http://www.altalex.com/documents/news/2018/05/21/data-protection-vademecum-last-minute-per-avvocati

GDPR, vademecum last minute per Avvocati

Primo consiglio: realizzate il registro dei trattamenti prima del 25 maggio

di Claudia Morelli e Maurizio Reale

Dopo fiumi di inchiostro, di post, di news e di schede esplicative, chiedo a voi Avvocati di fare mente locale sulla "vostra" Data protection ai tempi del Regolamento europeo.

Intendo per "vostra" sia la data protection che pensate di garantire nel vostro studio legale; sia la data protection come garanzia dei vostri clienti rispetto alla pubblica amministrazione (per esempio rispetto al potere giurisdizionale, alle procure, ai tribunali, alle autorità investigative); sia la data protection dei vostri clienti rispetto alle imprese con cui hanno a che fare e con riferimento ad eventuali data breach; sia la data protection di voi come privati cittadini.

Al di là degli adempimenti formali che vedremo più avanti nell'articolo, a ridosso del fatidico GDPR Day, il 25 maggio prossimo, ciò che tenteremo di fare in questo articolo- con l'ausilio tecnico di Maurizio Reale – è chiarire come voi potete contribuire a realizzare - in qualità ontologica di garanti e tutori dei diritti delle persone e dei cittadini - quel principio di accountability che informa tutte le norme precettive del regolamento europeo. Cioé il principio generale di responsabilizzazione e di consapevolezza sulla raccolta, trattamento e utilizzo dei dati personali ai tempi dei Big Data, Intelligenza artificiale, robotica, fake news, propaganda elettorale effettuata come qualsiasi campagna di web marketing.

Buona lettura!

Il 25 maggio è ormai prossimo e ancora tante sono le questioni aperte così come le domande che in eventi e convegni vengono poste da parte degli Avvocati.

In questo articolo cercheremo di dare qualche indicazione anche alla luce di quanto finora emerso a livello istituzionale (con le indicazioni del Garante italiano, i suggerimenti del Garante europeo, il Vademecum dell'Unione Triveneta degli Ordini forensi), in particolare sui temi Registro dei trattamenti, Misure di sicurezza, Informativa e Consenso, Data protection officer, Trattamento dati sensibili.

REGISTRO DEI TRATTAMENTI. Lo studio legale di piccole (e anche medie dimensioni) non ha l'obbligo generale di dotarsi del registro dei trattamenti. L'obbligo scatta a prescindere dal dato dimensionale quando i dati oggetto del trattamento possono rappresentare rischi per la libertà e i diritti dell'interessato o siano "sensibili" o giudiziari (condanne penali per esempio).

Obbligo o no, è doveroso segnalare quanto riferito dal Garante italiano, il quale ne auspica la predisposizione anche da parte dei soggetti non obbligati proprio in attuazione di quel principio di accountability generale.

Il registro aiuta a "mappare" le aree di rischio e dunque a rendere l'avvocato – in qualità del titolare del trattamento – consapevole della natura dei dati raccolti per l'esercizio dell'attività, la loro conservazione, le misure di sicurezza adottate.

La redazione e l'aggiornamento dello stesso non potrà prescindere dalla situazione reale, oggettiva ed effettiva in cui si opera; anche a tal proposito non dimentichiamo le parole del Garante Europeo a proposito di quanto detto per la predisposizione dell'informativa ed evitiamo quindi di fare semplici "copia e incolla" nella errata convinzione che l'importante sia comunque scrivere qualcosa posto che, non dimentichiamolo mai, ciò che scriviamo deve essere conforme alla realtà, obiettivo questo possibile da raggiungere solo se il titolare e del responsabile del trattamento, saranno veramente consapevoli dei contenuti.

Sarà sufficiente un foglio exel, predisposto ex ante (lo avete già predisposto?), in cui indicare le finalità del trattamento, ma anche informazioni quali le modalità di conservazione, le categorie dei dati personali conservati e degli interessati, gli eventuali trasferimenti verso paesi terzi, eventuali misure di sicurezza applicate, senza dimenticare che il registro deve essere messo a disposizione dell'autorità di controllo ove da questa richiesto.

TRATTAMENTO DATI SENSIBILI, GENETICI, BIOMETRICI, RELATIVI ALLA SALUTE. Il loro trattamento è generalmente vietato. Ma il GDPR esplicita una deroga qualora esso sia necessario per accertare, esercitare e difendere un diritto in sede giudiziaria e ogni qualvolta le autorità giurisdizionali esercitino la loro funzioni.

MISURE DI SICUREZZA. Uno dei quesiti che maggiormente ricorre tra i professionisti è se vi siano delle specifiche misure di sicurezza da porre in essere per proteggere i dati trattati nell'esercizio dell'attività professionali tali da consentire, una volta adottate, una assoluta tranquillità. Il riferimento e il pensiero va alle misure di sicurezza minime, così come elencate dal "Codice Privacy" 196/2003 in vigore fino al prossimo 24 maggio e alla possibilità o meno di continuare ad adottare quelle al fine di essere in regola anche con il regolamento 679/2016. Al quesito non è possibile dare una generale risposta in quanto è noto che l'articolo 32 del regolamento prevede che, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, il titolare del trattamento e il responsabile del trattamento devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Il titolare del trattamento e il responsabile del trattamento devono poi fare in modo che chiunque agisca sotto la loro autorità e abbia accesso a dati personali, non possa trattarli se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.
Le misure che il titolare e il responsabile del trattamento devono adottare devono quindi essere adeguate relativamente ad una serie di circostanze che non possono essere standardizzate o previste in assenza di specifica analisi della effettiva situazione nella quale si opera quali, ad esempio, il contesto in cui i dati vengono trattati, la tipologia dei dati oggetto di trattamento, le capacità e il grado di conoscenza di chi deve trattarli e le risorse economiche che possono essere utilizzate per attuare/migliorare il livello di sicurezza.
Proprio per il principio sopra esposto non può esistere un elenco predeterminato di misure di sicurezza ed anche quelle in vigore fino 24 maggio 2018, dettate dal Codice Privacy, così come specificato dal Garante italiano, se già poste in essere, dovranno essere valutate, caso per caso, al fine di verificare se possano considerarsi adeguate in relazione alla filosofia della normativa europea la quale richiede, come ribadito dal Garante europeo, un nuovo approccio da parte di coloro che i dati trattano "non essendo possibile risolvere i problemi del futuro con l'approccio del passato" dovendo quindi mettere in pratica ed applicare il principio di accountability attraverso il quale effettuare la valutazione dell'effettiva adeguatezza, ora come allora, delle misure adottate in passato e chiedersi quindi se siano ancora in grado di garantire una effettiva sicurezza o se invece non debbano ritenersi, nel presente, obsolete.

AVVOCATI E ADEMPIMENTI DATA PROTECTION EU general data protection regulation 2016/679 (GDPR)		
INFORMATIVA AL CLIENTE	- Chiara - Trasparente - Esplicita	Indica i riferimenti del titolare del trattamento, i diritti dell'interessato rispetto ai propri dati, le finalità del trattamento e le caratteristiche principali le principali misure di sicurezza. Deve essere firmata dal cliente.
CONSENSO	- Esplicito - Inequivocabile - Specifico	Non è necessario nel caso il trattamento dei dati avvenga per adempiere un obbligo di legge. Va richiesto in modo da essere provato
REGISTRO DEI TRATTAMENTI	**- Consigliata l'adozione anche nelle ipotesi non obbligatorie**	E' una mappa dei trattamenti, delle finalità, dei tipi di dati, del tempo di conservazione, dell'eventuale trasferimento all'estero
MISURE DI SICUREZZA	- Audit interna da fare	Il titolare del trattamento deve valutare il proprio livello di necessità in funzione della tipologia dei dati e del trattamento effettuato
DATA PROTECTION OFFICERS	- La sua nomina non è obbligatoria per studi legali piccoli e medi	Occorre comunque valutare sempre il tipo di dati e di trattamento realizzato
DATA BREACH	- Deve essere dichiarata	In caso di accesso abusivo e sottrazione di dati, l'avvocato deve comunicarlo al Garante e nei casi più gravi all'interessato

INFORMATIVA AL CLIENTE E CONSENSO. L'avvocato titolare dello studio deve verificare l'attualità delle informative sulla privacy già predisposte e del consenso già raccolto, alla luce dei nuovi requisiti previsti dal regolamento. In particolare è necessario verificare se è specificata la base legislativa del trattamento dei dati, il periodo di conservazione dei dati, e le informazioni utili riguardo ai diritti che spettano al soggetto interessato. Le info dovranno essere concise, semplici, chiare.
Va da sé che ai nuovi clienti, l'avvocato dovrà consegnare la informativa che dovrà essere firmata per presa visione. L'informativa deve essere chiara, trasparente, comprensibile e dare indicazioni concrete riguardo ai diritti che spettano all'interessato (revoca del consenso, accesso ai dati, rettifica, diritto all'oblio, portabilità) e alle modalità operative per il loro esercizio (i riferimenti di contatto dell'avvocato, per esempio). E' importante fare un audit sulle procedure necessarie per corrispondere efficacemente ad eventuali richieste che, ricordiamo, dovranno essere soddisfatte in 30

giorni. Inoltre, nel caso di rifiuto, occorre informare la persona interessata dei rimedi a suo vantaggio, come il ricorso al Garante o quello giudiziario.
Il consenso al trattamento dei dati non è previsto come base giuridica del trattamento, se quest'ultimo è effettuato per l'adempimento di un obbligo legale. Tuttavia è sempre bene raccoglierlo – ove non comprometta l'attività di assistenza/difesa, in maniera chiara ed inequivocabile.
NOMINA DEL DATA PROTECTION OFFICER. Se non vi è dubbio alcuno che gli Avvocati, solo in quanto esperti in maniera specifica della materia, possono essere nominati DPO presso strutture terze (anche per contratto), sembra ormai chiarito il criterio per stabilire se lo studio legale debba o meno nominare il proprio DPO. Anche qui vale la regola della situazione reale, oggettiva, concreta dello studio essendo fondamentale l'analisi dell'attività effettivamente svolta ponendola a confronto con l'articolo 37 del GDPR, che richiede la nomina del DPO ogni qualvolta: il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10. Sul punto si segnala che lo scorso 28 marzo il Garante ha pubblicato nuove FAQ sul Responsabile della Protezione dei Dati (RPD) in ambito privato che vanno ad aggiungersi a quelle adottate dal Gruppo Art. 29 in Allegato alle Linee guida sul RPD e, dalla risposta data alla FAQ numero 4 (chi sono i soggetti per i quali non è obbligatoria la designazione del responsabile della protezione dei dati personali?), si evince che "nei casi diversi da quelli previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679, la designazione del responsabile del trattamento non è obbligatoria (ad esempio, in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale; agenti, rappresentanti e mediatori operanti non su larga scala; imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti: v. anche considerando 97 del Regolamento, in relazione alla definizione di attività "accessoria").
Nel caso in cui non ricorrano tali condizioni, lo studio potrà comunque nominare un DPO su base volontaristica o magari incaricare il privacy officer che sovraintenda alla verifica costante delle procedure di studio, per suggerire le migliori pratiche di compliance data protection.
Qualsiasi sia la scelta, obbligata o volontaria, è buona pratica fare un report con le ragioni che hanno spinto ad adottare la soluzione prescelta. Ricordiamo che il DPO deve avere caratteristiche di competenza, indipendenza ed essere al riparo da eventuali conflitti di interessi.
Questo significa, per inciso, che lo studio legale può essere o esprimere tra i suoi avvocati un DPO a vantaggio di un proprio clienti facendo molta attenzione al profilo del conflitto di interesse.
IL DPO NON È RESPONSABILE. Occorre chiarire che, anche ove nominato, il DPO non assume su di sé le responsabilità che il regolamento assegna al titolare del trattamento, che sarà sempre chiamato a rispondere direttamente - se professionista - o nella persona del rappresentante legale del mancato adempimento agli obblighi di legge.
DATA BREACH. La sicurezza fisica del dato è un presupposto indispensabile perché la data protection possa realizzarsi. Per questo sarà indispensabile adottare tutte le buone pratiche di cybersecurity affinché i dati posseduti siano al riparo da data breach. Il poter dimostrare di aver adottato tutte le adeguate e proporzionate pratiche per assicurare il dato sarà indispensabile per escludere forme gravi di responsabilità. Tuttavia, se il data breach dovesse verificarsi, il regolamento chiede esplicitamente che se ne faccia denuncia al Garante e- nei casi più gravi- anche ai diretti interessati.
ATTIVITA' DIFENSIVA E AUTORIZZAZIONI GENERALI. Ricordiamo che attualmente valgono alcune Autorizzazioni del garante italiano per il trattamento dei dati sensibili da parte dei liberi professionisti (4/2016) e dei dati giudiziari (7/2016) che dovrebbero essere riconfermate.
L'AUSILIO DI INTERPRETAZIONE AUTENTICA DEL GARANTE EUROPEO. Venerdì 11 maggio scorso nella sede del Tribunale di Napoli, per iniziativa di IUSLAWEBRADIO, si è svolto il convegno dal titolo "Il regolamento generale sulla protezione dei dati. Aspetti principali e nuove opportunità per gli avvocati". Ospite d'eccezione è stato Giovanni Buttarelli, Garante Europeo Privacy il quale, nel corso del suo intervento ha da una parte voluto tranquillizzare gli avvocati presenti affermando che "… alle 9 del 25 maggio non avrete la guardia di finanza o i carabinieri a ispezionare i vostri studi legali…"; dall'altra, con toni altamente critici, ha aggiunto che "molto probabilmente, in quella data, in ragione di un ritardo italiano non giustificato, non avremo il decreto legislativo di "accompagnamento" … perché la delega è partita in ritardo, la commissione è stata costituita in ritardo e il lavoro non è stato all'altezza delle aspettative e questo ha comportato, da parte del Consiglio dei Ministri (riunitosi) il 22 marzo, l'approvazione del testo con la formula "salvo intese" … sono passati quarantanove giorni ed ancora non sappiamo quale testo verrà inviato alle camere… rimarranno le sanzioni penali (oggi previste dall'art. 167 del D.lgs. 196/2003) o no? Chi avrà udienza penale per questo reato il 26 maggio, cosa dovrà fare?".
Sarà quindi necessaria qualche settimana in più, ma ciò non pregiudicherà la piena applicazione del regolamento 679/2016 che, in quanto tale, non ha bisogno di norme attuative; a Bruxelles il 25 maggio verrà presentato il nuovo organismo che sostituirà il gruppo articolo 29 e che avrà quale principale fine quello di indirizzare i titolari del trattamento ad applicare meglio il regolamento.
Non ci saranno, avverte il Garante Europeo, altre linee guida e ciò perché uno dei principi cardine del regolamento 679/2016 è quello della "accountability" che permetterà ai destinatari delle norme di avere un margine di manovra in

più per renderne graduale l'applicazione posto che ci saranno meno prescrizioni dettagliate delle autorità ma, in cambio di tale flessibilità, al titolare del trattamento viene richiesto di andare oltre alla mera applicazione della legge e quindi, ad esempio, di adottare una policy al proprio interno al fine di rendere concreta ed effettiva la serie di salvaguardie che in parte vengono conservate e che in parte sono oggetto di innovazione, non essendo possibile risolvere i problemi del futuro con l'approccio del passato.
Chi ha un sistema informativo, afferma il Dott. Buttarelli, ha l'obbligo di strutturarlo in modo tale da renderlo "privacy-friendly", soprattutto quando è necessario aggiornarlo e se possono essere adottate diverse soluzioni, la scelta deve ricadere su quelle più favorevoli alla privacy del cliente.
"Se mi capitasse, in sede civile, di valutare la responsabilità simile al 2050 c.c., la prima cosa che chiederei sarebbe: CHE COSA HAI FATTO SUL PIANO DELL'ACCOUNTABILITY? CHE COSA HAI FATTO SUL PIANO DELL'EFFETTIVA VALUTAZIONE DEI RISCHI? Ciò perché il documento programmatico sulla sicurezza viene sostituito dalla valutazione d'impatto sui rischi dalla quale deve emergere che hai pensato veramente a quello che hai scritto non essendo quindi più possibile pensare di delegare gli adempimenti e gli obblighi esclusivamente ad un data protection officer di cui abbiamo sicuramente bisogno e che dovranno svolgere in maniera indipendente quel tipo di lavoro ma è necessario nel contempo che i diretti interessati siano maggiormente a conoscenza dell'organizzazione perchè saranno sicuramente responsabili anche delle scelte che faranno o non faranno o dei costi che decideranno di non sostenere".
Quanto all'attività dell'avvocato, ha richiamato l'attenzione dei presenti anche e soprattutto:
1) ai rapporti con i corrispondenti / domiciliatari, in quanto proprio in tali situazioni bisognerà rilevare e comprendere "chi fa cosa ed è responsabile di che;
2) alla verifica dell'esistenza o meno della condivisione di dati in studio, soprattutto in quelli dove non vi è formalmente uno studio associato vero e proprio ma vi sono più avvocati che, ad esempio, per abbattere i costi dividono i locali, situazione questa dalla quale potrebbe poi, molto probabilmente, prendere vita un fenomeno di sostituzioni ecc.;
3) alla raccomandazione di costruire e mantenere i rapporti con i clienti all'insegna della chiarezza e della sincerità;
4) ai piccoli studi legali ha suggerito di predisporre una PRIVACY POLICY dello studio, la quale potrebbe addirittura essere alternativa alla valutazione o al registro; una semplice Policy alla quale dovrà attenersi il titolare e chi collabora con lui;
5) quanto all'informativa, attenzione a ciò che si sottoscrive senza essere veramente consapevoli del significato; tutto ciò che scriviamo, infatti, ove non risultasse conforme alla realtà, potrebbe dar seguito all'effetto boomerang per cui, in tale ipotesi, meglio non scrivere nulla e rilasciare oralmente l'informativa mentre, se sono consapevole e soprattutto ho svolto un lavoro di adeguamento, allora benissimo al rilascio di informativa scritta.
TRIBUNALI, PROCURE E AUTORITÀ INVESTIGATIVE. Al riguardo ricordiamo che le Pubbliche amministrazioni hanno l'obbligo di nominare il DPO e di adeguarsi alle altre prescrizioni di regolamento. Gli avvocati in quanto difensori potranno esercitare anche una "vigilanza" sul rispetto delle garanzie e tutele. Inoltre ricordiamo che, nonostante il GDPR abbia assorbito tutte le attenzioni di "esperti", vi è un altro provvedimento importante e corredato al GDPR: la direttiva 680/2016, di cui Avvocatoquattropuntozero ha già parlato nell'articolo Giustizia predittiva: niente profilazione per assumere provvedimenti penali.
La direttiva "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" riguarda la protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento di reati ed esecuzione di sanzioni penali nonché di circolazione di tali dati. E avrebbe dovuto essere attuata entro il 6 maggio.
Lo scheda di decreto delegato di attuazione è stato approvato il 16 maggio scorso dal governo Gentiloni in via definitiva.
Il decreto regolamenta il trattamento dei dati personali per finalità di prevenzione e repressione di reati, esecuzione di sanzioni penali, salvaguardia contro le minacce alla sicurezza pubblica e prevenzione delle stesse, da parte sia dell'autorità giudiziaria, sia delle forze di polizia.
Si tratta di un testo unitario, dedicato alla complessiva disciplina del trattamento di dati personali in ambito penale, con l'obiettivo di creare un vero e proprio statuto, contenente principi generali di regolamentazione della materia e disposizioni di dettaglio nei vari settori in cui si può articolare il trattamento dei dati personali. La nuova normativa supera e sostituisce in gran parte quella attualmente contemplata nei titoli primo e secondo della parte seconda del Codice sul trattamento dei dati personali di cui al Decreto legislativo 30 giugno 2003, n. 196, dedicate a specifici settori, in particolare quello giudiziario e quello dei trattamenti da parte delle forze di polizia.
In particolare, il testo prescrive che i dati siano conservati per il tempo necessario al conseguimento delle finalità per le quali sono trattati, sottoposti a esame periodico per verificarne la persistente necessità di conservazione e cancellati o anonimizzati una volta decorso tale termine e introduce una nuova disciplina riguardo alla differenziazione tra categorie di dati (fondati su fatti ovvero su valutazioni) e di interessati, in ragione della loro specifica posizione processuale.
Inoltre, riguardo ai diritti dell'interessato (ricezione di informazioni, accesso, rettifica, cancellazione, limitazione del trattamento), il testo prevede che rispetto ai dati personali contenuti in una decisione giudiziaria, in atti o documenti oggetto di trattamento nel corso di accertamenti o indagini, nel casellario giudiziale o in un fascicolo oggetto di trattamento nel corso di un procedimento penale o in fase di esecuzione penale, l'esercizio di tali diritti è regolato dalle

disposizioni normative che disciplinano tali atti e procedimenti. In ambito giudiziario, la tutela degli interessati è quindi assicurata, per le parti, dalle garanzie che riconoscono i diritti di difesa all'interno del procedimento penale, anche con riguardo ai dati personali necessariamente oggetto di trattamento, assicurando quindi la possibilità di limitare l'esercizio dei diritti dell'interessato, conformemente alle esigenze di prevenzione, di indagine e processuali. Per garantire i diritti in ambito giudiziario anche con riferimento ai terzi, si è previsto uno speciale procedimento attraverso il quale qualsiasi interessato, durante il procedimento penale o dopo la sua definizione, può chiedere la rettifica, la cancellazione o la limitazione dei dati personali che lo riguardano.

In materia di sicurezza del trattamento, si prevede come obbligatoria anche per l'autorità giudiziaria la nomina del responsabile della protezione dati, in ragione dell'ausilio che tale figura può fornire nella gestione di trattamenti complessi e spesso inerenti dati sensibili, quali appunto quelli svolti in sede giurisdizionale. Per quanto riguarda i trasferimenti di dati personali verso Paesi terzi o organizzazioni internazionali, si stabilisce che esso sia consentito solo nei confronti delle autorità competenti e per le finalità di pubblica sicurezza oggetto della direttiva e in presenza di specifiche condizioni, tra cui l'adozione, da parte della Commissione dell'Unione europea, di una decisione di adeguatezza o, in mancanza, vi siano garanzie adeguate.

Il decreto individua nel Garante nazionale l'autorità deputata a vigilare sul rispetto delle norme attuative della direttiva in funzione della tutela dei diritti e delle libertà fondamentali delle persone fisiche, coinvolte dalle attività di trattamento di dati personali, escludendo il potere di controllo del Garante in ordine al trattamento svolto dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali, comprese quelle del pubblico ministero. Infine, per quanto riguarda la violazione delle nuove norme, il testo prevede sanzioni amministrative (che nei casi più gravi possono estendersi da 50.000 a 150.000 euro) per le violazioni inerenti alle modalità del trattamento e introduce sanzioni penali per il trattamento operato con finalità illegittime.

(Altalex, 21 maggio 2018. Articolo di Claudia Morelli e Maurizio Reale)