diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

Big Data e segreto industriale: tra diritti, doveri e tutele

Autore: Vittoria Piretti
In: Diritto industriale

Introduzione

In un contesto di mercato possedere l'esclusiva sui propri dati raccolti nel tempo da parte delle società che offrono beni e servizi ad una platea di consumatori, potrebbe anche significare proteggere gli investimenti effettuati dall'azienda per la loro raccolta e per il loro trattamento.
Raccogliere ed analizzare i dati dei propri clienti ed utenti, o, in generale, dei soggetti che usufruiscono di determinati servizi, significa capirne i gusti e le abitudini di consumo in modo tale da poterne anticipare le necessità e le richieste e, nei casi più estremi, sulla base di una profilazione molto accurata, da poterne consentire il dirottamento della scelta del consumatore verso un determinato prodotto (creato ad hoc sulla base dei dati raccolti).

In relazione al contenuto dei database (da ora in poi anche DB) e al tipo di dati raccolti, non sarà poi possibile prescindere da alcune considerazioni in tema di trattamento dei dati personali: le informazioni che si raccolgono aventi ad oggetto indicatori che consentono l'identificazione o l'identificabilità di persone fisiche, dovranno necessariamente essere protette in relazione a quanto disposto da parte del Regolamento UE 679/2016 – GDPR in tema di tutela dell'interessato: l'essenza della protezione risiede nel fatto che le logiche di mercato hanno spesso a che vedere con il trattamento, la raccolta e l'analisi dei dati personali e ciò implica dei rischi in capo all'azienda se questi dati non sono trattati con tutele per l'interessato e adottando misure di sicurezza, tecniche ed organizzative efficaci.

Ma non solo. L'interessato[1], al contempo, nel portare a termine le transazioni commerciali, potrà anche rivestire la qualifica di consumatore[2] e, inevitabilmente, anche da questo punto di vista, dovrà essere tutelato in quanto parte debole del rapporto.
L'intersecarsi di tutti questi soggetti, quindi, non potrà prescindere dal garantire tutele e diritti in capo a tutti gli agenti del mercato: alla società (che dovrà avere tutele sul proprio patrimonio di dati e dovrà essere protetta da illecite intrusioni di terzi che in modo illegittimo tenteranno di sottrarre quanto contenuto nei loro DB) e, in aggiunta, all'interessato/consumatore (i cui dati verranno raccolti e trattati e la cui posizione di debolezza potrebbe essere sfruttata mediante un illecito uso dei dati che si riferiscono a quest'ultimo).

Ciò detto, però, la protezione dei dati personali deve necessariamente essere contemperata anche con altri diritti quali la libertà di impresa, di espressione, il diritto alla diffusione ed accesso alle informazioni ai fini di rendere effettivo lo sviluppo di un libero mercato comune in cui sia gli offerenti, che gli acquirenti possano muoversi liberamente, senza subire le posizioni dominanti di dati operatori economici o senza subire le restrizioni derivanti dalle alterazioni della concorrenza.

Su questa premessa, sarà quindi necessario domandarsi se il patrimonio aziendale costituito da tutti i dati raccolti nel tempo possa o meno essere considerato come segreto industriale.
E se, una volta individuato tale alla luce della normativa europea e nazionale, quali possano essere le necessarie tutele che le grandi azienda debbano mettere in moto per tutelare la posizione degli interessati il cui patrimonio di dati costituisce valore economico da parte di chi li detiene.

Big Data e segreto industriale

Di base non esiste un diritto di proprietà su un segreto industriale, anche se chi ha materialmente raccolto i dati è autorizzato a proteggerli dalla loro indebita divulgazione.

L'esclusività di certi dati, infatti, non garantisce un diritto di proprietà sui dati stessi, ma produce un diritto di esclusiva in pendenza del quale le terze parti non possono utilizzare questi dati.

A riprova di quanto detto, deve rilevarsi che non esiste un diritto di trasferibilità sui dati, esiste, invece, la tutela dell'interesse del terzo i cui dati vengono sottratti: ciò implica risvolti pratici soprattutto se i dati in questione sono dati personali.

Quindi, nell'ottica di un bilanciamento di tutti questi interessi coinvolti, si dovrà analizzare un modo per proteggere i database e i relativi diritti al loro accesso e utilizzo[3].

I diritti sul database, la connessa protezione dei dati personali in essi contenuti e la protezione del segreto industriale sono tre aspetti che, dato l'evolversi della situazione attuale, non possono essere scissi. Definire esattamente cosa sia un segreto industriale non è facile: non esiste una definizione universale dello stesso e, pertanto, l'assenza di una definizione univoca può inevitabilmente portare a dubbi intrepretativi e, conseguentemente, ad una difficile tutela del segreto stesso.

Alla commissione UE il tema non è sfuggito e nel giugno 2016 è stata adottata la direttiva on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943): l'intento che la direttiva si prefiggeva non era quello di stabilire un regime unitario di protezione del segreto commerciale[4] negli stati membri, quanto, piuttosto, di cercare di armonizzare tutte le leggi nazionali degli stati membri sul

punto, concentrandosi sulla illegittima sottrazione, diffusione e uso dei segreti commerciali affidando poi proprio agli stati membri, a seconda di quanto accadesse sul tessuto nazionale, l'effettiva tutela del patrimonio aziendale.

Analogamente al possesso dei big data, infatti, nell'attuale sistema economico e di mercato anche i segreti commerciali rivestono un ruolo importante e fondamentale per la tutela del know-how e del patrimonio aziendale: per segreto commerciale, oltre alle informazioni prettamente tecniche, devono anche intendersi tutti gli elementi relativi alle informazioni commerciali in possesso dell'azienda quali, ad esempio, dati di mercato e di potenziali clienti che non sono di pubblico dominio e che, proprio perché aventi natura così dettagliata e confidenziale, posseggono un valore economico enorme.
La giurisprudenza nazionale in tema di identificazione di informazioni segrete aziendali si è così espressa: "La tutela delle informazioni aziendali ricomprende tendenzialmente qualsiasi tipologia di segreto, potendo trattarsi di informazioni di carattere tecnico (come formule o procedimenti industriali) o commerciale (come tecniche di marketing, liste e classificazioni della clientela, politiche di prezzi e sconti)" (Trib. Venezia 16/07/2015).
Per quanto riguarda l'Italia, una definizione del concetto di segreto industriale è rinvenibile all'art. 98 del codice di proprietà industriale[5], così come aggiornato alla luce della citata direttiva.
Nel nostro caso nazionale, deve rilevarsi che non esistono parametri assoluti per valutare l'adeguatezza delle misure a protezione del segreto commerciale: lo stesso riferimento alla ragionevolezza contenuto nel dato normativo (art. 98 CPI, lett. c) implica che l'analisi vada fatta con riferimento al caso concreto, avuto particolare riguardo all'attività imprenditoriale svolta dal titolare, al tipo e alla natura delle informazioni per cui si chiede tutela.

Pertanto, in via esemplificativa, l'azienda che vorrà tutelare il proprio patrimonio di dati ed informazioni come segreto industriale dovrebbe cercare di proteggere i dati che ritiene di particolare valore dall'accesso indiscriminato di terzi o di dipendenti aziendali la cui funzione non sia strettamente connessa al loro trattamento.
In caso di comunicazione e/o diffusione degli stessi, poi, dovrebbe rendere esplicito il fatto che gli stessi siano qualificati come riservati o confidenziali e in caso di presentazioni/esposizioni dovrebbe fare in modo che queste informazioni nel loro insieme o nella precisa configurazione e combinazione dei loro elementi, non possano essere rese note o facilmente accessibili agli esperti e agli altri operatori del settore.

Come sopra riportato, quindi, stante l'assenza di un vero e proprio diritto universale che lo tuteli, i singoli stati UE si sono adoperati adottando leggi nazionali per offrire dei rimedi territoriali mirati contro l'illegittima acquisizione, l'uso e lo svelamento: tutto ciò, inevitabilmente, dati i diversi sistemi legislativi e giudiziari nazionali, ha però creato situazioni e tutele difformi, andando a compromettere il contenuto stesso del segreto commerciale così come individuato dalla direttiva.
In ogni caso, l'adozione di questo atto comunitario ha significato un primo passo verso la soluzione del vuoto legislativo, andando ad imporre a tutti gli stati membri una minima forma di armonizzazione e uniformità sul punto: ciò, si badi bene, senza imporre un diritto comunitario di tutela del segreto industriale, quanto piuttosto lavorando sulle definizioni per poterlo inquadrare ed introducendo forme di

Diritto & Diritti ISSN 1127-8579

risarcimento per l'illegittima sottrazione, uso o disvelamento dello stesso.
E, sebbene il punto sia ancora da dettagliare e definire, l'adozione di questa direttiva ha svelato un primo accorgimento da parte del legislatore comunitario rispetto l'inscindibilità tra la tematica del valore commerciale dei big data, la tutela del segreto commerciale e dei diritti dei dati personali degli interessati che vanno ad implementare le relative banche dati.

Big Data e protezione dei dati personali

Una prima forma di tutela rispetto al patrimonio dei dati raccolti – in relazione al contenuto del DB - è stata sicuramente attuata con l'introduzione del Regolamento UE 679/2016 – GDPR: l'essenza della protezione risiede nel fatto che le logiche di mercato hanno spesso a che vedere con il trattamento, la raccolta e l'analisi dei dati personali e ciò implica dei rischi in capo all'azienda se questi dati non sono trattati con le dovute tutele per l'interessato e adottando misure di sicurezza, tecniche ed organizzativi efficaci.

Molto spesso, in relazione alla tipologia dei dati raccolti ed immagazzinati, non deve essere sottovalutata la complessità della raccolta di quelli personali che, proprio per la loro specificità di individuazione dell'interessato anche a seguito di operazioni di combinazione, analisi e profilazione, necessitano di processi ben determinati e specifici e, soprattutto, dell'adozione di misure ad hoc per tutelare l'individuo i cui dati sono oggetto di raccolta[6].

In primo luogo giova rilevare che il concetto di tutela dei dati personali deve sempre essere bilanciato con altri interessi e diritti tra cui il diritto alla libertà di espressione, il diritto di accesso alle informazioni, il diritto alle arti e alla scienza libere.
Per comprendere bene quale sia la portata dell'importanza del trattamento dei dati personali in relazione alla gestione dei big data è opportuno richiamare alcuni concetti base stabiliti dal GDPR.
Nel dettaglio, il dato personale viene definito come qualsiasi informazione relativa all'interessato (persona fisica) e che si ricolleghi direttamente od indirettamente a quest'ultimo: il concetto di dati personali comprende tutte le informazioni che appartengono alla vita privata ma anche quelle relative alla professione o alla vita pubblica. Ciò è indipendente dalla modalità in cui questi dati sono raccolti. Per alcune categorie di dati (ad esempio quelli sensibili o particolari) servono poi delle cautele aggiuntive anche se, come nel caso di dati riguardanti le convinzioni politiche, religiose e filosofiche, gli stessi, se anonimizzati, potrebbero perdere il loro valore intrinseco.
Per trattamento, poi, si intendono tutte quelle tecniche automatizzate o manuali e quelle operazioni quali raccolta, registrazione, organizzazione, conservazione, modifica, adattamento, consultazione, uso, diffusione, trasmissione, combinazione, blocco, cancellazione, distruzione.

Diritto & Diritti ISSN 1127-8579

Infine, in relazione a determinate operazioni, sarà necessario tenere a mente il concetto di consenso richiesto all'interessato che, ai sensi dell'art. 4 GDPR deve intendersi quale qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso esprime il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, al trattamento dei dati personali che lo riguardano[7]. Il presupposto indefettibile è che il soggetto che conferisce il consenso abbia la capacità giuridica per farlo. In aggiunta, l'interessato non deve ricevere pressioni per prestarlo e deve essere debitamente informato sull'oggetto e sulle conseguenze della prestazione dello stesso. Deve essere validamente espresso e non deducibile per fatti concludenti e deve sempre poter essere revocato. Questo punto deve ritenersi fondamentale in relazione al fatto che, molto spesso, per la fruizione di determinati servizi o l'utilizzo di determinate piattaforme, l'utente, quale controprestazione del servizio stesso, è obbligato a rilasciarlo, senza essere debitamente informato di tutto ciò che verrà fatto con i propri dati.

In aggiunta a ciò, pare anche necessario richiamare alcuni principi introdotti dal GDPR affinché il titolare, nello svolgimento della propria attività, possa procedere con un corretto trattamento dei dati, nel rispetto dei diritti dell'interessato e che, segnatamente, sono:

- principio di liceità, trasparenza e correttezza: concretamente, i dati a norma potranno essere raccolti solo per una finalità specifica, espressa e lecita e il trattamento dovrà poi essere adeguato, proporzionato, rilevante e necessario relativamente alla finalità indicate ed esplicate in modo granulare all'utente;
- principio di limitazione delle finalità: concretamente, il trattamento dovrà essere effettuato legittimamente e potrà essere considerato tale solo se in accordo con quanto prescritto dalla legge, se persegue determinate finalità specifiche e se, all'interno di una società democratica, sarà necessario per raggiungere finalità lecite. Da ciò ne consegue il principio della finalità specifica e della limitazione del trattamento, ossia il titolare deve specificare e rendere manifesta la finalità prima di procedere, ogni nuova finalità per il trattamento dei dati deve avere delle specifiche basi giuridiche e non può riferirsi al fatto che i dati sono già stati raccolti e trattati ma con finalità diverse;
- principio di minimizzazione, esattezza, integrità e riservatezza: concretamente, solo i dati considerati adeguati, rilevanti e non eccessivi in relazione allo scopo possono essere trattati, nessuna informazione deve essere usata senza essere sicuri con ragionevole certezza che i dati siano accurati ed aggiornati;

- principio di limitazione della conservazione: per quanto riguarda le tempistiche di conservazione dei dati, sarà necessario procedere alla cancellazione degli stessi nel momento in cui non saranno più necessari per le finalità per le quali erano stati raccolti;

- principio di accountability: ossia la trasparenza del trattamento che si riflette sui rapporti tra titolare ed interessato. L'interessato deve sempre essere informato prima che i suoi dati vengano trattati e deve avere i dati di contatto del titolare, il titolare, inoltre, deve essere in grado di assicurare e di dimostrare la compliance con i principi del GDPR e di avere adottato tutte le misure tecniche ed organizzative e di sicurezza adeguate.
L'interessato, poi, deve sempre essere libero di esprimere il proprio consenso – libero ed informato- e, allo

Diritto & Diritti ISSN 1127-8579

stesso modo, deve poterlo revocare e deve potere esercitare tutti i diritti di cui agli art. 15 – 22 GDPR.
Infine, altro tema da non trascurare sono tutte le garanzie posto a tutela dell'interessato anche in tema di trasferibilità di dati in paesi extra-UE e che, ai fini della sicurezza del trattamento, dovrebbero garantire le stesse tutele previste dal GDPR (o attraverso l'adozione di BCC – Binding Corporate Rules o mediante l'adesione ai privacy shields, o mediante la redazione di accordi che regolino il trasferimento dei dati).

In conclusione, stante quanto esposto, l'essenza della protezione dei dati personali in collegamento alla tematica dei Big Data ha a che fare molto spesso con il trattamento dei dati in forma automatizzata: e ciò, proprio per le caratteristiche di identificazione/identificabilità dell'individuo, comporta rischi che, necessariamente, dovranno fare emergere debite forme di tutela nei confronti dell'utente.
Senza dubbio, i due ruoli maggiori in questo contesto li giocano l'interessato da un lato e il titolare (società), dall'altro: l'interessato – i cui dati vengono trattati- ricopre un ruolo vitale proprio per il valore dei propri dati e, a riprova di ciò, il GDPR gli fa disporre di tutta una serie di diritti per potere tutelare la propria posizione, senza eccezioni.

Il titolare, dall'altro lato, è colui che tratta quei dati. Questo processo necessita di essere lecito e con finalità predeterminate, la qualità, la sicurezza e la trasparenza dei processi deve sempre essere garantita dal titolare.

Big Data e tutela del consumatore

Le nuove sfide e opportunità per i servizi digitali forniti dalla raccolta e dall'analisi dei dati non possono prescindere dalla protezione del consumatore, dei suoi dati e dalla responsabilità di chi questi dati materialmente li processa.
Oggi la capacità di prevedere i comportamenti dei consumatori offre agli operatori del mercato la possibilità di innescare alcune reazioni attraverso annunci pubblicitari creati appositamente o attraverso altri messaggi ad hoc rinvenibili durante le operazioni di navigazione.
Questa capacità, se non correttamente normata, potrebbe poi trasformarsi in manipolazione dell'utente finale, poiché le risposte dei consumatori potrebbero basarsi su aspetti irrazionali della loro psicologia, su una mancanza di informazioni o su una situazione di bisogno.

In quest'ottica, il trattamento dei dati dei consumatori (in quanto parte più debole) è rilevante ai fini della legge sulla protezione dei loro dati: in primo luogo, l'uso dei big data da parte di venditori/ rivenditori e fornitori di servizi può introdurre ulteriori squilibri tra queste parti dal lato dell'offerta e i consumatori dal lato della domanda. In secondo luogo, l'uso manipolativo dei big data può limitare l'indipendenza dei consumatori. In terzo luogo, le decisioni automatizzate possono andare a svantaggio di determinati individui e gruppi e senza alcuna logica accettabile.

Nel dettaglio, è proprio grazie ai big data che gli operatori di mercato possono sapere cosa può

influenzare determinati consumatori in un modo o nell'altro.
Più in generale, sta emergendo una data economy in cui vengono raccolti e scambiati tutti i tipi di dati personali, il cui valore consiste proprio nei possibili usi per anticipare e modificare il comportamento delle persone.
Il modello di business basato sulla fornitura di servizi "gratuiti" pagati attraverso la pubblicità ha un impatto che va oltre l'e-commerce: al fine di esporre i consumatori agli annunci pubblicitari, le piattaforme devono attirare e mantenere i consumatori sui loro siti Web.
Gli Internet providers, quindi, hanno due diverse classi di clienti - inserzionisti e utenti - e devono tenere conto di entrambi: esiste un'interdipendenza tra inserzionisti e utenti in quanto per soddisfare gli inserzionisti, gli intermediari devono attirare e trattenere gli utenti.
In altre parole, l'attenzione e le informazioni dei consumatori sui consumatori sono le merci chiave che gli Internet providers vendono agli inserzionisti.
Al giorno d'oggi, infatti, gli utenti di servizi gratuiti non sono consumatori ma sono un prodotto di scambio.

I consumatori online, quindi, spesso si trovano in una relazione sbilanciata con fornitori di servizi e rivenditori: si pensi a potenti intermediari che forniscono servizi chiave, come l'accesso all'infrastruttura Internet, i motori di ricerca online, la condivisione dei contenuti social, il cloud computing e i pagamenti online.
Il meccanismo è questo: alcuni di questi servizi sono offerti gratuitamente agli utenti finali, perché supportati da entrate pubblicitarie. Gli annunci vengono automaticamente indirizzati ai singoli consumatori, il targeting si basa sulle informazioni raccolte tracciandole.
In sostanza, la “gratuità” del servizio viene ricompensata con i dati di chi materialmente ne usufruisce.
I risultati sono quelli che conosciamo come filter bubbles o echo chambers: le informazioni che le persone ricevono vengono selezionate dai motori di ricerca e si basano sull’assunto per cui persone simili saranno attratte o soddisfatte da medesime informazioni e, quindi, dato che le persone sono generalmente colpite da ciò che viene chiamato "bias di conferma" (preferiscono vedere ciò che è coerente con la loro mentalità), ricevono informazioni che convalidano e rafforzano le loro attuali convinzioni per poi essere indirizzati sulle abitudini di consumo[8].

Questi nuovi intermediari, quindi, tendono a godere di una posizione di monopolio o di oligopolio, poiché hanno il vantaggio di possedere grandi quantità di informazioni di cui molte vengono raccolte nel contesto della fornitura di servizi: nei servizi online ai consumatori avviene una trasmissione bidirezionale di informazioni: dal fornitore al consumatore, ma anche dal consumatore al fornitore.
I sistemi informatici gestiti da fornitori / commercianti possono osservare, verificare e analizzare tutti gli aspetti della transazione, registrando ogni carattere digitato su tastiera e ogni link cliccato. Pertanto, i monopoli sulla fornitura di servizi online tendono a diventare monopoli sui dati raccolti.

Attualmente, i dati personali dei consumatori vengono spesso estratti gratuitamente dai servizi online e quindi utilizzati e scambiati a vantaggio dei fornitori.

Diritto & Diritti ISSN 1127-8579

Una via d'uscita da questa situazione potrebbe consistere nell'accettare che i dati personali siano un bene negoziabile e, allo stesso tempo, garantire che anche gli interessati possano trarre qualche beneficio dall'uso fatto dei loro dati, esercitando anche un certo controllo su questi dati.
Seguendo questa strada, quindi, oltre ad apprestare maggiori tutele per i consumatori, i loro dati dovendo considerarsi come loro proprietà, in caso di scambio dovrebbero essere retribuiti e, in aggiunta, il consumatore dovrebbe potere avere la possibilità di potere scegliere in che modo e quali dei propri dati potrebbero essere trattati e diffusi.
Ciò, implicherebbe, un forte potere in capo alla parte più debole della transizione.

In alternativa, l'altra via d'uscita potrebbe consistere nell'escludere che i dati personali possano essere una merce negoziabile, con la conseguenza di impedire ai venditori di offrire servizi o vantaggi in cambio di dati personali: seguendo quest'ultimo approccio, quindi, i dati personali dovrebbero essere utilizzati solo quando necessario per fornire un servizio richiesto dai consumatori e non come qualcosa fornito in cambio di un servizio diverso.

Il diritto dell'UE non ha ancora scelto tra questi due modelli adottare, né ha trovato un modo per riconciliarli[9].
Una soluzione interessante per la tutela dell'interessato è fornita dal California Data Privacy Act, che richiede alle compagnie di accompagnare l'accesso al proprio sito Web con le parole "do not sell my data" per consentire agli utenti di escludere la trasmissione dei loro dati a terzi.

Ciò esposto, in tema di tutela dei dati del consumatore, sarebbe auspicabile utilizzare i nuovi sistemi di intelligenza artificiale per supportare i cittadini in modo che possano non solo sfruttare meglio le opportunità disponibili sul mercato, ma possano anche resistere e rispondere a comportamenti sleali e illeciti da parte di colossi aziendali.
Le tecnologie di IA, infatti, potrebbero essere utilizzate a loro volta per aiutare i consumatori a proteggersi da pubblicità e spam indesiderati, o per consentire di identificare i casi in cui vengono raccolti dati non necessari o eccessivi o in cui vengono fornite informazioni false e non affidabili, o per supportare i consumatori e le loro organizzazioni nell'individuare violazioni della legge, valutare la conformità e ottenere tutele giudiziali.
E potrebbe essere compito della pubblica autorità quello di sostenere e incentivare la creazione e la distribuzione di strumenti di intelligenza artificiale a beneficio dei consumatori, in quanto soggetti interessati e cittadini[10].

Conclusioni

In relazione a tutto quanto esposto, quindi, nell'ottica degli attuali processi di sviluppo aziendale e di digitalizzazione, nessuno dovrebbe sottostimare il valore dei dati e delle relative informazioni sia dal punto di vista di avviamento industriale, che commerciale che dal punto di vista del trattamento del dato

Diritto & Diritti ISSN 1127-8579

personale appartenente all'utente/interessato.
Il patrimonio costituito dai dati, infatti, si riversa in un possibile investimento finanziario basato sulla loro raccolta ed organizzazione e ciò si rapporta necessariamente al valore stesso dei dati all'interno della nostra società dell'informazione in cui il libero accesso agli stessi e la disponibilità di tutte le informazioni rendono gli individui parte di un processo di scelta e colonna portante della società dell'informazione stessa: corrispondenza tra messa a disposizione delle informazioni e richiesta.

Quanto riportato sopra, inevitabilmente, si scontra sulla struttura stessa del database che, per tutto quanto esposto in precedenza, all'interno di una società digitale sarà necessario proteggere dall'accesso dei terzi: la protezione dei dati in collegamento alla protezione dei dati personali diventa così parte fondante della tutela dell'individuo, ma ciò, inevitabilmente comporterà un accesso ristretto al diritto di informazione.

E, sebbene il punto sia ancora da dettagliare e definire, l'adozione di queste normative e l'attuazione da parte degli stati membri di leggi in materia, rappresenta un primo passo di sensibilizzazione rispetto l'inscindibilità tra la tematica del valore commerciale dei big data, la tutela del segreto commerciale e dei diritti dei dati personali degli interessati che vanno ad implementare le relative banche dati.

Volume consigliato

Note

[1] Rif. Art. 4 GDPR - una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

[2] Rif. Art. 3 Codice del Consumo - consumatore o utente: la persona fisica che agisce per scopi estranei all'attività imprenditoriale, commerciale, artigianale o professionale eventualmente svolta

[3] Per la definizione di database si veda Database directive on the protection of databases 1996 OJ L. 77/20 che lo individua così come segue:
- una raccolta di materiale indipendente (ossia dati che non si interfacciano con altri dati in un sistema di interscambio);

- in cui i dati raccolti devono essere accessibili individualmente.

[4] L' Art.2 della direttiva definisce così il «segreto commerciale»: sono informazioni che soddisfano tutti i

Diritto & Diritti ISSN 1127-8579

seguenti requisiti:
a) sono segrete nel senso che non sono, nel loro insieme o nella precisa configurazione e combinazione dei loro elementi, generalmente note o facilmente accessibili a persone che normalmente si occupano del tipo di informazioni in questione;
b) hanno valore commerciale in quanto segrete;
c) sono state sottoposte a misure ragionevoli, secondo le circostanze, da parte della persona al cui legittimo controllo sono soggette, a mantenerle segrete.
2) è «detentore del segreto commerciale», qualsiasi persona fisica o giuridica che controlla legittimamente un segreto commerciale;
3) è «autore della violazione», qualsiasi persona fisica o giuridica che ha illecitamente acquisito, utilizzato o divulgato un segreto commerciale;
4) sono «merci costituenti violazione», le merci di cui la progettazione, le caratteristiche, la funzione, la produzione o la commercializzazione beneficiano in maniera significativa di segreti commerciali acquisiti, utilizzati o divulgati illecitamente.

[5] Costituiscono oggetto di tutela i segreti commerciali. Per segreti commerciali si intendono le informazioni aziendali e le esperienze tecnico-industriali, comprese quelle commerciali, soggette al legittimo controllo del detentore, ove tali informazioni:

a) siano segrete, nel senso che non siano nel loro insieme o nella precisa configurazione e combinazione dei loro elementi generalmente note o facilmente accessibili agli esperti ed agli operatori del settore;

b) abbiano valore economico in quanto segrete;

c) siano sottoposte, da parte delle persone al cui legittimo controllo sono soggette, a misure da ritenersi ragionevolmente adeguate a mantenerle segrete (…)".

[6] Sul punto si veda, J. Pila, P. L. C. Torremans, European Intellectual Property Law, 2nd Ed., Oxford University Press, 2019

[7] Sul consenso si tenga anche in considerazione considerando 32 GDPR: "il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire

Diritto & Diritti ISSN 1127-8579

immotivatamente con il servizio per il quale il consenso è espresso".

[8] si veda Prof. G. Sartor, STUDY, Requested by the IMCO committee and European Parliament, New aspects and challenges in consumer protection Digital services and artificial intelligence, Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies, April 2020

[9] Per una prima soluzione sul punto si veda Prof. G. Sartor, STUDY, Requested by the IMCO committee and European Parliament, New aspects and challenges in consumer protection Digital services and artificial intelligence, Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies, April 2020, secondo cui questo risultato può essere ottenuto considerando che la direttiva sui diritti dei consumatori non sostituisce il GDPR: se il consenso dei consumatori al trattamento dei loro dati non soddisfa i requisiti del GDPR, tale consenso non sarà valido e il trattamento da parte dei fornitori / commercianti sarà illegale. Tuttavia, i consumatori i cui dati sono stati trattati illegalmente dovrebbero comunque godere dei diritti dei consumatori ai sensi della direttiva 2019/770 e della direttiva 2011/83.

[10] Tra le innovazioni da prendere in considerazione al riguardo ci sono le seguenti: chiarire che le limitazioni di responsabilità si applicano anche ai motori di ricerca e ai social network; abbattere la distinzione tra intermediari attivi e passivi; chiarire che la portata del divieto di imporre ai fornitori di servizi un obbligo "generale" di impegnarsi nel monitoraggio si riferisce alla non disponibilità di tecnologie efficaci (AI) e al possibile impatto sulle libertà degli utenti. Le limitazioni alla responsabilità secondaria dei fornitori non dovrebbero applicarsi quando i fornitori hanno contribuito al comportamento illecito dei loro utenti non adottando misure ragionevoli che avrebbero potuto impedire tale comportamento o mitigarne gli effetti. Questo errore può anche dipendere dal fatto di non aver adottato le tecnologie più efficaci, cfr. Prof. G. Sartor, STUDY, Requested by the IMCO committee and European Parliament, New aspects and challenges in consumer protection Digital services and artificial intelligence, Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies, April 2020.

https://www.diritto.it/big-data-e-segreto-industriale-tra-diritti-doveri-e-tutele/

Diritto & Diritti ISSN 1127-8579