Privacy: le maggiori novità introdotte con il nuovo Regolamento Europeo sulla protezione dei dati personali di prossima applicazione.

*Sommario: Introduzione. – Le disposizioni generali del Regolamento. – Oggetto e finalità (art. 1). – Ambito di applicazione materiale e territoriale (artt. 2 e 3). – Nuove tipologie di obblighi e responsabilità. – Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (art. 25). – Principio di rendicontazione o di "*accountability*". – Violazione dei dati personali (artt. 33 e 34). – Registro delle attività di trattamento (art. 30). – Valutazione d'impatto sulla protezione dei dati (art. 35). – Registro delle attività di trattamento (art. 30). – Valutazione d'impatto sulla protezione dei dati (art. 35). – Nuove figure: il* Data Protection Officer *(artt. 37 e ss.). – Diritti dell'interessato: il diritto all'oblio (art. 17). – Il meccanismo dello sportello unico. – Sanzioni (artt. 83 e 84). – Le linee guida. – Considerazioni finali.*

Introduzione.

Dopo un *iter* durato circa quattro anni, il 14 aprile 2016 l'Assemblea plenaria del Parlamento Europeo ha adottato in seconda lettura il Regolamento Europeo in materia di protezione dei dati personali[1] e la Direttiva relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali[2] (c.d. "pacchetto protezione dati").
Il Regolamento (UE) 2016/679 mira ad introdurre una legislazione – in materia di protezione dati – uniforme e valida in tutta Europa, affrontando

[1] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
[2] Direttiva (UE) 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

temi innovativi come il diritto all'oblio e alla portabilità dei dati e stabilendo anche criteri che, da una parte, responsabilizzano maggiormente imprese ed enti rispetto alla protezione dei dati personali e, dall'altra, introducono notevoli semplificazioni e sgravi degli adempimenti per chi si conforma alle regole.
La Direttiva (UE) 2016/680 stabilisce, per la prima volta, norme comuni per il trattamento dei dati a fini giudiziari e di polizia all'interno di tutti gli Stati membri. Obiettivo della Direttiva, infatti, è quello di innalzare le garanzie per la *privacy* dei cittadini quando interviene un trattamento dei dati per motivi giudiziari e di polizia, ma anche di facilitare notevolmente lo scambio e l'uso delle informazioni utili per il contrasto a fenomeni come la criminalità e il terrorismo[3].
Il Regolamento e la Direttiva sono stati pubblicati il 4 maggio 2016 sulla Gazzetta Ufficiale dell'Unione Europea /GUUE). Il primo, vigente dal ventesimo giorno successivo alla pubblicazione in GUUE, sarà definitivamente e direttamente applicabile in tutti i Paesi UE *a partire dal 25 maggio 2018*, data per la quale dovrà essere garantito l'allineamento della normativa nazionale con le disposizioni del Regolamento. La Direttiva, invece, vigente *dal 5 maggio u.s.*, impegnerà gli Stati membri a recepire le sue disposizioni nel diritto nazionale *entro due anni*[4].

Le disposizioni generali del Regolamento

Oggetto e finalità (art. 1).
Fine ultimo del Regolamento è quello di stabilire un complesso normativo volto alla protezione del trattamento dei dati personali delle persone fisiche, nonché a disciplinare le regole sulla libera circolazione dei dati personali. Viene definita "dato personale" qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"), mentre il "trattamento" del dato consiste in qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o ad insieme di dati personali[5].

Ambito di applicazione materiale e territoriale (artt. 2 e 3)
Il Regolamento si applicherà sia al trattamento interamente o parzialmente automatizzato di dati personali, sia al trattamento non automatizzato di dati personali contenuti in un archivio[6] o destinati a figurarvi (art. 2). Lo stesso

[3] Garante per la protezione dei dati personali, *Il Parlamento UE approva in via definitiva il nuovo pacchetto protezione dati – Soro: si apre un percorso verso una più ampia tutela delle persone*, estratto da http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4889922 in data 30 dicembre 2016.
[4] Garante per la protezione dei dati personali, *Pubblicato sulla Gazzetta Ufficiale UE il nuovo pacchetto protezione dati*, estratto da http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4964718, in data 30 dicembre 2016.
[5] Vedansi definizioni all'art. 4, n. 1 e 2, del Regolamento (UE) 2016/679.
[6] "qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico" (art. 4, n. 6, del Regolamento (UE) 2016/679).

articolo stabilisce espressamente i casi sottratti alla portata di questa disposizione, tra cui i trattamenti effettuati dalle autorità di pubblica sicurezza.

Dal punto di vista "geografico", la nuova disposizione europea rovescia il tradizionale principio di stabilimento, sancendo l'applicabilità della disciplina dettata "*indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione*" e stabilendo l'applicazione delle sue regole anche nei confronti dei Titolari e Responsabili[7] non stabiliti nell'UE[8], quando le attività di trattamento riguardano:
a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

Nuove tipologie di obblighi e responsabilità

Il Capo II del Regolamento individua e disciplina i principi posti alla base della nuova normativa, ribadendo che i dati personali devono essere trattati nel rispetto degli obblighi di liceità, correttezza e trasparenza (artt. 5 e 12). Inoltre, introduce una serie di nuove tipologie di obblighi e responsabilità a livello europeo.

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (art. 25)
L'art. 25 del Regolamento introduce due differenti principi:
1.quello della "*privacy by design*", secondo cui il titolare del trattamento[9] deve adottare ed attuare misure tecniche ed organizzative, adeguate sin dal momento della progettazione oltre che nell'esecuzione del trattamento, che tutelino i principi di protezione dei dati[10]; e
1.quello della "*privacy by default*", il quale presuppone, invece, che il titolare del trattamento metta in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.
L'utente diventa quindi il punto di partenza per sviluppare il progetto in base alla legge sulla *privacy*, tramite un approccio *user-centric*. Pertanto, ogni volta che un progetto inizia deve prendere in considerazione, prima di

[7] Vedansi definizioni all'art. 4, n. 7 e 8, del Regolamento (UE) 2016/679.
[8] *Privacy: cosa cambia con il nuovo Regolamento Europeo*, di Andrea Fedi, Legance Avvocati Associati, maggio 2016.
[9] "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali […]" (art. 4, n. 7 del Regolamento UE 2016/679).
[10] Vedasi *sub* nota 8.

tutto, il ruolo dell'utente, progettando tutto attorno alla persona fisica[11].

Principio di rendicontazione o di "accountability".
In virtù di tale principio il Regolamento dispone che il responsabile del trattamento[12] debba adottare politiche ed attuare misure adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato risulta conforme allo stesso disposto normativo.
Ebbene, l'*accountability* investe tutte le operazioni dell'azienda, anche se lo stesso principio è nato con specifico riferimento alle informazioni economico-finanziarie e patrimoniali consuntive[13].

Violazione dei dati personali (artt. 33 e 34)
I dati personali che vengono conservati, trasmessi o trattati da aziende e pubbliche amministrazioni possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, ovvero di situazioni che possono comportare pericoli significativi per la *privacy* degli interessati cui si riferiscono i dati.
Pertanto, sulla base della normativa europea, il Garante per la protezione dei dati personali ha adottato negli ultimi anni una serie di provvedimenti che introducono in determinati settori l'obbligo di comunicare eventuali violazioni di dati personali ("*data breach*") all'Autorità stessa e, in alcuni casi, anche ai soggetti interessati. Il mancato o ritardato adempimento della comunicazione espone alla possibilità di sanzioni amministrative[14].
L'art. 33 prevede, infatti, che in caso di violazione di dati personali il titolare del trattamento notifichi la violazione all'autorità di controllo competente entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.
Va puntualizzato però che, mentre per la notifica all'autorità di controllo è richiesto "*un rischio per i diritti e le libertà degli individui*", per la notifica al diretto interessato è necessario che il rischio sia "*elevato*": in quest'ultimo caso, è richiesta una soglia di pericolo maggiore anche per evitare inutili allarmismi da parte dei soggetti interessati[15].

Registro delle attività di trattamento (art. 30)

---

[11] Nicola Fabiano, *Privacy by Design: l'approccio corretto alla protezione dei dati*, estratto da http://www.diritto24.ilsole24ore.com/art/dirittoCivile/2015-04-20/privacy-by-design-approccio-corretto-protezione-dati-personali-123915.php in data 10 gennaio 2017.
[12] "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento"(art. 4, n. 8, del Regolamento UE 2016/679.
[13] Michele Iaselli, *Protezione dei dati personali: il nuovo Regolamento Europeo in Gazzetta Ufficiale UE,* estratto da http://www.altalex.com/documents/news/2015/12/23/accordo-raggiunto-sul-regolamento-europeo-in-materia-di-protezione-dei-dati-personali in data 10 gennaio 2017.
[14] Garante per la protezione dei dati personali, *Violazioni di dati personali (data breach): gli adempimenti previsti – L'infonografica del Garante Privacy*, estratto da http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5033588 in data 10 gennaio 2017.
[15] Vedasi *sub* nota 8.

Altra novità di rilievo è l'introduzione dell'obbligo per ogni azienda titolare del trattamento dei dati di tenere un "registro delle attività" di trattamento, svolte sotto la propria responsabilità, nonché quello di effettuare una "valutazione di impatto sulla protezione dei dati".
Quest'ultimo adempimento, in particolare, è richiesto ad esempio in relazione *a*) ai trattamenti automatizzati, ivi compresa la profilazione, o con riguardo *b*) ai trattamenti su larga scala di categorie particolari di dati (sensibili), nonché relativamente ai dati ottenuti dalla sorveglianza sistematica, sempre su larga scala, di zone accessibili al pubblico. Sarà ad ogni modo il Garante Privacy (per quanto riguarda l'Italia), a redigere e rendere pubblico l'elenco delle tipologie di trattamenti soggetti al requisito della "valutazione di impatto sulla protezione dei dati".
Inoltre, va precisato come lo stesso art. 30 del Regolamento esoneri dai suddetti adempimenti le piccole e medie imprese, quelle dunque con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati (sensibili) o i dati personali relativi a condanne penali[16].

Valutazione d'impatto sulla protezione dei dati (art. 35).
Quando un tipo di trattamento prevede, in particolare, l'uso di nuove tecnologie e, considerata la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento è tenuto ad effettuare, prima di procedere, una valutazione d'impatto dei trattamenti previsti sulla protezione dei dati personali.
A tal proposito il titolare del trattamento che svolge una valutazione d'impatto sulla protezione dei dati dovrà consultarsi con il responsabile della protezione dei dati[17], qualora sia stato designato.
Inoltre, l'autorità di controllo redigerà e renderà pubblico un elenco delle tipologie di trattamenti soggetti al requisito della valutazione d'impatto sulla protezione dei dati, comunicandoli al Comitato europeo per la protezione dei dati[18]. La valutazione dovrà contenere: *a*) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento; *b*) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; *c*) una valutazione dei rischi per i diritti e le libertà degli interessati; e *d*) le misure previste per affrontare i rischi.
Infine, se necessario, il titolare del trattamento potrà procedere ad un riesame per valutare se il trattamento dei dati personali sia stato effettuato conformemente alla valutazione d'impatto sulla protezione dei dati.

[16] Gabriele Scafati, Stelè Perelli Studio Legale, La "*privacy europea", il Regolamento 2016/679*, estratto da http://www.diritto24.ilsole24ore.com/art/dirittoCivile/2016-05-16/la-privacy-europea-regolamento-ue-2016679-125453.php in data 9 gennaio 2017.
[17] Vedasi paragrafo 4.
[18] Organismo disciplinato all'art. 68 del Regolamento (UE) 2016/679.

Nuove figure: il *Data Protection Officer* (artt. 37 e ss.)

Tra i nuovi adempimenti è prevista l'adozione di una nuova figura professionale obbligatoria: il Responsabile per la protezione dei dati personali (*Data Protection Officer o "DPO"*).
Il *DPO* è un supervisore indipendente che sarà designato da soggetti apicali sia dalle pubbliche amministrazioni che in ambito privato. Pertanto, sarà obbligatorio all'interno di tutte *a*) le aziende pubbliche nonché in tutte quelle ove i trattamenti presentino specifici rischi, come ad esempio *b*) le aziende nelle quali sia richiesto un monitoraggio regolare e sistematico degli "interessati" su larga scala, e quelle *c*) che trattano i c.d. "dati sensibili".
Le società facenti parte di uno stesso gruppo, a livello nazionale o transfrontaliero, potranno nominare un unico *DPO*, a condizione che lo stesso sia facilmente raggiungibile da ciascuna società del gruppo stesso (art. 37, n.2 del Regolamento).

Il Responsabile per la protezione dei dati personali è tenuto a:
a) informare e consigliare il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento;
b) verificare l'attuazione e l'applicazione della normativa, oltre alla sensibilizzazione e formazione del personale e dei relativi auditors;
c) fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e a sorvegliare i relativi adempimenti;
d) fungere da punto di contatto per gli "interessati", in merito a qualunque problematica connessa al trattamento dei loro dati nonché all'esercizio dei loro diritti;
e) fungere da punto di contatto per il Garante per la protezione dei dati personali oppure, eventualmente, per consultare il Garante di propria iniziativa[19].
Infine, va sottolineato come non debba essere confusa la figura del *DPO* con quella di un responsabile *privacy ex* art. 29 del nostro Codice Privacy; sussiste, infatti, un elemento cruciale che differenzia le due figure: mentre il primo deve essere indipendente ed autonomo, il secondo deve agire seguendo soltanto le istruzioni del titolare del trattamento[20].

[19] Vedasi nota *sub* 16.
[20] Avv. Fabio Di Resta, Presidente del Centro Europeo per la Privacy (EPCE), *Il nuovo regolamento generale sulla protezione dei dati personali: un continente una legge, ma occorre essere preparati*, estratto da http://www.diritto24.ilsole24ore.com/art/dirittoCivile/2016-04-15/il-nuovo-regolamento-generale-protezione-dati-personali-continente-legge-ma-occorre-essere-preparati-171042.php in data 9 gennaio 2017.

Diritti dell'interessato: il diritto all'oblio (art. 17).

Una delle principali novità riguarda il diritto all'oblio, ovvero la possibilità per l'interessato di decidere che siano cancellati e non sottoposti ulteriormente al trattamento i propri dati personali. Tale diritto è oggetto di tre considerando nel preambolo del Regolamento[21]:

n.65 "Un interessato dovrebbe avere il diritto di ottenere la rettifica dei dati personali che la riguardano e il diritto all'oblio se la conservazione di tali dati violi il presente regolamento o il diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento […]";

n. 66 "Per rafforzare il diritto all'oblio nell'ambiente online, è opportuno che il diritto di cancellazione sia esteso in modo tale da obbligare il titolare del trattamento che ha pubblicato dati personali a informare i titolari del trattamento che trattano tali dati personali di cancellare qualsiasi link verso tali dati personali o copia o riproduzione di detti dati personali";

n. 156 "[…] Gli Stati membri dovrebbero essere autorizzati a fornire, a specifiche condizioni e fatte salve adeguate garanzie per gli interessati, specifiche e deroghe relative ai requisiti in materia di informazione e ai diritti alla rettifica, alla cancellazione, all'oblio, alla limitazione del trattamento, alla portabilità dei dati personali, nonché al diritto di opporsi in caso di trattamento di dati personali per finalità di archiviazione nel pubblico interesse, per finalità di ricerca scientifica o storica o per finalità statistiche […]".

Ebbene, secondo quanto disposto dall'art. 17 del Regolamento, è riconosciuta all'interessato la facoltà di decidere che siano cancellati e non sottoposti ulteriormente a trattamento i propri dati personali non più necessari per le finalità per le quali sono stati raccolti *ab origine*. Inoltre, alla lettera b) lo stesso articolo riconosce espressamente il "diritto all'oblio" anche nel caso di revoca del consenso o quando l'interessato si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al Regolamento.
L'art. 20, invece, stabilisce il diritto alla "portabilità dei dati", in virtù del quale l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati ad un altro titolare del trattamento senza impedimenti, qualora l'interessato abbia fornito il proprio consenso al trattamento o se questo sia necessario per l'esecuzione di un contratto[22].
In ambito nazionale il Garante della Privacy ha chiarito tramite una propria

[21] Laura Biarella, *Il nuovo diritto comunitario all'oblio: in vigore dal 25 maggio 2016*, estratto da http://www.diritto24.ilsole24ore.com/art/dirittoCivile/2016-05-25/il-nuovo-diritto-comunitario-oblio-vigore-25-maggio-2016-122503.php in data 10 gennaio 2017.
[22] Vedasi *sub* nota 16.

pronuncia[23] come lo stesso diritto all'oblio debba essere bilanciato con il diritto di cronaca; difatti, gli utenti non possono ottenere da Google la cancellazione dai risultati di ricerca di una notizia che li riguarda se si tratta di un fatto recente e di rilevante interesse pubblico[24].

Il meccanismo dello sportello unico.

Ulteriore novità è lo Sportello unico (c.d. *One-Stop-Shop*) che consente alle imprese con diversi stabilimenti in Europa di indirizzarsi verso un'unica Autorità garante nazionale, così garantendo una uniformità di applicazione della normativa *privacy* e semplificando notevolmente gli oneri burocratici, in quanto attualmente devono dialogare con ciascun Paese i cui è insediato lo stabilimento[25].

Sanzioni (artt. 83 e 84).

Il nuovo Regolamento prevede che ogni autorità di controllo (art. 51)[26] abbia il potere di imporre sanzioni amministrative. Le stesse verranno inflitte in funzione delle circostanze di ogni singolo caso, tenendo quindi conto della natura, della gravità e della durata della violazione, nonché del carattere doloso o colposo della violazione nonché degli altri fattori puntualmente elencati dallo stesso art. 83.
Le sanzioni oltre a dover essere proporzionate alla violazione posta in essere devono essere dissuasive, così da evitare che lo stesso soggetto reiteri il proprio comportamento. Pure se le autorità di controllo potranno stabilire autonomamente il *quantum* della sanzione tenendo conto degli indici sanciti dallo stesso Regolamento, tuttavia è la stessa disposizione europea che ne fissa l'importo pecuniario massimo che può essere applicato.

In effetti, a seconda del trasgressore (persona fisica o impresa) ed a seconda della violazione commessa, la sanzione potrà raggiungere un massimo di: *10.000.000,00 di euro*, o per le imprese, *fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente*[27]; alternativamente *20.000.000,00 di euro*, o per le imprese, *fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente*[28].

Inoltre, come stabilito dall'art. 84 saranno gli stessi Stati membri a stabilire

[23] Provvedimento del 18 dicembre 2014, Registro dei provvedimenti n. 618, doc. web n. 3736353.
[24] Garante per la protezione dei dati personali, Newsletter n. 400 del 31 marzo 2015, estratto da http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3822823 in data 10 gennaio 2017.
[25] Vedasi *sub* nota 20.
[26] Definita come "l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'art. 51", dall'art. 4, n. 21 del Regolamento (UE) 2016/679.
[27] Art. 83, paragrafo n. 4 del Regolamento (UE) 2016/679.
[28] Art. 83, paragrafo n. 5 del Regolamento (UE) 2016/679.

le norme relative alle altre sanzioni per le violazioni del Regolamento in questione, in particolare per le sanzioni amministrative pecuniarie non disciplinate dall'art. 83. Tali sanzioni dovranno sempre essere effettive, proporzionate e dissuasive[29].

I documenti del Gruppo dei Garanti UE (WP 29)

Il Gruppo dei Garanti Ue (WP 29) ha approvato lo scorso 13 dicembre tre documenti con indicazioni e raccomandazioni su importanti novità del Regolamento, in vista della sua applicazione da parte degli Stati membri a partire dal maggio 2018. Le Linee guida, alla cui elaborazione il Garante italiano ha attivamente partecipato, riguardano il "responsabile per la protezione dei dati" (*Data Protection Officer - DPO*), il diritto alla portabilità dei dati, " l'autorità capofila" che fungerà da "sportello unico" per i trattamenti transnazionali.

Le *Linee guida sul DPO* specificano i requisiti soggettivi e oggettivi di questa nuova figura, la cui designazione sarà obbligatoria per tutti i soggetti pubblici e per alcuni soggetti privati sulla base di criteri che il Gruppo ha chiarito nel documento. Nel documento vengono illustrate (anche attraverso esempi concreti) le competenze professionali e le garanzie di indipendenza e inamovibilità di cui il *DPO* deve godere nello svolgimento delle proprie attività di indirizzo e controllo all'interno dell'organizzazione del titolare.

Per quanto riguarda *il diritto alla portabilità*, il Gruppo evidenzia il suo valore di strumento per l'effettiva libertà di scelta dell'utente, che potrà decidere di trasferire altrove i dati personali forniti direttamente al titolare del trattamento (piattaforma di social network, fornitore di posta elettronica etc.) oppure generati dall'utente stesso navigando o muovendosi sui siti o le piattaforme messe a sua disposizione. Il documento esamina anche gli aspetti tecnici legati soprattutto ai requisiti di interoperabilità fra i sistemi informatici e alla necessità di sviluppare applicazioni che facilitino l'esercizio del diritto.

Infine, i Garanti Ue hanno chiarito i criteri per l'individuazione della *"autorità capofila"* che deve fungere da "sportello unico" per i trattamenti transnazionali (se il titolare o il responsabile tratta dati personali in più stabilimenti nell'Ue o offre prodotti o servizi in più Paesi Ue anche a partire da un solo stabilimento). Si tratta di un elemento importante del nuovo quadro normativo, al fine di aiutare i titolari o responsabili del trattamento a

[29] Il secondo paragrafo dell'art. 84 puntualizza che ogni Stato membro deve notificare alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 al più tardi entro il 25 maggio 2018, e comunicare senza ritardo ogni successiva modifica.

individuare correttamente l'autorità competente, così da evitare le controversie e garantire un'attuazione efficace del Regolamento[30].

Considerazioni finali.

Il nuovo Regolamento europeo sulla protezione dei dati si presenta come un insieme di regole assai complesso ma, al contempo, in grado di disciplinare gran parte degli aspetti di una *privacy* moderna ed "europea", attenta al nuovo mondo digitale e al flusso transfrontaliero dei dati.
La normativa europea, infatti, si propone di adattare la disciplina della *privacy* al mondo digitale: la tecnologia ha aumentato la diffusione di dati e cambiato il quadro di fondo, richiedendo una disciplina più coerente soprattutto nell'ottica di sviluppo della economia digitale.
A tal fine lo stesso disposto normativo cerca di fornire un livello di protezione equivalente in tutti gli Stati, pur lasciando alcuni margini agli Stati membri per regolamentare aspetti specifici[31].
Pertanto l'adeguamento delle singole legislazioni al nuovo Regolamento consentirà di rimuovere i contrasti e le mancanze di coordinamento normativo, mediante una disciplina sanzionatoria non più limitata a livello statuale, bensì declinata sui singoli attori.

[30] *Garante per la protezione dei dati personali, Privacy: nuovo Regolamento Ue, prime Linee guida dei Garanti europei*, estratto da http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5792160 in data 11 gennaio 2017.
[31] Giovanni Ziccardi, Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano, Professionisti e imprese: protezione dei dati con nuovi obblighi, estratto da http://www.ipsoa.it/documents/lavoro-e-previdenza/rapporto-di-lavoro/quotidiano/2016/04/29/professionisti-e-imprese-protezione-dei-dati-con-nuovi-obblighi in data 11 gennaio 2017.