Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

Sanzioni penali nel decreto Gdpr, i problemi interpretativi e applicativi

LINK: https://www.agendadigitale.eu/sicurezza/privacy/sanzioni-penali-nel-decreto-gdpr-i-problemi-interpretativi-e-applicativi/

Sanzioni penali nel decreto Gdpr, i problemi interpretativi e applicativi Home Sicurezza digitale Privacy Condividi questo articolo La scelta dell'Italia di optare per l'applicabilità delle sanzioni penali in materia di protezione dei dati personali, sancita dal D.lgs. 101/18, non risolve i dubbi interpretativi che la giurisprudenza precedente al GDPR aveva già evidenziato. Ecco le criticità interpretative e applicative 2 ore fa Giuseppe Vaciago Partner R&P Legal e fondatore di Tech&Law Center Con l'entrata in vigore del D.lgs. 101/18, l'Italia, dopo ampio e sofferto dibattito, ha optato per l'applicabilità delle sanzioni penali in materia di protezione dei dati personali modificando le fattispecie esistenti e aggiungendone delle nuove. La scelta, in controtendenza rispetto ad altri Stati Membri, non risolve i dubbi interpretativi che la giurisprudenza precedente al GDPR aveva già evidenziato e, anche se è ancora presto per dare giudizi definitivi, la lettura del combinato disposto del comma 2 della nuova formulazione dell'art. 167 che richiama le ipotesi previste degli artt. 2-sexies, septies, octies e quinquiesdecies, fa comprendere il livello di complessità che l'operatore del diritto, sia esso avvocato o magistrato, dovrà affrontare quando si troverà a interpretare o a applicare tale norma. Indice degli argomenti Il convitato di pietra in tema di misure minime di sicurezza Tutela del corpo fisico e del "corpo digitale" Prevenire gli incidenti informatici Il convitato di pietra in tema di misure minime di sicurezza Proprio per questa ragione, penso sia opportuno procedere per gradi. Prima di entrare nel merito dell'analisi delle singole fattispecie penali per le quali si rimanda a questa ottima sintesi e alla tabella in calce all'articolo relativa alle modifiche intervenute per gli artt. 167 e 168, mi sembra interessante evidenziare che il capo II del nuovo Codice della Privacy in tema di illeciti penali annoveri come 'convitato di pietra' l'art. 169 in tema di misure minime di sicurezza. L'abrogazione di questo articolo era scontata nel momento stesso in cui, grazie al noto principio dell'accountability, si è deciso di demandare al titolare del trattamento, tenuto conto dello 'stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche', la valutazione delle 'misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio'. Come è stato già osservato, l'articolazione dell'art. 32 del GDPR contrasta con il principio di tassatività del diritto penale, in quanto non indica con un sufficiente livello di dettaglio quali misure debbano essere adottate al fine di evitare di incorrere in una sanzione penale. Se è indubbio che questa osservazione non è superabile, rimane da chiedersi se abbia senso sanzionare penalmente l'invio di comunicazioni indesiderate (art. 130 D.lgs. 101/18) effettuate con finalità di profitto e conseguente 'nocumento' dell'interessato e, invece, sanzionare solo amministrativamente un titolare del trattamento del dato che permetta che i dati di centinaia di migliaia di interessati siano diffusi

Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

in Rete a causa di una precaria o, talvolta, inesistente policy in tema di sicurezza informatica. Tutela del corpo fisico e del "corpo digitale" Questa riflessione mi porta ad un parallelismo che spero faccia comprendere la logica che sottende al mio ragionamento: partendo dal presupposto che il GDPR introduce il concetto che il nostro 'corpo digitale' debba ricevere la medesima tutela del nostro corpo fisico, vedo una profonda disparità di trattamento nell'attenzione che il nostro Legislatore ha speso nel 2008 rivedendo la normativa per la sicurezza e salute sul luogo del lavoro con il D.lgs. 81/08, rispetto a quella offerta al tema della sicurezza informatica con il D.lgs. 101/18. La chiave di volta della normativa del 2008 è stata l'estensione della responsabilità penale dell'Ente ai sensi del D.lgs. 231/01 per le fattispecie di omicidio colposo (art 589 c.p.) e di lesioni personali colpose gravi o gravissime (art. 590 c.p.) entrambi commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro. La ratio della norma era semplice ed efficace: ove il datore di lavoro decida di risparmiare sulle misure di sicurezza idonee a proteggere il lavoratore, l'ente ne deve rispondere penalmente attraverso le severe sanzioni previste dal D.lgs. 231/01 che possono comportare anche l'applicazione delle misure interdittive, che, in pratica, consiste nella temporanea chiusura dello stabilimento produttivo dove si è verificato l'incidente. L'introduzione di questa normativa ha comportato i seguenti risultati: nel 2007 le denunce di infortunio sul luogo di lavoro in Italia sono passate da 913.000 a 469.008 nel 2018. Una diminuzione di quasi la metà. Sono fortemente convinto che una delle principali ragioni per le quali sia stato possibile ottenere questo risultato risieda nella severità della normativa realizzata nel 2008. Prevenire gli incidenti informatici Il nostro Paese non è endemicamente in grado di prevenire ipotesi patologiche ed è forse per questo che ha sviluppato una straordinaria forza di reazione una volta che il danno si è verificato. Tuttavia, quando si ragiona in ambito di sicurezza informatica, la programmazione e la prevenzione sono elementi fondamentali per evitare che un incidente informatico assuma proporzioni ragguardevoli per vastità e capacità di contenimento. Tuttavia, per un piano di sicurezza informatica adeguato, servono investimenti e, sotto questo profilo, l'attuale formulazione dell'art. 32 del GDPR lascia troppo spazio all'interpretazione che molto spesso confondiamo con improvvisazione, arte nella quale noi italiani abbiamo indubbiamente doti eccelse. Il ruolo del Legislatore, pertanto, avrebbe potuto essere più severo garantendo da un lato i principi dell'art. 32 del GDPR e dall'altro il rispetto tassativo di quelle misure minime previste dal disciplinare tecnico presente nell'allegato B del previgente codice della privacy oramai lettera morta dopo l'applicazione del D.lgs. 101/18. Sarò certamente criticato perché mi si dirà che l'art. 32 del GDPR consente una visione della sicurezza informatica più ampia e più duttile e sicuramente più adatta alla rapidità dell'evoluzione tecnologica, ma rileggendo quelle 'sante' regolette previste dal disciplinare tecnico mi viene da pensare che se tutte le realtà imprenditoriali italiane le adottassero, avremmo una diminuzione drastica degli incidenti informatici e dei conseguenti data breach. Da ultimo, una considerazione sul presunto problema del ne bis idem in forza del quale non si può essere giudicati due volte per lo stesso fatto. Ci si è posti l'interrogativo, infatti, se sia legittimo o meno che possa essere avviato un procedimento penale sugli stessi fatti oggetto di una sanzione amministrativa comminata dal Garante privacy. Concordo con chi ritiene che questo sia un falso problema e che la violazione dell'art. 4 Prot. 7 della Convenzione Europea dei Diritto dell'Uomo sancita nel famoso caso Grande Stevens non sia utilizzabile nel contesto del D.lgs. 101/18. Tuttavia, è facile prevedere nei prossimi mesi un annoso dibattito sul tema con particolare riferimento al comma 6 dell'art. 167 in cui viene statuito che 'quando per lo stesso fatto è stata applicata la

Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa e stata riscossa, la pena e diminuita'. Questo dibattito toglierà ulteriore enfasi al tema della sicurezza informatica che invece ritengo centrale per garantire il pieno rispetto dell'attuale normativa in materia di protezione dei dati personali. Del resto, così era successo nel 2013, quando con il Decreto legge 93/2013 si era paventata l'ipotesi di estendere la responsabilità penale degli enti alle fattispecie penali dell'allora Codice della Privacy. Anche in tal caso, tuttavia, fu subito chiaro che l'art. 169 essendo una contravvenzione non sarebbe rientrata in tale decreto che, per di più, non divenne mai legge. keyboard_arrow_right keyboard_arrow_left Versione D.lgs. 196/03 Versione post D.lgs. 101/18 Art. 167 (Trattamento illecito di dati) 1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi. Art. 167 (Trattamento illecito di dati) 1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi. 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per se' o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni. 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-quinquiesdecies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni. 3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato. keyboard_arrow_right keyboard_arrow_left Art. 168 (Falsità nelle dichiarazioni e notificazioni al Garante) 1. Chiunque, nella notificazione di cui all'articolo 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, + punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni. Art. 168 (Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante) 1. Salvo che il fatto costituisca più grave reato, chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito con la reclusione da sei mesi a tre anni. 2. Fuori dei casi di cui al comma 1, è punito con la reclusione sino a un anno chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti. @RIPRODUZIONE RISERVATA