IL REGOLAMENTO EUROPEO PRIVACY: UNA SVOLTA STORICA, MA SIAMO PRONTI?

Maria Rosaria Califano*

SOMMARIO: 1.- Premessa; 2.- Introduzione; 3.- Vecchi e Nuovi principi; 4.- Ampliamenti; 5.- Conclusioni.

1.- Premessa

Dal 25 maggio 2018 in tutte le aziende e nelle pubbliche amministrazioni di tutti gli stati membri, si applicherà il General Data Protection Regulation (GDPR), Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Pubblicato il 4 maggio 2016 nella Gazzetta Ufficiale dell'Unione Europea è entrato in vigore, così come prevede l'art. 99, il ventesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale (25 maggio 2016), ma si applicherà, appunto, a decorrere dal prossimo 25 maggio in ciascun stato membro[1].

Cosa e come cambia la disciplina, quali misure e adempimenti bisogna mettere in atto, quali processi avviare. Tenterò una sintesi delle novità più importanti e interessanti a partire dall'evidenza che il GDPR propone il tema della privacy come modello di organizzazione, gestione e controllo, non più come adempimento statico e formalistico[2].

2.- Introduzione

Il Regolamento abroga la Direttiva 95/46/CE la cosiddetta "direttiva madre" che era originariamente nata con due obiettivi:

- salvaguardare il diritto fondamentale alla protezione dei dati
- garantire la libera circolazione dei dati personali tra gli Stati membri.

Il Regolamento nasce in virtù di una riconosciuta esigenza di un quadro normativo più solido che *assicuri un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenga disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno*[3]*;* ma soprattutto perché, essendo aumentata significativamente la portata della raccolta e della condivisione dei dati personali, in seguito all'evoluzione tecnologica e alla globalizzazione, vi è bisogno di un livello più elevato di protezione dei dati personali, che sono ormai utilizzabili nello svolgimento di ogni attività. Pertanto, è opportuno che le persone fisiche abbiano il controllo dei propri dati personali e una certezza giuridica. Costituisce, una grande opportunità per aziende

*Funzionario Bibliotecario presso il Centro Bibliotecario di Ateneo dell'Università degli studi di Salerno.

[1] I regolamenti europei sono *self- executing* per cui non necessitano di alcun recepimento da parte degli stati membri: art. 288 comma 2 del Trattato sul funzionamento dell'Unione Europea (2012/C 326/01) versione consolidata.

[2] Cosi lo definisce Luca Bolognini, Presidente dell' Istituto Italiano per la Privacy e la Valorizzazione dei dati, http://www.lucabolognini.it/

[3] "Considerando" dell'art. 13 del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

pubbliche e private perché pone maggiore enfasi sulla circolazione dei dati rispetto alle implicazioni personalistiche del dato personale[4] ed è contemporaneamente una sfida in quanto nel mare magnum dei dati le aziende pubbliche e private devono analizzare e comprendere quali dati servono davvero e mettere in atto i meccanismi per proteggerli e sfruttarli rispettando i requisiti normativi.

Il testo ribadisce alcuni concetti fondamentali che sono alla base della stessa Direttiva e per quanto riguarda l'Italia, del Codice in materia di protezione dei dati personali, il D.lgs 30 giugno 2003 n. 196. È importante specificare che nel nostro Paese rimane in vigore tale decreto che a sua volta abrogava e sostituiva la Legge n. 675 del 1996 in attuazione della direttiva madre. In ambito europeo il Regolamento, insieme alla direttiva 2016/680, riformula la disciplina della privacy non la rivoluziona ma la innova e la armonizza notevolmente.

Primo concetto ribadito, la basilare premessa che la tutela delle persone fisiche con riguardo al trattamento dei dati personali è un diritto fondamentale[5], i principi e le norme a tutela, devono rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla nazionalità o dalla residenza dell'interessato. L'impianto messo in atto dovrebbe contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone. Altra importante premessa del Regolamento, condivisa con le precedenti normative, è che il trattamento dei dati personali deve essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ottemperanza al principio di proporzionalità (principio del pari grado). *Proteggere i dati personali vuol dire proteggere un elemento essenziale dell'essere umano, cioè va inteso – e così è palesemente inteso dal legislatore europeo sin dai Trattati – come diritto fondamentale strumentale alla tutela di altri diritti e libertà fondamentali* e non va considerata *come mera sicurezza dei dati personali* [6].

Tra gli obiettivi fondamentali del Regolamento vi sono quelli di garantire certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese; offrire alle persone fisiche in tutti gli Stati membri il medesimo livello di azionabilità dei diritti; definire obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento ed assicurare un monitoraggio costante del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri.

3.- Vecchi e Nuovi principi

Come già detto il Regolamento conferma i principi di base che ispirano tutta la disciplina della privacy e che devono servire da guida per qualsiasi trattamento.

Si tratta di quattro grandi principi:

[4] F. Piraino, *Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato* in *Le nuove leggi civili commentate* 40.2 (2017) 369 ss.

[5] L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea e l'articolo 16, paragrafo 1, del TFUE stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano

[6] L. Bolognini, *Valutazioni d'impatto sulla protezione dei dati (DPIA), attenzione ai malintesi interpretativi* in *http://www.istitutoitalianoprivacy.it/* 15 settembre 2017.

- principio di necessità;
- principio di proporzionalità;
- principio di finalità;
- principio di legittimità.

1.- Il **principio di necessità**

È quel principio per il quale il trattamento è lecito solo se è necessario al raggiungimento del fine, in altre parole l'identificazione dell'interessato è permessa laddove con altri mezzi non si riesce a raggiungere le medesime finalità. Secondo tale principio: *i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.*[7]

2.- Il **principio di finalità**

La raccolta e il successivo trattamento dei dati deve avvenire per un determinato motivo e non può in nessun caso eccedere. I dati devono essere raccolti per finalità determinate, esplicite e legittime, e quindi trattati secondo modalità compatibili con tale finalità. La finalità va dichiarata prima della raccolta, anche attraverso l'informativa all'interessato. Laddove non è specificata la finalità, il trattamento deve intendersi illegittimo.

3.- Il **principio di proporzionalità**

Tra i dati trattati e i gli strumenti per la raccolta ed il trattamento ci deve essere proporzionalità. Questo è un principio che sta acquistando sempre più valore in tutti gli ambiti del diritto pubblico e dell'azione amministrativa.

4.- Il **principio di legittimità**

Le finalità e le procedure attivate per i trattamenti devono essere legittimi, in nessun caso devono ledere i diritti dell'interessato.

Accanto a questi principi confermati vi sono molte e interessanti novità che se non conosciute e attivate rischiano di essere pericolose sia per le aziende ma soprattutto per i cittadini. Da un punto di vista manageriale, l'introduzione di nuovi principi e il mutato scenario tecnologico, obbliga ad una serie di responsabilità e adempimenti in capo a figure apicali delle organizzazioni ma anche a figure nuove che lo stesso Regolamento introduce, anzi obbliga a nominare. Un esempio è il responsabile della protezione dei dati, il c.d. Data Protection Officer[8]. Tutte le aziende pubbliche e private, ad eccezioni delle autorità giudiziarie, che trattano su larga scala dati sensibili, relativi alla salute o alla sfera sessuale o biometrici o comunque che richiedono un costante controllo dell'interessato, devono nominare un Responsabile. Il nome e i contatti del Responsabile devono essere resi noti anche nell'informativa sul trattamento.

È importante per le aziende e le pubbliche amministrazioni conoscere gli obblighi che derivano da quelli che potremmo definire i nuovi assi portanti del sistema[9] privacy e sono:

- il principio di accountability;
- la data protection impact assessment;

[7] Art. 3 del Codice in materia di protezione dei dati personali, Decreto legislativo 30 giugno 2003, n. 196.
[8] Art. 37 del Regolamento: Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati.
[9] M. Soffientini (curr.), *Privacy, protezione e trattamento dei dati*, Milanofiori Assago 2016, 31.

- la data breach notification;
- la privacy by design e by default.

Il **principio di Accountability**[10]

Potrebbe essere tradotto come "responsabilizzazione e obbligo di rendicontazione"[11], è l'obbligo in capo al titolare del trattamento di adottare politiche e attuare misure tecniche e organizzative per garantire ed essere in grado di dimostrare che il trattamento dei dati personali sia adeguato e conforme al Regolamento europeo.

Nel Regolamento viene specificato che il Titolare deve:

- essere in grado di *comprovare* di aver adottato adeguate misure tecniche ed organizzative;
- riesaminare e aggiornare le misure adottate in conformità a un principio di continuo miglioramento;
- adottare misure valutate di volta in volta, considerando una serie di elementi tra cui la natura, l'ambito di applicazione, il contesto e le finalità del trattamento;
- valutare i rischi connessi alla mancata adozione di misure non idonee.

Il principio di accountability. richiama due accezioni importanti che sottolineano l'introduzione di un nuovo approccio nella gestione della protezione dei dati da parte delle singole organizzazioni:

- mostrare all'esterno, in particolare agli stakeholder, di saper adottare un modello di gestione privacy affidabile e coerente con le finalità dei trattamenti;
- garantire all'interno della propria organizzazione logiche e meccanismi in grado di rafforzare la responsabilizzazione interna.

È un principio di effettività, cioè di effettiva garanzia verso l'interessato che vengono rispettati i suoi diritti, tutelati i dati.

Il **Data Protection Impact Assessment**

Il Regolamento introduce un istituto che è destinato a diventare il cardine del sistema privacy: il Data Protection Impact Assessment (DPIA[12]), ovvero il piano di valutazione di impatto sulla protezione dei dati personali. Con tale istituto si stabilisce che la valutazione è obbligatoria quando sono trattati dati sensibili o giudiziari e nei casi di automazione e profilazione. Il presupposto è la considerazione che ogni trattamento di dati personali presenta rischi per i diritti e le libertà degli individui, soprattutto se prevede l'uso di nuove tecnologie. La valutazione, che sostituisce l'obbligo generale di notificare alle autorità di controllo il trattamento dei dati personali, è richiesta nei casi in cui i dati:

a) sono trattati per prendere decisioni che hanno effetti giuridici o incidono in modo significativo sulle persone fisiche a seguito di valutazione sistematica e globale di aspetti personali basata su un trattamento automatizzato, compreso la profilazione;
b) personali rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale;
c) sono relativi a condanne penali e ai reati o a connesse misure di sicurezza;

[10] Art. 5 comma 2 del Regolamento: Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo (responsabilizzazione)

[11] M. Alovisio, F. Di Resta, *Norme privacy UE, ecco tutto ciò che bisogna sapere su accountability e sicurezza* in *https://www.agendadigitale.eu* 20 giugno 2016 (ultima consultazione 2 febbraio 2018)

[12] Art. 35 del Regolamento cit. Il DPIA va inquadrato come uno strumento essenziale e fondamentale per tutti i titolari e responsabili del trattamento al fine di dar corso al nuovo approccio alla protezione dei dati personali voluto dal legislatore comunitario e fortemente basato sul principio della responsabilizzazione (cd. *accountability principle*).

d) derivano dalla sorveglianza sistematica su larga scala di zone accessibili al pubblico;
e) sono genetici, biometrici o comunque intesi ad identificare in modo univoco la persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
f) trattati potrebbero incidere su un vasto numero di interessati a livello regionale, nazionale o sovranazionale.

La valutazione d'impatto va fatta prima del trattamento, per acquisire le necessarie conoscenze sulle misure, sulle garanzie e sui meccanismi previsti, per attenuare il rischio e assicurare la conformità del trattamento agli standard normativi. Se dalla valutazione emerge un grado elevato di rischi specifici deve essere consultata l'autorità di controllo prima dell'inizio delle operazioni, affinché verifichi se un trattamento rischioso sia conforme al Regolamento e formuli proposte per ovviare a tale situazione; è compito dell'autorità garante redigere e rendere pubblico un elenco delle tipologie dei trattamenti soggetti a rischio di valutazione d'impatto.

La valutazione deve contenere almeno:

1) - una descrizione dei trattamenti previsti e le finalità del trattamento (per il principio di finalità);
2) - l'interesse legittimo perseguito dal titolare del trattamento (per il principio di legittimità);
3) - la valutazione dei rischi per i diritti e le libertà degli interessati (per il principio di necessità);
4) - la necessità e la proporzionalità del trattamento in relazione alla finalità (per il principio di proporzionalità);
5) - la descrizione delle misure di sicurezze applicate e applicabili.

Il DPIA ha una valenza doppia in quanto è sia un processo finalizzato all'aggiornamento, miglioramento e adattamento, e sia uno strumento vero e proprio che garantisce al titolare del trattamento, la possibilità di dimostrare di avere eseguito la valutazione dell'impatto. Il Regolamento non stabilisce una periodicità di aggiornamento ma assegna al titolare l'onere della verifica della necessità di interventi modificativi.

È obbligo del titolare del trattamento effettuare la DPIA anche se quest'ultimo richiede di essere assistito dal responsabile del trattamento e anche se materialmente la valutazione è affidata ad un altro soggetto, magari esterno.

La **data breach notification**[13]

L'obbligo del titolare di comunicare le violazioni dei dati personali all'autorità di controllo perché una violazione dei dati personali se non affrontata in maniera adeguata e tempestiva può provocare danni fisici, materiali o immateriali alle persone fisiche: perdita del controllo dei dati personali o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della psudonimizzazione, pregiudizio della reputazione, perdita di riservatezza.

Il titolare ha l'obbligo, non appena viene a conoscenza della violazione, di darne comunicazione all'autorità, se possibile entro 72 ore, superate le quali deve giustificare il ritardo. Nei casi gravi, dove c'è rischio elevato per i diritti e le libertà della persona fisica, deve darne comunicazione anche all'interessato in modo da consentirgli di prendere tutte le precauzioni necessarie.

[13] Art. 33 del Regolamento disciplina il *data breach* prevedendo espressamente un obbligo di notifica e comunicazione in capo al titolare, in presenza di violazioni di dati personali che possano compromettere le libertà e i diritti dei soggetti interessati.

Le violazioni possono essere:
violazione della riservatezza - in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
violazione della disponibilità - in caso di perdita accidentale o non autorizzata di accesso o distruzione di dati personali;
violazione dell'integrità: in caso di alterazione non autorizzata o accidentale dei dati personali.
Fondamentale per il corretto assolvimento dell'obbligo stabilire, in via preliminare e concretamente, quando la violazione dei dati determini un "rischio", o un "rischio elevato", tale da far scattare, rispettivamente, l'obbligo di notifica all'autorità di vigilanza e di comunicazione agli interessati. *Prima ancora di definire una procedura di gestione della violazione, il titolare e il responsabile del trattamento, sulla falsariga di quanto prevede lo stesso GDPR in relazione alla valutazione d'impatto sulla protezione dei dati (DPIA), dovrebbe però effettuare una preliminare ricognizione dell'insieme dei dati personali trattati e dei rischi potenziali determinati dalle operazioni di trattamento ed attribuire un valore ai differenti dati personali che detiene e ai pericoli cui gli interessati sono esposti, determinando, così, la propria soglia di accettazione dei rischi e fissando le opportune strategie di azione.*[14]
La notifica al garante deve contenere:

a) la descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) le probabili conseguenze della violazione dei dati personali;
d) le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

La **privacy by design e by default**[15]
La privacy fin dalla progettazione e come impostazione predefinita: un approccio concettuale innovativo che impone l'obbligo di avviare un progetto prevedendo, fin da subito, gli strumenti a tutela dei dati personali. In altri termini, qualsiasi progetto ad impatto privacy deve nascere ed essere costruito con impostazioni di default, che rispetti la disciplina in tema di protezione dei dati personali[16].
È facile anche se non scontato capire le motivazioni, i principi che sorreggono questa impostazione[17]e sono:
- prevenire non correggere, cioè i problemi vanno valutati nella fase di progettazione, anche e soprattutto per impedire che intervengono;

[14] A. Nenzioni, *Data Breach Notification:le indicazioni del gruppo di lavoro articolo 29 per un corretto assolvimento dell'obbligo* in *Il quotidiano giuridico*, 1 dicembre 2017 http://www.quotidianogiuridico.it/ (ultima consultazione 2 febbraio 2018).
[15] Art. 25 del Regolamento impone al titolare del trattamento l'adozione di misure tecniche ed organizzative adeguate al fine di tutelare i dati da trattamenti illeciti.
[16] Soffientini, Privacy cit., 33.
[17] A. Cavoukian, *Privacy by Design, The 7 Foundational Principles Implementation and Mapping of Fair Information Practices* in *www.privacybydesign.ca* (ultima consultazione 2 febbraio 2018).

- privacy come impostazione di default, la protezione è automatica in qualsiasi sistema informatico o pratica commerciale;
- privacy incorporata nel progetto, non aggiunta;
- massima funzionalità, in maniera da rispettare tutte le esigenze (rifiutando le false dicotomie quali più privacy = meno sicurezza);
- sicurezza durante tutto il ciclo del prodotto o servizio perché già inserito nel progetto;
- trasparenza;
- centralità dell'utente attraverso setting forti e informative accurate e ben esposte.

Il sistema di tutela dei dati personali così delineato dal GDPR deve l'utente al centro, obbliga ad una tutela effettiva da un punto sostanziale, non solo formale. Non è sufficiente che la progettazione del sistema sia conforme alla norma, è necessario che l'utente sia effettivamente tutelato.

La privacy by design è senza dubbio la nuova dimensione della privacy che trae le sue origini dall'innovazione tecnologica e dal progresso delle comunicazioni elettroniche. Ribadisce che la tecnologia non può costituire una minaccia per la privacy, piuttosto un ausilio per la riduzione dei rischi. L'obbligo di privacy by design assicura che il trattamento sia adattato nel corso del tempo in quanto essendo basato sulla valutazione del rischio obbliga a considerare lo stato e l'evoluzione della tecnologia. Importante precisare che anche il concetto di *privacy by default* deve considerare i principi di necessità, di finalità e di proporzionalità, i dati personali vanno trattati solo nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. In fase di progettazione occorre assicurarsi e garantire che il sistema di trattamento di dati raccolti non sia eccessivo.

4.- Ampliamenti

Come più volte evidenziato, se da un lato sono numerosi i nuovi adempimenti introdotti dalla normativa comunitaria, d'altro lato restano invariati, ed anzi si rafforzano alcuni principi fondamentali regolanti l'ambito privacy. Rafforzati due strumenti fondamentali per la tutela degli interessati, l'informativa ed il consenso.

L'art. 12 rafforza il concetto di informativa come obbligo del titolare del trattamento nei confronti dell'interessato a motivo del principio della *trasparenza*[18]cardine non solo della disciplina sulla protezione dei dati personali. Ciascuno ha il diritto di essere informato sul trattamento dei propri dati sia prima dell'inizio del trattamento, attraverso l'informativa e sia successivamente grazie alla possibilità di accedere ai propri dati e controllarne l'utilizzo. L'informativa è stata sempre al centro della disciplina privacy, essendo presente sia nella legge n. 675/1996, che nel D. Lgs. n. 196/2003. L'informativa deve essere concisa, intelligibile, redatta con un linguaggio semplice e chiaro e deve contenere una serie di elementi considerati indispensabili perché l'interessato possa esercitare i diritti sui propri dati. Secondo il comma 1 dell'art. 13 del Codice Privacy, l'informativa non può essere generica ma deve contenere:

- le finalità e le modalità del trattamento cui sono destinati i dati;
- i diritti dell'interessato;
- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati.

Può essere fornita per iscritto o con altri mezzi elettronici e perfino oralmente se richiesto dall'interessato.

[18] Art. 5 comma 1 del Regolamento: i *dati personali devono essere trattati in modo lecito, corretto e trasparente*.

Non deve contenere dati già noti, cioè oggetti di precedente informativa e deve essere resa all'interessato prima del trattamento affinché questi possa controllare il flusso dei dati che lo riguardano: deve essere fornita all'interessato all'atto della registrazione dei dati o non oltre la prima comunicazione. Qualora il titolare del trattamento intenda trattare i dati personali per una finalità diversa da quella per cui sono stati raccolti, dovrebbe fornire all'interessato, prima di tale ulteriore trattamento, informazioni in merito a tale finalità diversa e altre informazioni necessarie. Comparando la vecchia (ma ancor vigente) disciplina al Regolamento, con riguardo all'informativa, si può senz'altro confermare che il suo perimetro è di certo più ampio e più dettagliato. L'informativa delineata è più intellegibile, più immediatamente comunicativa e accessibile, composta da un linguaggio chiaro e semplice. Può esser fornita anche con l'utilizzo di icone al fine di rendere il nucleo informativo più snello e fruibile.

Per quanto concerne, invece, il consenso della persona interessata è definito come "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento"*[19] . Da ribadire a chiare lettere che il consenso è un atto positivo, può essere una dichiarazione scritta o semplicemente firmata ma anche un'apposita casella in un sito web, ma non può prevedere il silenzio o l'inattività. Ogni organizzazione dovrà necessariamente verificare le modalità con cui viene richiesto, raccolto e gestito. Anche il consenso può essere reso oralmente tranne quando si tratta di dati sensibili. È legittimo quando è differenziato per trattamento, deve essere modulare, nel senso che l'esercizio dell'autodeterminazione informativa da parte dell'interessato deve riguardare le singole operazioni di trattamento o singole fasi dello stesso[20]. Solo nei casi in cui il trattamento è richiesto per legge o per la conclusione di un contratto come la fatturazione o per far valere un diritto in sede giudiziaria si può procedere al trattamento senza consenso. Il consenso rappresenta una spina nel fianco per le aziende sia da un punto di vista gestionale perché prima della data del 25 maggio devono verificare che i consensi raccolti rispettino la disciplina e sia in considerazione delle sanzioni previste. Nell'ipotesi della violazione delle disposizioni sull'obbligo del consenso, il Regolamento[21] prevede una sanzione che arriva fino a 20 milioni di euro o fino al 4% del fatturato annuo per il caso di violazione dei principi alla base del trattamento dei dati. Le organizzazioni perciò devono verificare che il consenso ottenuto prima dell'entrata in vigore del Regolamento abbiamo le caratteristiche stabilite, deve essere: libero, specifico, informato, verificabile, revocabile e soprattutto inequivocabile, caratteristica che non lascia scampo ad interpretazioni deresponsabilizzanti. Concludendo su questo punto, appare evidente che, per il legislatore comunitario, il consenso al trattamento dei dati personali si colora di tinte più intense e diventa il punto nevralgico della normativa privacy al quale gli operatori dovranno prestare particolare attenzione.

5.- Conclusioni

Semmai ce ne fosse stato bisogno ho tentato di dimostrare che la privacy non è un argomento su cui si possa improvvisare ma ancora una volta nel nostro paese le aziende e le pubbliche amministrazioni rincorrono con affanno una scadenza fissata con largo anticipo. L'entrata in vigore del Regolamento, *"un'esigenza temporale molto stringente, con una serie di passaggi non banali*

[19] Art. 4 punto 11 del Regolamento: Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile.
[20] Soffientini, Privacy cit., 202.
[21] Art. 83 comma 4 del Regolamento: Condizioni generali per infliggere sanzioni amministrative pecuniarie.

per la Pubblica Amministrazione e non solo"[22] impone una vera e propria riorganizzazione dei processi interni ma soprattutto secondo me la consapevolezza che il sistema privacy debba essere spalmato e sotteso a tutto il management pubblico o privato che sia. Anche la PA è obbligata a fare analisi dei rischi, valutazione di impatto, data breach e a nominare, un responsabile, il DPO che essendo una figura nuova è anche occasione professionale e di lavoro da non perdere. Interessante la spinta, che in Europa è già molto evidente, verso la terziarizzazione, l'esternalizzazione dei servizi informatici e del trattamento dei dati, le pubbliche amministrazioni possono scegliere se gestire i trattamenti in house o invece affidarli all'esterno, valutando quelle che sono le caratteristiche dei provider.

Abstract.- Nell'articolo una sintesi delle novità più importanti e interessanti, partendo dall'assunto che la proposta del GDPR propone un modello di organizzazione, gestione e controllo della privacy, e non più un mero adempimento statico e formalistico. Il regolamento conferma i quattro grandi principi di base che ispirano la disciplina della privacy nella sua totalità: principio di necessità, principio di proporzionalità, principio di finalità, principio di legittimità, insieme al Data Protection Impact Assessment (DPIA), un piano di valutazione di impatto sulla protezione dei dati personali, un'assoluta novità contenuta all'interno del regolamento. I nuovi adempimenti della normativa permettono un conseguenziale rafforzamento di due strumenti fondamentali per la tutela degli interessati, l'informativa ed il consenso. L'idea è quella di mostrare, in questo articolo, quanto la privacy non sia un argomento adatto ad essere trattato con approssimazione, e di quanto tutto il sistema privacy debba essere spalmato con consapevolezza a tutto il management pubblico o privato.

In the article a summary of the most important and interesting novelties, starting from the assumption that the proposal of GDPR proposes a model of organization, management and control of privacy, and no longer a mere static and formalistic fulfillment. The regulation confirms the big four basic principles which inspire the discipline of privacy in its entirety: necessity principle, the principle of proportionality, the principle of purpose, and the principle of legality, together with the Data Protection Impact Assessment (DPIA), a plan for the assessment of impact on the protection of personal data, an absolute novelty contained within the regulation. The new obligations of the regulations allow a consequential strengthening of two fundamental instruments for the protection of the persons concerned, information and consent. The idea of this article is to demonstrate that ones privacy is not a suitable subject to be treated with approximation, and how much the entire privacy system should be handled with awareness to all the management both public and private.

[22] Così il Presidente dell'Autorità Garante, Antonello Soro, http://www.agcm.it/.