nel non poter argomentare liberamente il rigetto delle istanze di costituzionalità "senza rischiare il danneggiamento della sicurezza nazionale"[9].

8 USA, Jewel et al v. National Security Agency et al, 10.2.15, https://www.eff.org/document/order-motions-summary-judgment-1

9 Va sottolineato che sono diverse le azioni giudiziarie predisposte dalle associazioni a difesa della privacy ovvero dei diritti civili. Finora la maggioranza di essere sono risultate essere soccombenti, pertanto pendono di fronte alle giurisdizioni d'appello. Tra queste si rammentano ACLU v. Clapper, Smith v. Obama e Klayman v. Obama (unico caso in cui un giudice federale ha stabilito che la raccolta massiva dei dati è incostituzionale).

Al contrario, nel Regno Unito l'*Investigatory Powers Tribunal* (IPT)[10], giudice specializzato nell'esaminare le denunce relative all'attività delle agenzie di intelligence britanniche, ha affermato che la sorveglianza di massa delle comunicazioni effettuate via internet dei cittadini britannici viola gli articoli 8 e 10 della Convenzione europea per la salvaguardia dei diritti umani e delle libertà fondamentali, recepita in diritto inglese dallo Human Rights Act 1998. Specificamente interpellato sul PRISM[11], il medesimo organo giudiziario britannico ha sottolineato che, qualunque siano le circostanze di raccolta dei materiali intercettati dai servizi di intelligence i seguenti elementi di diritto sono di fondamentale importanza: 1. L'utilizzo da parte dei servizi di intelligence del materiale intercettato all'estero è sempre illegale a causa dell'assenza di un mandato giudiziario autorizzativo della raccolta, poiché in questo modo, deliberatamente, verrebbero eluse le disposizioni di legge del Regno Unito incaricando un altro Stato a fare ciò che per i servizi di intelligence inglesi non sarebbe legittimo ottenere; 2. *"La pesca a strascico indiscriminata di informazioni intercettate*", sia di massa o in altro modo, è illegittima, in quanto inutile e sproporzionata. In questo contesto, il materiale può essere legittimamente intercettato solo in presenza di mandato giudiziario in caso di interesse e salvaguardia della sicurezza nazionale, al fine di prevenire o individuare forme gravi di criminalità o al fine di salvaguardare il benessere economico del Regno Unito ("le finalità statutarie"); ed è proporzionato soltanto se è proporzionata all'obiettivo che si chiede di essere raggiunto da un comportamento lecito; 3. una volta che sono stati analizzati dai servizi di intelligence, i dati legittimamente intercettati, inclusi i dati di comunicazione, possono essere conservati solo per il tempo necessario per le finalità statutarie; successivamente devono essere distrutti. 4. Per quanto concerne le informazioni intercettate, esse sono conservate sotto la responsabilità di servizi di intelligence. La ricezione, manipolazione e distruzione del materiale devono essere gestiti con attenzione, monitorati e registrati e devono essere sempre a disposizione delle preposte autorità di controllo per le dovute ispezioni.

L'aspetto rilevante concerne il fatto che i programmi PRISM e UPSTREAM della NSA americana sono stati sottoposti a scrutinio giudiziario di fronte ad un'autorità giudiziaria di un Paese alleato e non esclusivamente da una corte statunitense. Secondo la decisione dell'IPT tale attività di sorveglianza è altresì illegale perché carente di un mandato giudiziario ai sensi

10 *UK: IPT, Liberty & Others vs. the Security Service, SIS, GCHQ, 06 February 2015.*

11 United Kingdom Investigatory Powers Tribunal, Liberty (The National Council of Civil Liberties) v The Government Communications Headquarters & Ors [2014] UKIPTrib 13_77-H (05 December 2014).

del *Regulation of Investigatory Powers Act* (RIPA) inglese durante tutti i suoi anni di esercizio, a partire dal 2007.

3. I "salti di qualità" di Cambridge Analytica

In questa nuova fase risulta evidente l'interconnessione del commercio dei dati: essi vengono raccolti per motivo (per esempio, una indagine di mercato), vengono utilizzati per un altro motivo (quale il *behavioural advertising* a fini di promozione di prodotti di e-commerce) e gli stessi dati vengono ceduti per ragioni ancora diverse (come la manipolazione delle opinioni politiche in corso di campagne elettorali). Quanto delineato in poche righe può sembrare lo *script* di un romanzo o di una nuova serie televisiva, invece rappresenta il "salto di qualità" nel trattamento dei dati personali avvenuto con lo scandalo di Cambridge Analytica (M. Festa, 2018).

Cambridge Analytica era una società di consulenza online che, una volta prelevati i dati da Facebook, effettuava attività di digital marketing su elementi conoscitivi delle attività individuali quali i "mi piace" ai vari post, i commenti, i luoghi dai quali i commenti venivano pubblicati, le condivisioni o i post stessi. Tali informazioni, relative a ogni singolo utente, erano elaborate da algoritmi al fine di riconstruire personalità, attitudini, gusti, emozioni e comportamenti, formulando una pubblicità "altamente personalizzata" su ciascun utente.

Questa vicenda ha reso l'opinione pubblica, specializzata e non, consapevole che le tecniche di indagine e di marketing commerciale vengono applicate anche alla politica e alle campagne elettorali sono trattate come se fossero un "prodotto da piazzare" sul mercato degli elettori/consumatori profilati attraverso l'analisi dei Big Data raccolti, a titolo esemplificativo con procedimenti di *microtargeting, retargeting, data mining, webcrawling e data strategies* (M. Festa, cit.).

Il "salto di qualità" è quindi doppio: da un lato esso riguarda la metodologia di raccolta, dall'altro lato esso concerne il cambiamento di scopo della raccolta dei dati "ex post", con il loro utilizzo a scopo politico. Attraverso la profilazione dell'elettore (considerato alla stregua di un consumatore) si massimizza il risultato attraverso un minimo sforzo comunicativo con l'applicazione delle tecniche di *behavioural advertising* (pubblicità comportamentale), del quale si erano già occupati i Garanti Europei (WP29, Opinion n.2/2010), limitandosi però al settore commerciale (Festa, cit.). Da una prospettiva commerciale, le attività legate alla profilazione commerciale manifestano sovente contrasti con la tutela della privacy, in

particolare in merito alla violazione del principio di finalità, all'assenza del consenso degli interessati, alla mancata o carente informativa sul trattamento dei dati personali dei soggetti interessati[12]. In ambito di "targettazione politica", tali criticità assumono maggiore valenza negativa.

Infatti, considerando i trattamenti effettuati in ambito politico ed elettorale, si può notare come, in questo caso, le operazioni di raccolta, analisi e rielaborazione delle informazioni utili sui cittadini/elettori (dall'adesione o affiliazione a un partito politico alle liste di follower su Twitter o alle informazioni presenti sui profili Facebook) vengono incrociate con dati anagrafici e demografici più "tradizionali" come età, reddito, stato civile, recuperati sia tramite internet sia con mezzi più tradizionali. Operazioni di questo tipo servono a comprendere cosa i cittadini desiderano che i loro rappresentanti facciano e, dunque, cosa è bene che i candidati propongano per poter essere eletti.Le criticità emerse dal summenzionato rapporto si estendono in un settore ancora più delicato, cioè quello della manifestazione delle opinioni politiche (che avviene attraverso la condivisione o l'apposizione di "mi piace" a post di contenuto politico), trasformando in massa i cittadini/elettori, in consumatori e, da ultimo, manipolando il sistema democratico stesso.

Da un punto di vista politico si può notare come nel tempo si sia svolto un lento procedimento, sviluppatosi spesso a fasi alterne, che ha trasformato, a partire dal XVIII secolo, il suddito in cittadino, parte attiva della vita politica. Al contrario, la fase involutiva ha avuto inizio con l'avvento delle piattaforme sociali, di Internet e dei Big Data. Infatti, il cittadino non viene più considerato parte della vita politica, che si esprime attraverso l'intermediazione dei partiti politici, ma diventa un consumatore di materiali prodotti da terzi e fruiti "direttamente" attraverso una piattaforma digitale, la quale preordina una limitata possibilità di scelta di opzioni, individuate attraverso, appunto, l'analisi dei big data raccolti online. Si tratta di un circolo vizioso, apparentemente senza fine, che alimenta se stesso. A questo punto la domanda è: cosa è possibile fare per spezzarlo?

Una soluzione a tal fine parrebbe essere quella di rafforzare le strutture della partecipazione rappresentativa attraverso un duplice approccio: da un considerare le piattaforme digitali un mezzo e non un fine, mentre dall'altro lato valorizzare il principio di responsabilità nella

12 La citata dottrina ricorda come, nel 2014, l'Autorità Garante della Privacy sia inervenuta con un provvedimento diretto ai partiti politici imponendo loro il divieto generale " di utilizzo per finalità di propaganda elettorale e connessa comunicazione politica per i dati reperiti liberamente sul web, riferendosi in particolare proprio ai dati raccolti automaticamente in internet tramite appositi software o dati ricavati da social network, forum o newsgroup. Questo perché il trattamento deve essere improntato nel più ampio rispetto del principio di finalità".

gestione dei dati (Re, 2018, 1409 ss), sia sotto un profilo privato (diffusione dei dati per scopi sanitari, commerciali, culturali etc), sia sotto un profilo pubblico (in merito alla manifestazione del pensiero e alla partecipazione alla vita politica).

Svolto questo primo (ipotetico) passaggio occorre domandarsi che cosa differenzia una raccolta di dati per ragioni di sicurezza, da quella per scopi commerciali da quella per scopi politici? Si tratta di raccolte "interscambiabili"? Dal punto di vista di chi raccoglie, tratta e conserva i dati probabilmente si: dalla moltiplicazione dei profili effettuata con algoritmi o programmi di intelligenza artificiale vengono profilati le attitudini e gli orientamenti sia del singolo, sia della massa. Dal punto di vista del titolare di tali dati, è probabile che questi non si renda neppure più conto della spoliazione informativa che sta subendo essendo ormai costui assuefatto ad accettare condizioni o formulari all'uopo predisposti e spesso neppure letti. Spesso ci si autoassolve della distrazione con la quale si "cliccano" siffatti formulari ripetendo a se stessi il noto e summenzionato luogo comune che "tanto non ho niente da nascondere", ma così ci si ritrova nudi e indifesi di fronte alle intemperie, in questo caso rappresentate dalla altrui oscura gestione del proprio patrimonio informativo.

4. **Davvero non abbiamo niente da nascondere?**

Se è vero che non tutto di noi può e deve essere svelato, che non possiamo vivere in una casa di vetro perché ciò lederebbe la nostra dignità personale, allora occorre trovare uno strumento giuridico che abbia la forza e l'autorevolezza, di proteggerci dalle invasioni altrui nella sfera personale. A questo proposito, a mio avviso, il concetto di habeas corpus non è superato, ma consiste in una risposta efficiente ai problemi esposti, sia sotto un profilo comparatistico, sia sotto un profilo storico. Ecco perché.

Chiunque possiede una propria idea di cosa si intenda per "habeas corpus". Tradizionalmente questa espressione si riferisce alla legalità (valutata da un giudice) della detenzione di qualcuno (B. Farrell, 2008, 551). Sotto il profilo storico, il *writ of habeas corpus* ha avuto origine nel XIII Sec. Nel common law inglese (W. F. Duker, 1980, 17) venne utilizzato come garanzia di libertà personale (B. Farrell, 2008, 553). Seppure esso consistesse non in un diritto, ma in un privilegio fondato sulla prerogativa reale e emanato a discrezione dei giudici del *King's Bench* dopo una valutazione sommaria dell'istanza di parte (P. D., Halliday, G. E.,White, 2008, 593), esso era già orientato alla protezione della libertà individuale (A. L. Tyler, 2016, 1956), in particolare contro gli abusi commessi sui prigionieri e sui loro corpi (P.

D. Halliday, 2012, 11). Analizzando l'evoluzione storica della giurisprudenza in materia, con la concessione del *writ of habeas corpus* il re chiedeva conto della restrizione della libertà del suo suddito. La dottrina osserva che il potere del sovrano di liberare i prigionieri proviene direttamente dalla disponibilità che il sovrano aveva dei loro corpi (P. D. Halliday, G. E. White, cit.; A. L. Tyler, cit.). Infatti, "*Thus a writ concerned with moving, holding, and releasing bodies from imprisonment arose directly from this fundamental aspect of the king's prerogative*" (P. D. Halliday, G. E. White, cit.). In termini "moderni" si tratta della manifestazione del patto di mutua cura (del re verso i suoi sudditi) e di obbedienza (dei sudditi verso il re), espressione di un'alleanza (P. D. Halliday, G. E. White, cit.)[13]. Nei secoli successivi, in particolare dal XVII, i tempi turbolenti della storia politica inglese cambiarono la natura dell'habeas corpus a seguito della guerra civile e della *Great Revolution*. Il primo a dare una valenza diversa alla natura di questo istituto fu Edward Coke, che lo utilizzò quale strumento per correggere ogni *"manner of misgovernment*" (E. Coke, 1644, 4; H. A. Nutting, 1960, 527). Infatti, nell'Inghilterra del XVII secolo furono caratterizzati dalla lotta tra il re Carlo I Stuart, il suo governo, il parlamento e le corti di common law ed equity. (K. Zweigert, J. Kötz, 1998, 189). Il parlamento rafforzò le garanzie dell'habeas corpus per limitare gli effetti delle azioni della Corona e del governo (B. Farrell, cit., 555), in particolare per limitare gli effetti contro le detenzioni arbitrarie ordinate dal re medesimo (B. Farrell, cit.). Durante la guerra civile inglese, gli atti di detenzione continuarono e i prigioneri venivano deportati oltremare. Nel 1679 venne approvata la versione definitiva dell'*Habeas Corpus Act*, il quale attribuiva nuove garanzie procedurali (come il diritto a un processo equo) e sostanziali (come il divieto di deportazioni non autorizzate oltremare). Data la sua natura costituzionale, la giurisprudenza continuò a sviluppare l'habeas corpus come garanzia di libertà personale (B. Farrell, op. cit.).

Cosa possiamo imparare oggi da questa esperienza? È possibile utilizzare le garanzie sostanziali e costituzionali, come sopra delineate, quali strumenti di protezione dei dati personali? Il punto che voglio analizzare riguarda proprio tali garanzie con le questioni sollevate dal trasferimento, raccolta e trattamento di massa dei dati personali che avviene

13 *"the bond of allegiance is not a bond of servitude but of freedom:* come liber homo*." By giving allegiance to the person of the king, the person of the free subject was protected. Not only was his body protected, so too was what was thought of as his "inheritance." Inheritance did not mean only the ability to gain possessions from one's family. It meant something far greater: succession to the traditional privileges of a subject. Law was part of that inheritance because it helped protect subjects. In protecting law, partly through the use of the royal prerogative, the king protected the subject, just as the protected subject protected the king. To our eyes, this reasoning appears circular".*

oggi. Il passaggio logico che sto cercando di sviluppare parte dal dato concreto che se i dati personali sono intangibili in quanto proiezione della persona fisica, essi devono essere trattati con le stesse garanzie riconosciute alla persona fisica.

5. È possibile adegaure le garanzie dell'habeas corpus al trattamento dei big data?

Nella ricostruzione della tutela della privacy e dei dati personali sono emersi in dottrina due modelli divergenti. Da un lato si segnala quello promosso da Richard A. Posner (1978: 393), il quale teorizza il diritto degli individui di non essere posti in cattiva luce a seguito di pubblicazioni di informazioni false o diffamatorie. In conseguenza di ciò si propugnerebbe il controllo e la cancellazione delle inforamzioni che mettono in pericolo la reputazione della persona, con la prevenzione di interpretazioni fuorvianti. Si tratta del modello su cui si basa il c.d. "diritto all'oblio" (right to be forgotten) fatto proprio dalla Corte di Giustizia dell'Unione Europea con la nota decisione "Costeja Gonzales"[14].

Dall'altro lato vi è un diverso modello che segue la dottrina del c.d. "habeas data" formulata da Alan Westin (1970) e Stefano Rodotà (2012) che definiscono l'inviolabilità dell'identità digitale come il diritto personale dell'individuo di controllare l'utilizzo dei dati sparsi durante le attività quotidiane e richiedere la loco cancellazione (A. Guadamuz, 2000; M. T. Gonzales, 2016, 642; K. S. Rosenn, 2011, 1022; W. O. Bastos, 2007, 2). Alla luce di questa prospettiva, alcune esperienze comparatistiche hanno mostrato un approccio simile, seppure minoritario e connesso con sistemi giuridici non di lingua inglese (M. T. Gonzalez, 2016, 642; A. Guadamuz, 2000, 7)[15]. Altresì, tale approccio è assimilabile a quanto stabilito dall'art. 8 della Carta dei diritti fondamentali dell'Unione Europea, elaborato sulla base della giurisprudenzia della Corte Europea dei diritti umani[16].

Con l'applicazione del concetto di habeas corpus alle tecnologie in grado di raccogliere massivamente dati personali ovvero alle piattaforme di social networking, intendo riferirmi non soltanto agli aspetti relativi al controllo dell'utilizzo dei dati personali, che sono comunque rilevanti, ma voglio riferirmi alla creazione di un confine, di una barriera, se non un ostacolo, alla raccolta di dati personali attraverso strumenti fisici (come tecnologie

14 Corte di Giustizia dell'Unione Europea, Grande Sezione, 13 maggio 2014, causa C-131/12, Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González.

15 In particolare nelle costituzioni di diversi paesi dell'America Latina e in Germania.

16 Tale articolo afferma che "1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2.Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3.Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

indossabili, computer, laptop, smartphone). In questo senso, e sotto un profilo concettuale, vorrei proporre quale parametro di riferimento per il civil law la decisione del *Bundesverfassungsgericht* del 27 febbraio 2008[17].

Questa decisione ha riconosciuto l'esistenza del diritto di qualsiasi utente di tecnologie telematiche ad avere diritto alla propria libertà come espressione della propria personalità digitale. La decisione ha preconizzato la creazione di una "intimità digitale" dove l'individuo racchiude i suoi dati, raccolti in webmail, o un laptop o un dispositivo on uno smartphone di uso quotidiano. In realtà, quel caso costituzionale è stato promosso da un gruppo di persone (un giornalista, un membro di un partito politico locale e tre avvocati) contro una disposizione del "*Gesetzes zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen vom 20. Dezember 2006 (GVBl NW 2006, S. 620*) che consentiva l'utilizzo di "trojan horse" di stato per effettuare ricerche sui sistemi e strumenti informatici privati, senza che i titolari ne fossero a conoscenza. Il BVerfG ha dichiarato nulla tale disposizione perché ammettava la sorveglianza statale senza autorizzazione giudiziaria.

In effetti, tali programmi di sorveglianza erano in violazione del diritto della personalità "come diritto fondamentale alla garanzia della riservatezza e dell'integrità dei sistemi informatici", nonché del principio di proporzionalità.

Nonostante tale decisione dei giudici costituzionali tedeschi, relativi all'uso nascosto di software-spia, fosse ormai di quasi dieci anni fa, la questione critica del trasferimento delle masse di dati raccolti emerge nuovamente. In questo senso, una versione trasformative dell'habeas corpus, adattata all'immaterialità, può essere utile. Un simile approccio in common law è avvenuto con la concettualizzazione del *cybertrespass* (Epstein, 2003, 73 ss).

17 BVerfG, Judgment of the First Senate of 27 February 2008 - 1 BvR 370/07. La Corte si è espressa sul punto nei seguenti termini: "*the guarantee of the inviolability of the home leaves loopholes as regards access to information technology systems. Article 13.1 GG does not confer on the individual any across-the-board protection regardless of the access modalities against the infiltration of his or her information technology system, even if this system is located in a dwelling. The encroachment may take place regardless of the location, so that space-oriented protection is unable to avert the specific endangerment of the information technology system. Insofar as the infiltration uses the connection of the computer concerned to form a computer network, it leaves the spatial privacy provided by delimitation of the dwelling unaffected. (...) The manifestations of the general right of personality, in particular the guarantees of the protection of privacy and of the right to informational self-determination, previously recognised in the case-law of the Federal Constitutional Court, also do not comply sufficiently with the special need for the protection of the user of information technology systems. The need for protection of the user of an information technology system is however not restricted solely to data to be allotted to his or her privacy. The right to informational self-determination also does not fully do justice to personality endangerments. A third party accessing such a system can obtain data stocks which are potentially extremely large and revealing without having to rely on further data collection and data processing measures. In its severity for the personality of the person concerned, such access goes far beyond individual data collections against which the right to informational self-determination provides protection*".

Questo approccio potrebbe essere contestato con due obiezioni, che potrebbero essere facilmente superate. Da un lato, si potrebbe sottolineare che questi dati sono intangibili e quindi non possono essere trattati come oggetti fisici. La risposta a questa affermazione è che fanno parte del corpo umano e appartengono al corpo del titolare del diritto. In altre parole: i dati sul mio corpo, la mia salute, il mio comportamento appartengono al mio corpo e quindi appartengono a me e dovrebbero essere trattati come tali.

D'altra parte, si potrebbe sostenere che l'immaterialità dei dati potrebbe impedire il loro trattamento come gli altri beni (fisici) legali. Tuttavia, in altre circostanze, queste preoccupazioni sull'immaterialità di tali beni non sorgono. Ad esempio, in caso di sequestro di materiale illecito diffuso da siti Internet o programmi peer-to-peer, come materiale protetto da copyright o immagini di abusi sui minori.

L'applicazione del concetto di habeas corpus riuscirà a contenere anche la lucratività altrui sui dati propri? (Mayer-Schonberger-Cuckier, p. 99/100 e ss.) In questo senso, detto utilizzo potrebbe restituire il valore, anche economico, al loro titolare consentendogli di limitare efficacemente il loro riuso ovvero la cessione.

6. Conclusioni

Autorevole dottrina si esprime in termini di "datificazione di tutto" (Datafication of everything, V. Mayer-Schonberger, K. Cukier, 2013, 94), perché da tale procedimento è possibile ricostruire dalle nostre tracce la nostra personalità. Infatti, attraverso l'utilizzo di smartphone o di tecnologie indossabili, sempre più evolute, invasive e *fashion* nelle loro forme, ogni nostro gesto, ogni percorso, ogni singolo attimo viene trasformato in dato potenzialmente utile, controllabile e lucrativo: individualmente e come massa. Da questa riflessione nasce la mia idea di utilizzare il concetto di habeas corpus adattandolo alla immaterialità, alla smaterializzazione attuale: a me interessa indagare il concetto e la sua possibile applicazione quale garanzia nei confronti della raccolta a strascico di Big Data. A questo proposito, ritengo che riportare la materialità della difesa del "corpus" nell'epoca della immaterialità diffusa può (e vuole) significare che, nonostante l'evoluzione scientifica e tecnologica, il corpo e la corporeità rimangono una caratteristica irrinunciabile della dignità umana.

7. Bibliografia

Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising

Bastos, A. W. (2007), O habeas data e a proteção da privacidade individual: recuperação histórica da evolução conceitual e constitucional no Brasil, <http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/viewFile/15977/1554>.

Coke E, (1644), Institutes of the Laws of England;

Duker, W. A., (1980), A Constitutional History Of Habeas Corpus, Greenwood Press, Westport, Connecticut;

Epstein R. A., (2003), Cybertrespass, 70 U. CHI. L. REV. 73;

Farrell, B., (2008), From Westminster to the World: The Right to Habeas Corpus in International Constitutional Law, 17 Mich. St. J. Int'l L. 551;

Festa M., 2018, Caso Facebook Cambridge Analytica: una minaccia al diritto alla privacy, Quotidiano Giuridico, 13 aprile 2018;

Goldman, D. (2018) Tim Cook wants stricter privacy laws, CNN, 24 October, 2018, https://edition.cnn.com/2018/10/24/tech/tim-cook-privacy/index.html?utm_medium=social&utm_source=fbCNN&utm_content=2018-10-24T13:49:38;

Gonzalez, M. T., (2016), Habeas Data: Comparative Constitutional Interventions From Latin America Against Neoliberal States Of Insecurity And Surveillance, 90 Chi.-Kent L. Rev. 641;

Guadamuz A, (2000) 'Habeas Data: The Latin-American Response to Data Protection', 2000 (2) The Journal of Information, Law and Technology (JILT);

Halliday, P. D. (2012), Habeas Corpus: From England to Empire, Harvard University Press, Boston;

Halliday, P. D., White, G. E., (2008), The Suspension Clause: English Text, Imperial Contexts, and American Implications, 94 Va. L. Rev. 575;

K. Zweigert, H. Kotz, Introduction to Comparative Law, 1998 (Oxford-London-New York);

Mayer-Schonberger V., Cukier K., (2013), Big Data, 2013;

Mayer-Schonberger, V., (2010) Beyond Privacy, Beyond Rights-Toward a "Systems" Theory of Information Governance, 98 Calif. L. Rev. 1853;

Nutting, H. A., (1960), The Most Wholesome Law - The Habeas Corpus Act of 1679, 65 Am. Hist. Rev. 527;

Post, R. C. (2018), DATA PRIVACY AND DIGNITARY PRIVACY: GOOGLE SPAIN, THE RIGHT TO BE FORGOTTEN, AND THE CONSTRUCTION OF THE PUBLIC SPHERE, 67 Duke L.J. 981;

Re R. M. (2018), Fourth Amendment Fairness, 116 Mich. L. Rev. 1409;

Rodotà, S. (2012), *Il diritto di avere diritti* (Bari);

Rosenn, K. S. (2011), Procedural Protection of Constitutional Rights in Brazil, 59 Am. J. Comp. L. 1009;

Solove J. D. (2011), Nothing to Hide, The False Tradeoff between Privacy and Security, Yale University Press;

Tyler, A. L. (2016), Federal Courts, Practice & Procedure Honoring Daniel Meltzera "SECOND Magna Carta": The English Habeas Corpus Act And The Statutory Origins Of The Habeas Privilege, 91 Notre Dame L. Rev. 1949;

Westin, A. (1970), Privacy and Freedom (London).