La re-identificazione dei dati anonimi e il trattamento dei dati personali per ulteriore finalità: sfide alla privacy

Mario Viola de Azevedo Cunha, Danilo Doneda e Norberto Andrade[1]

1. Introduzione

Questo articolo introduce e descrive due aspetti relativi alla protezione dei dati, uno di natura tecnologica e l'altro di carattere giuridico. Entrambi gli aspetti costituiscono due importanti sfide alla privacy: la re-identificazione dei dati anonimi e il trattamento dei dati personali per ulteriori finalità. Le due possibilità, curiosamente, non hanno ricevuto finora la meritata attenzione dalla dottrina specializzata, rimanendo in un "limbo" giuridico che potrà portare dei seri problemi alla difesa della privacy.

Alcuni recenti sviluppi tecnologici riguardanti la re-identificazione dei dati anonimi hanno richiamato l'attenzione su uno dei concetti fondamentali della protezione dei dati: la loro tassonomia. Infatti, la possibilità di deanonimizzazione dei dati insieme alla grande offerta di dati personali risultante dal Data Mining hanno non soltanto creato una nuova categoria - "Big Data", ma hanno anche cambiato l'approccio al concetto di dato anonimo o statistico, richiedendo il cambiamento della natura di alcuni degli strumenti e istituti ormai classici nella protezione dei dati.

La tendenza - presente nella stragrande maggioranza delle leggi riguardanti la protezione dati - a considerare i dati anonimi o statistici come l'esatto contrario dei dati personali e, di conseguenza, non sottoposti alla normativa che regola questi ultimi, è una visione binaria troppo semplice e riduttiva, che non prende in considerazione la nuova realtà tecnologica, specificamente i progressi tecnologici nel campo della re-identificazione dei dati anonimi. Come l'articolo proverà a dimostrare, la divisioni binaria tra dati personali e dati anonimi viene meno nella riconsiderazione del concetto dei dati anonimi e dei suoi diversi profili normativi. Tenendo conto di questa

[1] Mario Viola e Norberto Andrade sono dottorandi nel Dipartimento di Giurisprudenza dell'Istituto Universitario Europeo di Firenze. Danilo Doneda è consigliere legale del Ministero della Scienza e Tecnologia di Brasile sul tema della protezione dei dati personali. Gli autori vogliono ringraziare la Professoressa Camilla Salvi, dell'Istituto Universitario Europeo, per la correzione dell'italiano.

insufficienza, l'articolo svilupperà anche una distinzione fra dati personali e dati anonimi – compresi quelli per scopo statistico - con l'obiettivo di chiarire quando i dati possano veramente essere considerati anonimi e, di conseguenza, possano evitare l'incidenza della normativa sulla protezione dei dati personali.

L' altra sfida alla privacy oggetto di analisi sarà il trattamento dei dati personali per ulteriore finalità. In questa materia, nuovi criteri devranno guidare la utilizzazione dei dati, siano questi anonimi o meno, per finalità altre da quelle originarie.

In questo senso, il contributo si propone di identificare i più frequenti usi ulteriori dei dati personali, focalizzandosi sul settore privato, ed anche i criteri adottati delle autorità europee per la protezione dei dati allo scopo di valutare se un ulteriore uso sia legittimo.

2. Dati personali, dati anonimi e dati statistici

Prima di affrontate il discorso sul trattamento dei dati anonimi e statistici è importante esaminare la definizione di dati personali che, secondo quanto stabilito dal codice per la protezione dei dati personali, corrispondono a "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".[2]

Nell'ambito della categoria dei dati personali è stata individuata la sotto-categoria dei cosiddetti dati "sensibili", i quali sono definiti come "i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale".[3] È importante sottolineare che il trattamento realizzato a partire da altre informazioni di carattere personale può essere qualificato come un trattamento sensibile dei dati personali, come la Corte Costituzionale Tedesca ha già osservato nel giudizio sulla legge del censimento del 1983, poiché anche partendo dai dati non sensibili il trattamento potrebbe consentire di ottenere informazioni ritenute sensibili.[4]

[2] Articolo 4(b).
[3] Articolo 4(d).

Resta ugualmente necessario definire anche il concetto di dato anonimo, sia per fini statistici che per la protezione dei dati stessi. Nell'Unione Europea il concetto di dato anonimo continua ad essere costruito in modo da riflettere un dato che non è collegato ad una persona identificata o identificabile. È in questo senso, infatti, che la definizione viene adottata dal legislatore italiano:

> "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile

La caratterizzazione di un dato come anonimo ha una notevole importanza, nel senso che le informazioni che non sono suscettibili di essere collegate ad una persona identificata o identificabile possono, invece, indurre la non-applicazione delle norme in materia di protezione dei dati o eventualmente la sua applicazione in modo individualizzato. Diversi ordinamenti giuridici prevedono, per esempio, una procedura di anonimizzazione del dato personale in relazione al soggetto corrispondente come requisito per il libero trattamento di questo dato in determinate circostanze.

Si noti, tuttavia, che la distinzione tra i dati personali e i dati anonimi non è assoluta e recentemente diversi dubbi sono stati sollevati riguardo alla sua validità come eccezione alla applicazione di norme in materia di protezione dei dati personali. Questo perché moderne tecniche di trattamento dei dati applicati a volumi di dati personali anonimi (e quindi liberamente utilizzati in base al concetto dominante nella maggior parte delle leggi sulla protezione dei dati), sono in grado di recuperare la connessione tra un'informazione anonima e il suo detentore.

Per quanto concerne la relazione tra le tecniche di anonimizzazione[5] dell'informazione personale e la sicurezza su cui il legislatore contava, è da richiamare all'attenzione uno studio realizzato nel 2000 da Latanya Sweeney. Questa specialista in informatica ha dimostrato che era possibile determinare l'identità dell'87% dei cittadini nordamericani a partire da sole tre

[4] "Un dato insignificante di per sé può acquisire un nuovo valore: cosi, non esistono più dati che possono essere considerati insignificanti nel contesto dell'elaborazione elettronica dei dati." Leonardo Martins. (org.) Cinqüenta anos de Jurisprudência do Tribunal Constitucional federal Alemão. Montevidéu: Fundação Konrad Adenauer, 2005, p. 244 e 245.

[5] La parola 'anonimizzazione' è un derivato del anglicismo 'anonymization' che è stato utilizzato sia dal Garante Europeo per la Protezione dei Dati, che dalla Commissione Nazionale Portoghese per la Protezione dei Dati con il significato di 'disaccoppiamento'." É anche in questo senso che la parola verrà utilizzata in questo testo, cioè, quello di rendere anonimo un dato personale.

informazioni non identificate (in cui cioé la corrispondenza con il soggetto detentore non era stata definita).[6]

In uno studio recente, Paul Ohm ha attestato che le tecniche di anonimizzazione dei dati personali, ossia la dissociazione tra le informazioni riguardanti un soggetto e il soggetto stesso che non potrà più essere identificato soltanto a partire da esse, sono ormai essenzialmente fallaci. Ohm giunge a questa conclusione considerando le ampie possibilità di re-identificazione, vale a dire il ricorso a tecniche statistiche e matematiche che permettono, attraverso l'incrocio di diverse banche-dati, che le informazioni originalmente anonime identifichino nuovamente il loro effettivo detentore.[7] In breve, l'idea di Ohm è che tutte le informazioni potrebbero diventare personali se combinate con altre informazioni rilevanti, seppur anonime.[8]

Questa volatilità del concetto di dato anonimo non è passata inosservata visto che oggi la tendenza internazionale procede verso la distinzione tra dati anonimi per scopi statistici e dati anonimi per scopi di protezione dei dati. Il Gruppo dell'Articolo 29, in un parere su questioni di protezione di dati relativi ai motori di ricerca su internet, ha rilevato che un determinato dato può essere considerato anonimo, e pertanto al di fuori del campo di applicazione della direttiva sulla protezione dei dati, solo se la sua anonimizzazione è completamente irreversibile, permettendo cioé al soggetto detentore di questo dato di non essere più identificato o identificabile.[9] L'anonimizzazione completa, tuttavia, anche se possibile non sarà un compito facile sia dal punto di vista tecnico che dal punto di vista dell' adeguamento alle norme di protezione dei dati.[10]

Il Garante europeo della protezione dei dati nell'esaminare questo tema ha stabilito una netta distinzione tra "dati anonimi" o "anonimizzati", ai fini della normativa di protezione dei dati, e "dati anonimi statistici." I primi consistono in tutte le informazioni relative ad un singolo individuo attraverso le quali questo individuo non può essere identificato, né dal responsabile per il

[6] <http://lab.privacy.cs.cmu.edu/dataprivacy/papers/LIDAP-WP4abstract.html>

[7] Ohm, Paul. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (August 13, 2009). University of Colorado Law Legal Studies Research Paper No. 09-12. Disponibile a SSRN: http://ssrn.com/abstract=1450006 .

[8] La relatività degli effetti di anonimato in relazione ai dati personali viene specificamente considerata, negli ultimi tempi, dall'industria stessa. Come per esempio, nel social network Buzz (www.buzz.com/), la sua politica della privacy chiarisce che: "Note that anonymity is not privacy. It might be possible for someone to accurately determine that you are the author of a particular piece of information, based on other contextual information. For example, if you are friends with only two other people in your community, and you ask a question that they then answer, it would not be difficult for a fourth person to surmise that you asked the question. For this reason, you should not use buzz.com to share information that requires a guarantee of secrecy.". <http://buzz.com/sharing/>.

[9] Gruppo di Lavoro Articolo 29 per la protezione dei dati. Parere 1/2008 in materia di protezione dei dati relativi ai meccanismi di ricerca. p. 22. Disponibile a: <ec.europa.eu>.

[10] Ian Walden. Anonymising Personal Data. International Journal of Law and Information Technology. Vol 20, N° 2. Oxford University Press, 2002. P. 226. "Achieving effective anonymisation may be a challenging task, from both a technical and compliance perspective. Sophisticated data analysis and data mining techniques on supposedly anonymous data may eventually yeld data that does 'directly or indirectly' relate to a specific individual (…)."

trattamento né da qualsiasi altra persona. Inoltre, questa definizione dovrà tenere conto di tutti i mezzi che possono essere ragionevolmente utilizzati dal responsabile per il trattamento dei dati o da qualsiasi altra persona per identificare l'individuo in questione. I dati anonimi consistono quindi in quei dati che precedentemente si riferivano ad una persona identificabile, ma che ha cessato di esserlo. I dati anonimi statistici, invece, consistono in quei dati per i quali non è possibile un'identificazione diretta. Questa definizione implica che la possibilità di identificazione indiretta potrebbe anche qualificare i dati in questione come anonimi dal punto di vista statistico, ma non necessariamente dal punto di vista della protezione dei dati."[11]

Per quanto riguarda la questione della persona identificata o identificabile, il Gruppo dell'Articolo 29, analizzando il concetto dei dati personali, ha cercato di stabilire una distinzione tra di essi. A parere del Gruppo, "un individuo può essere considerato identificato quando tra un gruppo di persone, lui o lei è distinto da tutti gli altri membri del gruppo. Allo stesso modo un individuo è identificabile quando, nonostante il fatto di non essere stato ancora identificato, è possibile farlo".[12]

È da rilevare, inoltre, che la stessa direttiva europea nel suo considerando 26 prevede un criterio per stabilire se una determinata persona è identificabile oppure no:

> "per determinare se una persona è identificabile, è opportuno prendere in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona; che i principi della tutela non si applicano a dati resi anonimi in modo tale che la persona interessata non è più identificabile; che i codici di condotta ai sensi dell'articolo 27 possono costituire uno strumento utile di orientamento sui mezzi grazie ai quali dati possano essere resi anonimi e registrati in modo da rendere impossibile l'identificazione della persona interessata;"

---

[11] Parere del Garante europeo della protezione dei dati sulla proposta di regolamento del Parlamento Europeo e del Consiglio relativo alle statistiche europee [COM(2007) 625 final]. P. 4. Disponível em: <www.edps.europa.eu>. La stessa posizione può essere trovata anche nel Parere del garante europeo della protezione dei dati, sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo alle statistiche comunitarie sulla sanità pubblica e sulla salute e sicurezza sul luogo di lavoro [COM(2007) 46 definitivo]. P. 4. "18. L'analisi è simile per il concetto di anonimato. Benché dal punto di vista della protezione dei dati il concetto di anonimato riguardi dati non più identificabili (v. considerando 26 della direttiva), da un punto di vista statistico i dati anonimi sono quelli che non possono essere identificati direttamente. Da un punto di vista statistico, in base a questa definizione, i dati identificabili indirettamente vengono considerati dati anonimi."

[12] Gruppo di Lavoro sulla Protezione dei Dati del Articolo 29. Parecer 4/2007 su il concetto dei dati personali. P. 13. Disponibile a: <ec.europa.eu>.

Questo vuol dire che non basta che esista la possibilità di identificare la persona, questa possibilità d'identificazione deve essere ragionevole. La Raccomandazione R (97) 15 del Comitato dei Ministri del Consiglio d'Europa sulla protezione dei dati sanitari, nel suo articolo 1 (1) ritiene che un dato non dovrebbe essere considerato come 'identificabile' se questa identificazione necessita un ecessivo volume di tempo e di manodopera.[13] Nello stesso modo prevede la legge tedesca sulla protezione dei dati, quando stabilisce che un dato "sarà considerato 'spersonalizzato' solo se la persona può essere identificata con un'enorme quantità di tempo, denaro e lavoro."[14] [15]

Così, se le misure necessarie per identificare la persona legata al dato che viene trattato è sproporzionata, questo dato non sara considerato come dato personale, ma soltanto anonimo e, come conseguenza, non sottomesso alle regole di protezione dei dati.[16]

3. La finalità della raccolta e l'utilizzo dei dati per altri scopi – Un esame di proporzionalità

L'utilizzo dei dati personali da parte di vari attori delle relazioni del consumo di massa non può essere fatto indiscriminatamente, essendo fondamentale l'applicazione di alcuni parametri per governare tale utilizzo, tra i quali il più rilevante è il principio della finalità.

---

[13] Council of Europe, Committee of Ministers, Recommendation No. R (97) 5 on the Protection of Medical Data (Feb. 13, 1997). "1. Definitions. For the purposes of this recommendation:
- the expression "personal data" covers any information relating to an identified or identifiable individual. An individual shall not be regarded as "identifiable" if identification requires an unreasonable amount of time and manpower. In cases where the individual is not identifiable, the data are referred to as anonymous". Disponibile a: www.coe.int (17.11.2009).

[14] Apud Ian Walden. Anonymising Personal Data. In: International Journal of Law and Information Technology. Vol 20, N° 2. Oxford University Press, 2002, p. 226.

[15] Il Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientific in Italia stabilisce, all'articolo 4 (1) (b) un mezzo che può essere considerato ragionevole per identificare un determinato interessato.
"Art. 4. Identificabilità dell'interessato
1. Agli effetti dell'applicazione del presente códice (...)
b) i mezzi ragionevolmente utilizzabili per identificare un interessato afferiscono, in particolare, alle seguenti categorie:
• risorse economiche;
• risorse di tempo;
• archivi nominativi o altre fonti di informazione contenenti dati identificativi congiuntamente ad un sottoinsieme delle variabili oggetto di comunicazione o diffusione;
• archivi, anche non nominativi, che forniscano ulteriori informazioni oltre quelle oggetto di comunicazione o diffusione;
• risorse *hardware* e *software* per effettuare le elaborazioni necessarie per collegare informazioni non nominative ad un soggetto identificato, tenendo anche conto delle effettive possibilità di pervenire in modo illecito alla sua identificazione in rapporto ai sistemi di sicurezza ed al *software* di controllo adottati;
• conoscenza delle procedure di estrazione campionaria, imputazione, correzione e protezione statistica adottate per la produzione dei dati;"

[16] Catarina Sarmento e Castro. Direito da informática, privacidade e dados pessoais. Coimbra: Almedina. 2005. P. 72.

Questo principio stabilisce che i dati devono essere raccolti per uno scopo specifico e compatibile con l'oggetto del contratto, e che la successiva utilizzazione deve essere sempre compatibile con la finalità iniziale per la quale i dati erano stati raccolti. Tuttavia, il principio della finalità non può essere considerato assoluto, dato che molte leggi che trattano del tema riconoscono la possibilità di utilizzare i dati raccolti per scopi diversi da quelli per i quali i dati erano stati raccolti, a condizione che la nuova finalità sia compatibile con quella iniziale[17] o quando la legge preveda espressamente la possibilità di utilizzo ulteriore del dato per un rilevante interesse pubblico. [18]

Ció significa che la richiesta di un dato deve essere collegata ad un negozio giuridico specifico tra il richiedente del dato (fornitore di servizi o prodotti) e l'interessato (consumatore).[19] Questo legame, però, non è assoluto e quindi la relazione tra l'uso dei dati e la finalità per cui erano stati raccolti non deve essere interpretata in senso stretto, ma come un rapporto di compatibilità e di adattamento tra le finalità e la modalità di raccolta. Esiste, dunque, un rapporto di proporzionalità tra le finalità del trattamento e gli interessi in gioco e la ragione della raccolta.

Per verificare questa proporzionalità, sono stati sviluppati alcuni criteri. I più rilevanti sono: 1) se l'individuo sia in grado di prevedere che i suoi dati verrano utilizzati a tale scopo (anche se non letteralmente citato);[20] 2) se i dati da trattare siano indispensabili per la realizzazione di attività previste; e, 3) se la finalità per la quale si desidera utilizzare i dati presenta un rilevante interesse pubblico.[21]

La compatibilità tra la ragione della raccolta e l'utilizzazione dei dati deve essere verificata mediante l'applicazione del principio della proporzionalità, consentendo l'uso di criteri specifici per

---

[17] "Schedule 1 to the Data Protection Act lists the data protection principles in the following terms: (...) 2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes." In: UK Information Commissioner. The Guide to Data Protection. Disponível em www.ico.gov.uk (19.12.2009).

[18] L'articolo 13 della Direttiva Europea 95/46/CE porta una serie di esempi di rilevante interesse pubblico, che possono derogare principi della protezione dei dati, tra i quali il principio della finalità.
"Articolo 13. Deroghe e restrizioni
1. Gli stati membri possono adottare disposizioni legislative intese a limitare la portata degli obblighi e dei diritti previsti dale disposizioni dell'articolo 6, paragrafo 1, dell'articolo 10, dell'articolo 11, paragrafo 1 e degli articoli 12 e 21, qualora tale restrizione costituisca una misura necessaria alla salvaguardia: a) della sicurezza dello Stato; b) della difesa; c) della pubblica sicurezza; d) della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali o di violazioni della deontologia delle professioni regolamentate; e) di un rilevante interesse economic o finanziario di uno Stato membro o dell'Unione europea, anche in material monetaria, di bilancio e tributaria; f) di un compito di controllo, ispezione o disciplina connesso, anche o occasionalmente, con l'esercizio dei pubblici poteri nei casi di cui alle lettere c); d); ed e); g) della protezione della persona interessata o dei diritti e delle libertà altrui."

[19] Antonio Herman de Vasconcellos e Benjamin et al. Código Brasileiro de Defesa do Consumidor Comentado pelos Autores do Anteprojeto. 7ª ed. Forense Universitária: Rio de Janeiro, 2001, pp. 389-390.

[20] Catarina Sarmento e Castro. Direito da informática, privacidade e dados pessoais. Coimbra: Almedina, 2005, p. 231.

[21] Parere nº 22/2001 della Comissione Nazionale per la protezione dei dati di Portogalo: <http://www.cnpd.pt/bin/decisoes/2001/htm/par/par022-01.htm>.

valutare se l'uso dei dati non sia ingiusto e se superi i limiti che potevano essere ragionevolmente previsti dagli interessati al momento della consegna dei dati. Tali criteri dovrebbero inoltre indicare se ci siano interessi rilevanti che potrebbero suggerire la necessità di una maggiore elasticità e tolleranza con un uso più ampio dei dati personali. Questa ponderazione non può essere fatta in astratto: "Solo analizzando il caso concreto, con un attento bilanciamento dei valori in gioco, è possibile ottenere la risposta."[22] Questi sono i parametri che limitano l'uso dei dati per fini diversi da quelli per i quali i dati erano stati inizialmente raccolti.

4. Modalità per il successivo trattamento dei dati più utilizzati nel settore privato – adeguatezza

L'uso più frequente dei dati personali per scopi diversi nel settore privato è, in generale, quello vincolato al marketing diretto - *targeting marketing* - in cui vengono selezionate le categorie di consumatori in accordo con delle determinate caratteristiche che si presume li qualifichino come potenziali acquirenti di un certo prodotto o servizio. Nell'analisi di questo trattamento è importante verificare la rilevanza della sua finalità. L'uso dei dati personali a fini di marketing diretto, anche se comune in molti settori, si verifica in uno spazio in cui la sua legittimità può essere contestata. Da una parte succede che i dati trattati a questo scopo siano spesso raccolti in circostanze in cui tale utilizzo non è comunicato all'interessato, dall'altra c'è l'esigenza che l'industria sia sottoposta a regolamentazione al fine di non generare discriminazioni nel mercato dei consumatori, dato che possono crearsi può provocare delle situazioni in cui la sua pratica consentirà la creazione di offerte adatte a determinate categorie di consumatori, escludendo però altre, "non qualificate" dai vantaggi e perciò escluse dall' acesso stesso a determinati prodotti. Questi ed altri problemi relativi al *targeting marketing* sono stati recentemente evidenziati in una relazione pubblicata dalla Federal Trade Commission degli Stati Uniti[23] che, oltre a richiamare l'attenzione sui rischi per la privacy dei consumatori che le pratiche di marketing comportamentale e simili rappresentano, punta ad un numero di principi di natura autoregolatoria[24] da seguire afinchè la tutela della privacy possa essere armonizzata con queste attività.

[22] Leonardo Roscoe Bessa. O Consumidor e os Limites dos Bancos de Dados de Proteção ao Crédito. São Paulo: Revista dos Tribunais, 2003. p. 187.
[23] Federal Trade Commission. Self-Regulatory Principles For Online Behavioral Advertising: Tracking, Targeting, and Technology. fev. 2009, <http://ftc.gov/os/2009/02/P085400behavareport.pdf>.
[24] I principi sono: (A) trasparenza e controllo da parte del consumatore dei suoi dati, (2) sicurezza ragionevole e limitazione della conservazione dei dati di consumo, (3) consenso esplicito per cambiamenti nelle politiche di privacy (4), consenso espresso informato, o divieto dell'uso di dati sensibili.

A livello europeo, la Commissione Europea ha approvato di recente un Codice di condotta e di autodisciplina per l'uso dei dati personali nelle attività di direct marketing, proposto dalla Federazione Europea di Direct Marketing. In questo Codice si possono osservare, al senso del 2.4, criteri di legittimità per l'uso di dati personali per scopi diversi da quelli per cui i dati dati sono stati originariamenti raccolti:

> "2.4 Scopi diversi
>
> 2.4.1 Qualora si desideri trattare i Dati Personali per uno scopo significativamente diverso da quello per il quale sono stati originariamente raccolti, il Responsabile del trattamento dei dati dovrà verificare che il nuovo scopo sia compatibile con lo scopo notificato. Qualora sia compatibile, il trattamento per questo nuovo scopo sarà consentito. Qualora il nuovo scopo sia incompatibile con lo scopo notificato, l'ulteriore trattamento sarà consentito solo se conforme alle vigenti leggi sulla protezione dei dati.
>
> 2.4.2 Nel valutare la compatibilità del nuovo scopo, il Responsabile del trattamento dei dati dovrà considerare, tra gli altri, i seguenti criteri: se il nuovo scopo è sostanzialmente diverso dallo scopo per cui i dati sono stati raccolti, se l'Interessato possa ragionevolmente averlo previsto o se sia probabile che avrebbe obiettato se ne fosse stato a conoscenza. Il Responsabile del trattamento dei dati dovrà sempre prendere in considerazione le indicazioni legali nazionali espresse dall'Autorità garante nazionale per la protezione dei dati."[25]

È possibile osservare che non esiste una vera e propria libertà assoluta di inviare pubblicità diretta ai consumatori[26] e che nemmeno il trattamento dei dati personali a scopi pubblicitari può godere di prerogative particolari, dato che per questo scopo di trattamento servono i parametri ordinari, applicabili ad altre situazioni, con la specificità che si tratta di un rapporto di consumo e, quindi, è doveroso riconoscere la priorità degli interessi dei consumatori. C'è, però, un'eccezione a queste limitazioni, quando esiste un rapporto commerciale

[25] Vedi Codice Europeo di condotta e di autodisciplina per l'uso dei dati personali nelle attività di direct marketing Federazione Europea di Direct Marketing. <http://ec.europa.eu/ >.

[26] Si osservi che anche in un ordinamento che è solitamente permissivo alle diverse tecniche utilizzate dal settore di marketing, come negli Stati Uniti, si afferma che il discorso pubblicitario (commercial speech) ha le stesse garanzie della libertà di espressione (free speech).

anteriore tra il consumatore e l'azienda che fa la comunicazione pubblicitaria. In questo rapporto anteriore è possibile identificare un eventuale consenso espresso dal consumatore per il trattamento dei suoi dati personali, oppure il consenso presunto.

In questo senso si è pronunciata la Autorità di Protezioni dei Dati personali del Regno Unito (*UK Information Commissioner*), quando ha riconosciuto la possibilità di trattamento dei dati personali con la finalità di fare marketing anche senza il consenso espresso dal titolare dei dati, sempre che ci siano tre condizioni: 1) che i dati personali siano ottenuti in contemplazione di una compravendita oppure nei rapporti di compravendita di prodotti o servizi; 2) che i messaggi pubblicitari inviati siano solo di prodotti o servizi similari a questi; 3) che sia data al titolarr dei dati personali la scelta di non permettere che i suoi dati siano utilizzati per scopi pubblicitari oppure, se il titolare non ha fatto uso di questa possibilità al momento della raccolta dei suoi dati, che gli sia sempre offerta questa possibilità al momento della consegna di ulteriori messaggi pubblicitari.[27]

Un'altra finalitá, di solito utilizzata dai settori finanziari e delle assicurazioni, è quella della lotta contro la frode. In questi casi, il trattamento dei dati personali ha lo scopo specifico di ridurre le distorsioni nel mercato causate da atti non leciti con l'obiettivo di ottenere vantaggi abusivi per gli operatori di tali mercati.

In questo caso particolare, si può notare un collegamento tra questo scopo e l'interesse pubblico, che sarebbe presente nella riduzione di queste distorsioni così come nella possibilità di controllare più accuratamente lo svolgimento di certe attività criminali.

La lotta alla frode può essere, così, un fattore da considerare nell'applicazione di alcuni dei principi di protezione dei dati personali. In questo senso, disponiamo dell' esperienza del DVLA (Driver and Vehicle Licensing Agency), un'agenzia del Regno Unito con competenza per fornire le autorizzazioni per i conduttori di veicoli. Questa agenzia, anche se deve osservare i principi di protezione dei dati personali presenti nel DAP (Data Protection Act, di 1998), ha usualmente fornito dati personali di veicoli e di conduttori alle pubbliche autorità che le richiedono, con una giusta ragione, così come a terzi che avessero una "causa ragionevole"[28]. Nella stessa direzione, ad esempio, é orientata la decisione dell'Autorità di Protezione dei Dati di Malta che, nelle sue linee guida sulla protezione dei dati per la promozione di buone condotte nel settore delle assicurazioni, riconosce come legittimo il trattamento dei dati personali con gli scopi di prevenzione

[27] Disponibile in <http://www.ico.gov.uk/for_organisations/topic_specific_guides/marketing.aspx>
[28] DVLA, "Request for information" de 5 de agosto de 2009, disponibile in <http://www.dft.gov.uk/dvla/foi/Disclosure/ReleaseofInfo.aspx>.

e lotta alla frode contro l'assicurazione privata, oltre a stabilire che questo trattamento può includere lo scambio di informazioni tra i diversi responsabili per il trattamento dei dati nell settore delle assicurazioni.[29]

Una terza ed ultima utilizzazione dei dati personali ha come fine agevolare il pagamento dei debiti. In questa ipotesi ci sembra che esista anche una possibile proporzionalità e legittimità nel trattamento di tali dati, sempre che sia "necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata".[30]

In questo senso, è interessante l'esempio dell'UK Information Commissioner, che riconosce non solo l'interesse legittimo di un' azienda a trasferire i dati personali di un consumatore ad un ufficio di protezione al credito senza il suo consenso quallora questo consumatore, dopo aver cessato di pagare i suoi debiti, abbia cambiato indirizzo senza farlo sapere all' azienda di cui era debitore, ma riconosce anche che l'interesse del titolare sui suoi dati non prevale sull'interesse dell'azienda in questa situazione.

5. Conclusioni

Il controllo sulle finalità dell' uso continua ad essere uno dei principi fondamentali di una politica di protezione dei dati personali. È doveroso, però, che sia presa in considerazione la sfida lanciata circa l'uso secondario dei dati personali - e che questo uso possa accadere in una scala molto ampia, con l'aiuto, per esempio, di tecniche come il *data mining*. Inoltre, è in crescita anche il ricorso all'uso secondario di dati personali per scopi pubblicitari, come per il *targeted marketing*, ad esempio. Questi fenomeni, sempre più sofisticati, suggeriscono che il cittadino titolare dei dati debba avere a sua disposizione mezzi di controllo sempre più efficaci sul trattamento dei suoi dati in queste circostanze.

Il controllo dello scopo del trattamento dei dati personali è oggetto di sfida anche per le tecniche di deanonimazzione dei dati personali, capaci di trasformare un grande volume di informazioni senza un titolare identificabile in un'informazione almeno potenzialmente identificabile e, dunque, personale - cosa che indebolisce concretamente la distinzione tra dati

[29] Disponibile in www.dataprotection.gov.mt (20.12.2009).
[30] V. art. 7º (f) della Direttiva Europea 46/95/CE.

personali e dati anonimi presente in diverse normative sulla protezione dei dati personali. Non è un caso che, in alcune normative di stati-membri dell'Unione Europea, siano considerati alcuni fattori aggiuntivi per caratterizzare un dato come anonimo, ovvero il tempo ed il lavoro necessari per l'identificazione del titolare di un dato specifico.

Dobbiamo riconoscere, perciò, che l'anonimità di un dato personale è un suo aspetto sempre più dinamico oltre che una sua caratteristica definitiva e statica. E che, anche nei casi in cui l'anonimità non è in gioco, ci siano delle eccezioni al divieto dell'uso secondario dei dati personali che possono fare a meno di una lettura rigida del principio della finalità, in particolare nelle occasioni in cui l'utilizzazione secondaria ha una natura compatibile con quella primaria, sempre che sia in conformità con gli altri principi e norme di protezione di dati.

Ciononostante, è importante sottolineare che questa utilizzazione secondaria dei dati personali come pure la re-identificazione dei dati anonimi sfidano la visione tradizionale del concetto del dato personale intrapresa dal legislatore comunitario, mettendo in pericolo la privacy dell'individuo. In tal senso, la nozione di dato personale inteso come elemento di durata ed esistenza limitata e destinato ad essere cancellato oppure anonimizzato dopo aver servito la finalità per la quale è stato creato, è chiaramente obsoleta. Come dimostrato in questo articolo, il rapporto tra dato personale e dato anonimo è ormai dinamico e reversibile, dal momento che esistono modi per prolungare l'esistenza del dato personale (tramite l'uso secondario di questi dati, compatibile con il principio della finalità) e modi per far ritornare il dato anonimo nel campo dei dati personali (tramite i nuovi e sofisticati processi di re-identificazione). In questo modo, più che una "ever-expanding category,"[31] il concetto di dato personale può anche diventare una "ever-lasting category," fatto che sicuramente lancerà in futuro delle importanti sfide alla privacy.

[31] Ohm, Paul: "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (August 13, 2009). University of Colorado Law Legal Studies Research Paper No. 09-12. Available at SSRN: http://ssrn.com/abstract=145006