CJN

# Diritto Penale Contemporaneo

## RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL

A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

*Nuove frontiere tecnologiche e sistema penale. Sicurezza informatica, strumenti di repressione e tecniche di prevenzione*

IX Corso di formazione interdottorale di Diritto e Procedura penale 'Giuliano Vassalli' per dottorandi e dottori di ricerca

(AIDP Gruppo Italiano, Siracusa International Institute for Criminal Justice and Human Rights – Siracusa, 29 novembre - 1° dicembre 2018)

ISSN 2240-7618

2/2019

Editore Associazione "Progetto giustizia penale", via Altaguardia 1, Milano - c.f. 97792250157
ANNO 2019 - CODICE ISSN 2240-7618 - Registrazione presso il Tribunale di Milano, al n. 554 del 18 novembre 2011.
Impaginazione a cura di Chiara Pavesi

**Diritto penale contemporaneo – Rivista trimestrale** è un periodico on line ad accesso libero e non ha fine di profitto. Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione. La rivista, registrata presso il Tribunale di Milano, al n. 554 del 18 novembre 2011, è edita attualmente dall'associazione "Progetto giustizia penale", con sede a Milano, ed è pubblicata con la collaborazione scientifica e il supporto dell'Università Commerciale Luigi Bocconi di Milano, dell'Università degli Studi di Milano, dell'Università di Roma Tre, dell'Università LUISS Guido Carli, dell'Universitat de Barcelona e dell'Università Diego Portales di Santiago del Cile.

La rivista pubblica contributi inediti relativi a temi di interesse per le scienze penalistiche a livello internazionale, in lingua italiana, spagnolo, inglese, francese, tedesca e portoghese. Ogni contributo è corredato da un breve abstract in italiano, spagnolo e inglese.

La rivista è classificata dall'ANVUR come rivista scientifica per l'area 12 (scienze giuridiche), di classe A per i settori scientifici G1 (diritto penale) e G2 (diritto processuale penale). È indicizzata in DoGI e DOAJ.



La rivista può essere citata in forma abbreviata con l'acronimo: *DPC-RT*, corredato dall'indicazione dell'anno di edizione e del fascicolo.

La rivista fa proprio il Code of Conduct and Best Practice Guidelines for Journal Editors elaborato dal COPE (Committee on Publication Ethics).

La rivista si conforma alle norme del Regolamento UE 2016/679 in materia di tutela dei dati personali e di uso dei cookies (clicca qui per dettagli).

Ogni contributo proposto per la pubblicazione è preliminarmente esaminato dalla direzione, che verifica l'attinenza con i temi trattati dalla rivista e il rispetto dei requisiti minimi della pubblicazione.

In caso di esito positivo di questa prima valutazione, la direzione invia il contributo in forma anonima a due revisori, individuati secondo criteri di rotazione tra i membri dell'Editorial Advisory Board in relazione alla rispettiva competenza per materia e alle conoscenze linguistiche. I revisori ricevono una scheda di valutazione, da consegnare compilata alla direzione entro il termine da essa indicato. Nel caso di tardiva o mancata consegna della scheda, la direzione si riserva la facoltà di scegliere un nuovo revisore.

La direzione comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se entrambe le valutazioni sono positive, il contributo è pubblicato. Se una o entrambe le valutazioni raccomandano modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se uno o entrambi i revisori esprimono parere negativo alla pubblicazione.

La direzione si riserva la facoltà di pubblicare, in casi eccezionali, contributi non previamente sottoposti alla procedura di peer review. Di ciò è data notizia nella prima pagina del contributo, con indicazione delle ragioni relative.

Se desideri proporre una pubblicazione alla nostra rivista, invia una mail a editor.criminaljusticenetwork@gmail.com. I contributi che saranno ritenuti dalla direzione di potenziale interesse per la rivista saranno sottoposti alla procedura di peer review sopra descritta. I contributi proposti alla rivista per la pubblicazione dovranno rispettare i criteri redazionali scaricabili qui.

**Diritto penale contemporaneo – Rivista trimestrale** es una publicación periódica *on line*, de libre acceso y sin ánimo de lucro. Todas las colaboraciones de carácter organizativo y editorial se realizan gratuitamente y no se imponen a los autores costes de maquetación y publicación.
La Revista, registrada en el Tribunal de Milan, en el n. 554 del 18 de noviembre de 2011, se edita actualmente por la asociación "Progetto giustizia penale", con sede en Milán, y se publica con la colaboración científica y el soporte de la *Università Commerciale Luigi Bocconi* di Milano, la *Università degli Studi di Milano,* la *Università di Roma Tre*, la *Università LUISS Guido Carli*, la *Universitat de Barcelona* y la *Universidad Diego Portales de Santiago de Chile.*
La Revista publica contribuciones inéditas, sobre temas de interés para la ciencia penal a nivel internacional, escritas en lengua italiana, española, inglesa, francesa, alemana o portuguesa. Todas las contribuciones van acompañadas de un breve abstract en italiano, español e inglés.
El lector puede leer, compartir, reproducir, distribuir, imprimir, comunicar a terceros, exponer en público, buscar y señalar mediante enlaces de hipervínculo todos los trabajos publicados en "Diritto penale contemporaneo – Rivista trimestrale", con cualquier medio y formato, para cualquier fin lícito y no comercial, dentro de los límites que permite la licencia *Creative Commons - Attribuzione - Non commerciale 3.0 Italia* (CC BY-NC 3.0 IT) y, en particular, debiendo mantenerse la indicación de la fuente, el logo, el formato gráfico original, así como el autor de la contribución.
La Revista se puede citar de forma abreviada cn el acrónimo *DPC-RT*, indicando el año de edición y el fascículo.
La Revista asume el Code of Conduct and Best Practice Guidelines for Journal Editors elaborado por el COPE (*Comitte on Publication Ethics*).
La Revista cumple lo dispuesto en el Reglamento UE 2016/679 en materia de protección de datos personales (clica aquí para los detalles sobre protectión de la privacy y uso de cookies).
Todas las contribuciones cuya publicación se propone serán examinadas previamente por la Dirección, que verificará la correspondencia con los temas tratados en la Revista y el respeto de los requisitos mínimos para su publicación.
En el caso de que se supere con éxito aquella primera valoración, la Dirección enviará la contribución de forma anónima a dos evaluadores, escogidos entre los miembros del *Editorial Advisory Board*, siguiendo criterios de rotación, de competencia por razón de la materia y atendiendo también al idioma del texto. Los evaluadores recibirán un formulario, que deberán devolver a la Dirección en el plazo indicado. En el caso de que la devolución del formulario se retrasara o no llegara a producirse, la Dirección se reserva la facultad de escoger un nuevo evaluador.
La Dirección comunicará el resultado de la evaluación al autor, garantizando el anonimato de los evaluadores. Si ambas evaluaciones son positivas, la contribución se publicará. Si alguna de las evaluaciones recomienda modificaciones, la contribución se publicará después de que su autor la haya revisado sobre la base de los comentarios recibidos y de que la Dirección haya verificado que tales comentarios han sido atendidos. La contribución no se publicará cuando uno o ambos evaluadores se pronuncien negativamente sobre su publicación.
La Dirección se reserva la facultad de publicar, en casos excepcionales, contribuciones que no hayan sido previamente sometidas a *peer review*. Se informará de ello en la primera página de la contribución, indicando las razones.

Si deseas proponer una publicación en nuestra revista, envía un mail a la dirección editor.criminaljusticenetwork@gmail.com. Las contribuciones que la Dirección considere de potencial interés para la Revista se someterán al proceso de *peer review* descrito arriba. Las contribuciones que se propongan a la Revista para su publicación deberán respetar los criterios de redacción (se pueden descargar aquí).

**Diritto penale contemporaneo – Rivista trimestrale** is an on-line, open-access, non-profit legal journal. All of the organisational and publishing partnerships are provided free of charge with no author processing fees. The journal, registered with the Court of Milan (n° 554 - 18/11/2011), is currently produced by the association "Progetto giustizia penale", based in Milan and is published with the support of Bocconi University of Milan, the University of Milan, Roma Tre University, the University LUISS Guido Carli, the University of Barcelona and Diego Portales University of Santiago, Chile.

The journal welcomes unpublished papers on topics of interest to the international community of criminal scholars and practitioners in the following languages; Italian, Spanish, English, French, German and Portuguese. Each paper is accompanied by a short abstract in Italian, Spanish and English.



For citation purposes the journal's abbreviated reference format may be used: *DPC-RT,* indicating year of publication and issue.

The journal strictly adheres to the Code of Conduct and Best Practice Guidelines for Journal Editors drawn up by COPE (Committee on Publication Ethics).

The journal complies with the General Data Protection Regulation (EU) 2016/679 (GDPR) (click here for details on protection of privacy and use of cookies).

All articles submitted for publication are first assessed by the Editorial Board to verify pertinence to topics addressed by the journal and to ensure that the publication's minimum standards and format requirements are met.

Should the paper in question be deemed suitable, the Editorial Board, maintaining the anonymity of the author, will send the submission to two reviewers selected in rotation from the Editorial Advisory Board, based on their areas of expertise and linguistic competence. The reviewers are provided with a feedback form to compile and submit back to the editorial board within an established timeframe. If the timeline is not heeded to or if no feedback is submitted, the editorial board reserves the right to choose a new reviewer.

The Editorial Board, whilst guaranteeing the anonymity of the reviewers, will inform the author of the decision on publication. If both evaluations are positive, the paper is published. If one or both of the evaluations recommends changes the paper will be published subsequent to revision by the author based on the comments received and verification by the editorial board. The paper will not be published should one or both of the reviewers provide negative feedback.

In exceptional cases the Editorial Board reserves the right to publish papers that have not undergone the peer review process. This will be noted on the first page of the paper and an explanation provided.

If you wish to submit a paper to our publication please email us at editor.criminaljusticenetwork@gmail.com. All papers considered of interest by the editorial board will be subject to peer review process detailed above. All papers submitted for publication must abide by the editorial guidelines (download here).

# Contents

# Contents

*Financial cybercrime*

Cibercrimen financiero

Financial Cybercrime

# Contents

La tutela penale della privacy nel cyberspazio

*La tutela penal de la privacidad en el ciberespacio*

*Criminal Law and the Protection of Privacy in Cyberspace*

# Contents

# Contents

# Contents

# La tutela penale della privacy nel cyberspazio

*La tutela penal de la privacidad en el ciberespacio*

*Criminal Law and the Protection of Privacy in Cyberspace*

# *Corporate liability e compliance* in the *cyber privacy crime*: il nuovo "modello organizzativo *privacy*"

## *Responsabilidad corporativa y compliance en el delito de privacidad cibernética:El nuevo "modelo organizativo de privacidad"*

## *Corporate Liability and Compliance in the Cyber Privacy Crime: the New "Privacy Organizational Model"*

Valentina Aragona
*Dottoranda di ricerca presso l'Università Luiss Guido Carli di Roma*
*valentina.aragona@luiss.it*

Riciclaggio | Lavado de activos | Money Laundering

**Abstracts**

L'esigenza di garantire un'adeguata protezione dai rischi in materia di trattamento illecito dei dati personali provenienti dallo spazio virtuale ha messo in luce lo stretto legame esistente tra *cybercrime* e *privacy* e ha condotto il legislatore europeo a valorizzare il momento della prevenzione, incentivando l'adozione di efficaci misure di protezione dei dati personali nelle reti e nei sistemi informatici. Il GDPR adotta un nuovo approccio basato sul rischio, ponendo in evidenza come il trattamento illecito dei dati personali non sia frutto della condotta del singolo, ma derivi da una precisa politica di impresa. Ciò induce a interrogarsi circa la possibilità di costruzione e adozione di un modello organizzativo integrato, che garantisca un coordinamento tra la disciplina di cui al D.Lgs. n. 231/2001 e la normativa in materia di *privacy*[*].

La exigencia de garantizar una adecuada protección de los riesgos en material de tratamiento ilícito de los datos personales provenientes del espacio virtual ha puesto en evidencia la estrecha relación entre cibercrimen y privacidad, provocando que el legislador europeo haya comenzado a preocuparse de la prevención de tales conductas, incentivándola adopción de medidas de protección eficaces de los datos personales en la red y en los sistemas informáticos. El GDPR adopta un nuevo enfoque basado en el riesgo, destacando cómo el tratamiento ilícito de datos personales no es fruto de la conducta del individuo, sino que deriva de una precisa política de empresa. Ello lleva a interrogarse acerca de la posibilidad de construir y adoptar un modelo de organización integrado, que garantice una coordinación entre la regulación del Decreto Legislativo n. 231/2001 y la normativa en materia de privacidad.

The need to ensure adequate protection against the risks of unlawful data processing from virtual space has highlighted the close link between cybercrime and privacy, inducing the European legislator to promote prevention, by encouraging the adoption of effective means to protect personal data in networks and computer systems. The GDPR adopts a new risk-based approach, highlighting how the unlawful data processing is not the result of the conduct of the individual, but derives from a precise business policy. This leads to question the possibility of constructing and adopting an integrated organizational model that guarantees coordination between the provisions of Legislative Decree no. 231/2001 and the legislation on privacy.

[*] Si ringraziano i Prof.ri Antonino Gullo e Roberto Flor per i preziosi suggerimenti e gli Avv.ti Marco Ferrante e Maria Valeria Feraco, esperti in materia di *privacy*, per gli innovativi spunti di riflessione forniti.

**Sommario**



# 1. "La *privacy* nel mondo di *internet*: una nuova sfida".

«*Internet, il più grande spazio pubblico che l'umanità abbia conosciuto, la rete che avvolge l'intero pianeta*»[1].

In questo grande spazio pubblico, potenzialmente incontrollato, i giuristi si trovano continuamente di fronte a nuove sfide, alla necessità di un continuo adeguamento e ripensamento dei paradigmi e delle categorie tradizionali del diritto e all'esigenza, sempre più pressante, di garantire la tutela dei diritti fondamentali della persona, anche nel mutato contesto tecnologico.

Difatti, l'irrompere della tecnologia informatica ha messo in evidenza, da un lato, la potenzialità di tale fenomeno, e dall'altro lato, la vulnerabilità dei fruitori dello stesso, completamente esposti in rete[2].

Il processo di trasformazione digitale ha, infatti, investito la maggior parte delle relazioni tra persone, imprese e pubbliche amministrazioni[3]. La rete è ormai divenuta la nuova dimensione in cui si svolge e si esprime la personalità umana.

Con specifico riferimento alla *privacy,* la rete rappresenta per molti versi uno strumento di libertà, ma spesso determina anche un'invasione nelle sfere più intime dell'individuo. Oggi non vi è attività pubblica o privata che, essendo fondata su tecnologie, non sia anche alimentata da dati personali.

Il passaggio all'*Internet of things*, che rende oggetti comuni strumenti di connessione interattiva, ha digitalizzato ogni aspetto della vita quotidiana, moltiplicando esponenzialmente il volume dei dati personali trattati[4].

Si può osservare come i dati personali circolino in rete senza alcun filtro: basti pensare che il funzionamento e la crescita del *web* e dei *social network* si fondi soprattutto sulla registrazione, attraverso gli stessi, di una grande quantità di informazioni personali e non, acquisite anche dagli altri utenti, i quali, proprio grazie a queste tecnologie, gestiscono una vera e propria rete di contatti, che consente loro di acquisire, registrare e diffondere informazioni di varia natura, anche riferite a terzi.

Nella maggioranza dei casi tali dati sono forniti volontariamente dal titolare, ma, molto spesso, vengono fagocitati dalla rete e rimangono nella stessa, che li diffonde anche laddove il titolare non abbia prestato il consenso o non ne sia neppure a conoscenza[5].

Ne deriva l'esigenza pressante di tutelare i dati personali in rete, tentando di garantire il rispetto della dignità, dell'identità e della riservatezza della persona[6]. In questo contesto garantire la tutela dei dati personali significa «*coniugare tecnologia e umanità, libertà e sicurezza, trasparenza del pubblico e riservatezza del privato, informazione e dignità, iniziativa economica e autonomia individuale, scienza e libertà dal determinismo*»[7].

Punto di riferimento in tal senso è l'art. 8 della Carta dei diritti fondamentali dell'Unione Europea, a mente del quale il trattamento dei dati deve avvenire secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. La norma in esame individua il diritto alla protezione dei dati

[1] Rodotà, (2010), p. 338
[2] Può evidenziarsi, peraltro, come l'evolversi dell'*Information tecnology* abbia creato anche ulteriori diritti da protegge quali il diritto all'oblio o la "riservatezza informatica", quale autonomo bene giuridico ed, anzi, diritto fondamentale della persona, da intendere come diritto ad uno spazio informatico esclusivo, che a prescindere dai contenuti che vi siano presenti, trattati o comunicati, deve essere lasciato libero da intrusioni manomissioni di terzi, in quanto strumento essenziale per la piena realizzazione della persona nell'odierna vita individuale e sociale.
[3] Soro, (2018), p. 11
[4] Soro, (2018), p. 13.
[5] Galdieri, (2012), p. 2699.
[6] Pizzetti, (2010), p. 62, ha affermato che «*non si vive senza lasciare tracce della propria esistenza e, dunque, senza "produrre" dati*».
[7] Soro, (2018), p. 13.

come un diritto autonomo rispetto al rispetto della vita privata e familiare e al domicilio[8].

Similmente, l'art. 1, comma 1, D.Lgs. 30 giugno 2003, n. 196 – c.d. Codice in materia di protezione dei dati personali, come modificato dal D.Lgs. n. 10 agosto 2018, n. 101- dispone che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato.

Può ricordarsi, peraltro, che anche la Dichiarazione dei diritti in *internet*, documento fondamentale per garantire a ciascun individuo l'esercizio di una cittadinanza digitale attiva nel rispetto della libertà, della dignità e della diversità di ogni persona, agli artt. 5 e 6 si occupa di *privacy*, esprimendo principi, che ricalcano quelli sopra menzionati contenuti nella CEDU e nel D.Lgs. n. 196/2003, evidenziando così la stretta connessione tra rete e trattamento dei dati personali[9].

Peraltro, si osservi come il mutato contesto digitale impone un ripensamento del concetto di *privacy*, intesa non come diritto alla non divulgazione dei propri dati, ma come diritto a una corretta diffusione e gestione degli stessi. La *privacy*, comunemente intesa nell'accezione minimale di *right to be let alone,* vede «*mutare il suo contenuto da diritto alla riservatezza a diritto all'autodeterminazione informativa*»[10], arricchendosi di un contenuto ulteriore «*non solo ius excludendi alios dalla conoscenza di informazioni private, ma altresì diritto positivo al controllo dei propri dati personali*»[11]. Viene in rilievo, quindi, la proiezione sociale del diritto alla *privacy*, quale diritto non tanto alla segretezza, ma al controllo dei propri dati personali in rete e alla diffusione consapevole degli stessi[12].

Pertanto, una componente fondamentale della tutela della *privacy* diviene il diritto dell'interessato di accedere ai dati che lo riguardano e di ottenerne la rettifica ed è proprio l'aggiornamento e la contestualizzazione delle informazioni la chiave di volta per garantire una corretta rappresentazione della realtà della persona[13]. È evidente come tali attività di controllo, verifica e aggiornamento risultino particolarmente complesse in rete, in quanto mancano i riferimenti circa il luogo di conservazione dei dati e chiarezza sui criteri utilizzati per selezionarli e analizzarli, emergendo una forte asimmetria tra chi li fornisce e chi effettivamente li utilizza.

Il diritto alla *privacy*, pertanto, non può essere confinato in una sfera statica, ma la sua tutela va adeguata al «*processo evolutivo incrementale in cui si snoda la costruzione della persona*»[14], processo oggi connotato dal sempre maggiore sviluppo delle nuove tecnologie e dalla digitalizzazione di moltissimi aspetti della vita umana.

## 2. "L'approccio preventivo nel trattamento dei dati personali: la *privacy by design* e la *privacy by default*".

In questo scenario, stante la potenziale incontrollabilità dei dati personali una volta collocati in rete, la tutela della *privacy* si sostanzia principalmente nella necessità di prevenire un

[8] Balducci Romano, (2015), pp. 1619 ss.; Rossi Dal Pozzo, (2016), pp. 690 ss.

[9] Il testo individua una serie di principi generali che abbracciano le diverse tematiche connesse all'uso di internet: il diritto alla conoscenza e all'educazione in Rete, la neutralità della Rete, il diritto all'identità. La Dichiarazione è fondata sul pieno riconoscimento di libertà, eguaglianza, dignità e diversità di ogni persona. La garanzia di questi diritti è condizione necessaria per assicurare il funzionamento democratico delle Istituzioni. L'Art. 5. (Tutela dei dati personali), dispone che «*1. Ogni persona ha diritto alla protezione dei dati che la riguardano, per garantire il rispetto della sua dignità, identità e riservatezza. 2. Tali dati sono quelli che consentono di risalire all'identità di una persona e comprendono anche i dati dei dispositivi e quanto da essi generato e le loro ulteriori acquisizioni e elaborazioni, come quelle legate alla produzione di profili 3. Ogni persona ha diritto di accedere ai dati raccolti che la riguardano, di ottenerne la rettifica e la cancellazione per motivi legittimi 4. I dati devono esser trattati rispettando i principi di necessità, finalità, pertinenza, proporzionalità e, in ogni caso, prevale il diritto di ogni persona all'autodeterminazione informativa. 5. I dati possono essere raccolti e trattati con il consenso effettivamente informato della persona interessata o in base a altro fondamento legittimo previsto dalla legge. Il consenso è in via di principio revocabile. Per il trattamento di dati sensibili la legge può prevedere che il consenso della persona interessata debba essere accompagnato da specifiche autorizzazioni. 6. Il consenso non può costituire una base legale per il trattamento quando vi sia un significativo squilibrio di potere tra la persona interessata e il soggetto che effettua il trattamento. 7. Sono vietati l'accesso e il trattamento dei dati con finalità anche indirettamente discriminatorie*». L'art. 6. (Diritto all'autodeterminazione informativa) del medesimo provvedimento prevede che «*1. Ogni persona ha diritto di accedere ai propri dati, quale che sia il soggetto che li detiene e il luogo dove sono conservati, per chiederne l'integrazione, la rettifica, la cancellazione secondo le modalità previste dalla legge. Ogni persona ha diritto di conoscere le modalità tecniche di trattamento dei dati che la riguardano. 2. La raccolta e la conservazione dei dati devono essere limitate al tempo necessario, rispettando in ogni caso i principi di finalità e di proporzionalità e il diritto all'autodeterminazione della persona interessata*»

[10] Cfr. Torre, (2004), p. 41.

[11] Cfr. D'Agostino, (2019).

[12] Picotti (2004), p. 176; Torre, (2004), p. 239; La Manuzzi, (2017), p. 22.

[13] Tampieri, (2017), pp.101 ss.

[14] Soro, (2018), p. 8

trattamento illecito degli stessi.

Tale esigenza di prevenzione, volta a garantire un'adeguata protezione degli individui dai rischi provenienti dallo spazio virtuale, ha condotto il legislatore europeo a intervenire con Regolamento (UE) 2016/679 (c.d. GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, recepito in Italia dal citato D.Lgs. n. 101/2018, che, come anticipato, modifica il D.Lgs. n. 196/2003[15].

Innanzitutto, può osservarsi, come l'Unione Europea, attraverso l'emanazione di un Regolamento in materia di *privacy*, abbia voluto riconoscere una tutela universale della protezione dei dati personali, prevedendo diritti uniformi per tutti i cittadini europei.

Dall'individuazione della protezione dei dati personali come diritto fondamentale ne deriva il passaggio da una tutela prevalentemente rimediale, a un'essenzialmente preventiva, basata sulla responsabilizzazione dei titolari del trattamento.

Il Regolamento si caratterizza, infatti, per un mutamento di ottica, emancipandosi dagli schemi riduttivi del mercato, per accedere a una tutela più ampia della *privacy*, considerata come diritto fondamentale e protetta tramite un approccio fondato sui principi di prevenzione e precauzione[16].

Ciò che connota maggiormente le nuove previsioni contenute nel GDPR è proprio la valorizzazione del momento della prevenzione, incentivando l'adozione di efficaci misure di protezione dei dati personali, soprattutto nelle reti e nei sistemi informatici.

Tale mutamento di paradigma può ravvisarsi, *in primis*, nell'art. 25 del GDPR, che introduce i concetti di *privacy by design*, a mente del quale la protezione dei dati personali deve essere garantita sin dalla progettazione di un processo aziendale e di *privacy by default*, il quale sottintende il fatto che la protezione dei dati personali sia garantita per impostazione predefinita. Ne deriva che le tutte le valutazioni, che il titolare del trattamento deve effettuare in tema di protezione dei dati personali, devono essere compiute a monte, cioè prima di procedere al trattamento dei dati vero e proprio.

Tale norma va letta in combinato disposto con il considerando n. 78 del GDPR, a mente del quale «*la tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita*».

Risulta di particolare interesse anche il principio di *accountability*, in virtù del quale i soggetti gravati dagli obblighi del GDPR dovranno autoresponsabilizzarsi e adottare precise strategie volte ad assicurare la tutela dei dati personali, avendo soprattutto riguardo ai rischi di trattamento illecito degli stessi. In dettaglio, l'art. 24 del GDPR dispone che «*tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*»[17]. Si evince come il legislatore europeo abbia abrogato le misure minime idonee previste dal vecchio art. 33, D.Lgs. n. 196/2003, sostituendole con "*misure tecniche e organizzative*", che impongono di proteggere i dati secondo modalità adeguate al caso concreto. In particolare, l'art. 32, GDPR, rubricato "*sicurezza del trattamento*", 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, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative ade-*

[15] Per un'analisi delle innovazioni apportate con la riforma in parola, tra gli altri, D'Agostino, (2019), 1 ss.; D'Onofrio e T. & Macculi, (2018), pp. 1838-1841; Costantini, (2018), pp. 545-555; Castellaneta, (2018), pp. 259-265; Cuffaro (2018), pp. 1181-1185; Fronticelli Baldelli, (2018), pp. 3109-3114.

[16] Soro, (2018), p. 20; Piraino, (2017), pp. 369 ss.; Senigaglia, (2017), pp. 1023 ss.

[17] La Manuzzi (2017), p. 247; Soro, (2018), 5 ss. La responsabilizzazione viene, altresì, perseguita dal legislatore europeo tramite la cifratura - una tecnica che rende i dati incomprensibili a chiunque non sia autorizzato ad accedervi e consiste nel convertire, in maniera apparentemente casuale una sequenza di numeri e segni che solo chi ha la chiave per decifrare potrà convertire - e la pseudonimizzazione dei dati ovvero un processo, che consente di trattare i dati in maniera tale da non poterli più attribuire ad un utente in particolare senza l'accostamento di informazioni aggiuntive; la valorizzazione del ruolo di controllo e monitoraggio dell'Autorità di sorveglianza; la gestione della procedura di *data breach,* volta anche a informare l'interessato della possibile violazione dei propri dati personali.

*guate per garantire un livello di sicurezza adeguato al rischio*»[18]. Il livello di sicurezza e misure di protezione non è predeterminato *ex ante*, dovendo piuttosto essere adeguato al caso concreto. Il Regolamento introduce, quindi, accanto al concetto di idoneità quello di adeguatezza e, se è vero che le misure di sicurezza devono essere adeguate al livello di sicurezza e, a sua volta, quest'ultimo deve essere adeguato al rischio, è chiaro che la sicurezza di ciascun tipo di trattamento del dato personale parte dall'analisi di rischio.

Analizzato ed individuato il rischio di distruzione, perdita, modifica, divulgazione non autorizzata ovvero accesso, in modo accidentale o illegale, ai dati personali trasmessi, conservati o comunque trattati, il livello di sicurezza è adeguato quando è in grado di prevenire il rischio attraverso, appunto, misure di sicurezza idonee a mantenerlo entro una soglia di accettabilità.

Si delinea, in definitiva, un *risk based approach*, che impone alle aziende di dotarsi di misure di *compliance* tecniche e organizzative, atte a garantire un adeguato livello di sicurezza dei dati personali, facendo particolare attenzione ai rischi che connotano il trattamento.

Tale approccio preventivo pare particolarmente rilevante laddove i dati personali siano trattati in *internet,* in quanto la garanzia del consenso e dell'informativa si relativizza, atteso che la rete, per le sue dimensioni e le modalità di trattamento, si connota per la frammentazione del processo di gestione di dati, che facilmente sfugge al controllo individuale.

## 3. "Reati cibernetici e reati *privacy* impropri a confronto".

Il sopra descritto approccio preventivo ha posto in evidenza come il trattamento illecito dei dati personali non sia frutto della condotta del singolo, ma derivi da una precisa politica di impresa e ha fatto, quindi, emergere la necessità per le società, che inevitabilmente trattano dati personali in tutti i settori della loro attività, di attuare misure specifiche di *compliance* preventive, idonee a garantire la sicurezza dei dati. Difatti, i sopra richiamati principi di *privacy by design* e *privacy by default*, nel richiedere che la protezione del dato personale sia assicurata *ab origine,* come se fosse un'impostazione predefinita, sembrano prodromici a un'estensione dell'autoresponsabilità in ogni fase della vita dell'impresa[19].

Peraltro, ciò che caratterizza l'attività di impresa è il trattamento e coordinamento di un gran numero di dati, comuni e sensibili[20], non solo dei propri dipendenti, ma spesso anche di terzi quali agenti, fornitori, clienti e professionisti.

Tale circostanza sembra essere tenuta in considerazione dal legislatore europeo, che nel Regolamento n. 679/2016 inserisce numerose disposizioni indicative della volontà di imporre gli obblighi di corretta gestione dei dati direttamente in capo alle società.

Significativi in tal senso sono gli obblighi gestionali e organizzativi di cui al Capo IV del GDPR attuabili solo all'interno di un ente che predisponga un'adeguata politica aziendale in tal senso.

Negli stessi termini, può richiamarsi l'apparato sanzionatorio previsto dal GDPR, che sembra essere stato concepito avendo a mente la capacità economica delle grandi imprese, visti i limiti edittali così elevati nel massimo.

A ciò si aggiunga che la gestione dei dati personali confluisce nelle materie soggette a *disclosure* nella dichiarazione non finanziaria cui sono tenuti alcuni tra i cc.dd. enti di interesse pubblico[21], ai sensi del D.Lgs. n. 30 dicembre 2016, n. 254, che ha recepito la Direttiva 2014/95/UE sugli obblighi di «*comunicazione di informazioni di carattere non finanziario e di informazioni sulla diversità da parte di talune imprese e di taluni gruppi di grandi dimensioni*»[22].

Tale disposizione normativa prevede che gli enti interessati debbano comunicare le c.d. informazioni non finanziare legate, in generale, agli impatti sociali e ambientali delle azioni dell'impresa, al rispetto dei diritti umani e delle pari opportunità, alla gestione del personale

[18] Cavallari, (2018), pp. 3 ss.
[19] Bolognini, *et al.*, (2016), p. 324.
[20] Può osservarsi come le società non si limitino a trattare dati comuni dei propri dipendenti, ma ricevano anche una grande quantità di dati personalissimi e sensibili attinenti alla partecipazione ai sindacati, ad aspetti giudiziari e penali ecc.
[21] La previsione riguarda obbligatoriamente gli enti di interesse pubblico con oltre 500 dipendenti e che abbiano superato almeno uno dei due seguenti limiti dimensionali: a) totale dello stato patrimoniale: € 20.000.000; b) totale dei ricavi netti delle vendite e delle prestazioni: € 40.000.000. Per le aziende non ricadenti nell'obbligo fissato dal Decreto in parola, è ammessa la possibilità di pubblicare Dichiarazioni di carattere non finanziario su base volontaria
[22] Per un commento sul tema Bellisario, (2017), pp. 19-46; Rimini, (2018), pp. 187-199; Bonfanti, (2018), pp. 169-192; Del Prete e Ricci, (2017), pp. 509-518.

e alla lotta alla corruzione e, quindi, anche alle *policy* relative alla tutela dei dati personali[23].

Ne deriva che la normativa sui dati personali è divenuta una delle parti centrali della *compliance* societaria.

Il concetto di prevenzione, rischio e adeguatezza e la sua attuazione da parte delle imprese, inevitabilmente richiama un'assonanza con la disciplina di cui al D.Lgs. 8 giugno 2001, n. 231, sulla responsabilità amministrativa da reato delle persone giuridiche e ne fa emergere la connessione con la normativa in materia di trattamento dei dati personali.

Come noto, i reati in materia di *privacy* esulano dall'ambito applicativo del D.Lgs. n. 231/2001[24].

Un tentativo di riavvicinamento delle due discipline vi era stato tramite il decreto legge 14 agosto 2013, n. 93, recante «*Disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di genere, nonché in tema di protezione civile e di commissariamento delle province*», il cui art. 9 aveva apportato, tra l'altro, una significativa modifica all'art. 24 *bis*, D.Lgs. n. 231/2001, includendo nel catalogo dei reati presupposto le seguenti fattispecie: art. 640 *ter* c.p. (frode informatica); art. 55, comma 9, del d.lgs. 21 novembre 2007, n. 231 (utilizzo indebito e falsificazione di carte di credito); artt. 167, 168 e 170 del D. Lgs. 196/2003 (illecito trattamento di dati, falsità nelle dichiarazioni e notificazioni al Garante, e inosservanza di provvedimenti del Garante).

Detta modifica legislativa sorgeva dall'esigenza di recepire le indicazioni europee e internazionali, e, in specie, la Convenzione di Budapest del 2008, che, non solo aveva imposto agli Stati Membri la produzione di una normativa tale da coprire penalmente l'eventualità del compimento di *computer crimes* in tema aziendale, ma aveva anche previsto l'introduzione di una tutela simile anche per quanto riguarda il trattamento illecito dei dati personali. La riforma in parola era destinata ad avere un forte impatto nella tutela dei dati personali all'interno delle persone giuridiche, ma non è stata confermata in sede di conversione; la legge 15 ottobre 2013 n. 119 ha, infatti, soppresso il secondo comma dell'art. 9 del decreto legge[25]. La ragione va probabilmente rinvenuta nel fatto che l'introduzione nel catalogo dei reati-presupposto dei delitti in materia di *privacy* era destinata a comportare importanti riflessi sul piano operativo per le imprese, soprattutto in relazione alla responsabilità amministrativa derivante dall'illecito trattamento dei dati; novità queste troppo rilevanti per poter essere introdotte con decretazione d'urgenza.

Il D. Lgs. 101/2018 di riforma del Codice della *privacy* non ha previsto alcuna disposizione sul punto. Il legislatore delegato ha così perduto l'ennesima occasione per introdurre una tale forma di responsabilità in tale settore nel quale l'ente continua ad essere il "grande assente"[26].

Nell'attuale formulazione dell'art. 24 *bis*, D.Lgs. n. 231/2001, quindi, seppure la rubrica reciti *"Delitti informatici e trattamento illecito di dati"*, non reca alcun riferimento ai reati in materia di *privacy*, ma solo ai delitti informatici[27].

---

[23] In particolare, l'art. 3, co. 1, D.Lgs. n. 254/2016, prevede che «*La dichiarazione individuale di carattere non finanziario, nella misura necessaria ad assicurare la comprensione dell'attività di impresa, del suo andamento, dei suoi risultati e dell'impatto dalla stessa prodotta, copre i temi ambientali, sociali, attinenti al personale, al rispetto dei diritti umani, alla lotta contro la corruzione attiva e passiva, che sono rilevanti tenuto conto delle attività e delle caratteristiche dell'impresa, descrivendo almeno: a) il modello aziendale di gestione ed organizzazione delle attività dell'impresa, ivi inclusi i modelli di organizzazione e di gestione eventualmente adottati ai sensi dell'articolo 6, comma 1, lettera a), del decreto legislativo 8 giugno 2001, n. 231, anche con riferimento alla gestione dei suddetti temi; b) le politiche praticate dall'impresa, comprese quelle di dovuta diligenza, i risultati conseguiti tramite di esse ed i relativi indicatori fondamentali di prestazione di carattere non finanziario; c) i principali rischi, generati o subiti, connessi ai suddetti temi e che derivano dalle attività dell'impresa, dai suoi prodotti, servizi o rapporti commerciali, incluse, ove rilevanti, le catene di fornitura e subappalto*».

[24] Un primo tentativo volto a introdurre la responsabilità della persona giuridica in materia di *privacy*, in epoca antecedente all'entrata in vigore del D. Lgs. 231/2001, si deve alla proposta di legge AC- 2097 presentata alla Camera dei Deputati il 12 gennaio 1993, con la quale, si delineavano alcune sanzioni applicabili direttamente alla persona giuridica per illeciti riguardanti l'omessa nomina del responsabile per la protezione dei dati personali o per la lacunosa notifica della tenuta di una banca di dati che secondo alcuni avrebbero dovuto essere inflitte dal giudice penale. Si sarebbe così ottenuto un doppio beneficio: una maggiore efficacia general-preventiva della sanzione, dotata dello stigma penale e un rispetto rigoroso delle garanzie procedurali per l'ente-imputato. Sul punto Manna, (1993), p. 185; D'Agostino, (2019), p. 50.

[25] Pistorelli, (2013), p. 7; Santoriello (2015), p. 2;

[26] Cfr. D'Agostino, (2019), p. 4; Sul punto anche Sarzana, (2008), p. 1572 ss; Corasaniti e Corrias Lucente, (2009), p. 156 ss.; Beltrani, (2008), pp. 24 ss.

[27] I reati inclusi nel catalogo del D.Lgs. n. 231/2001, all'art. 24 *bis*, sono: l'accesso abusivo ad un sistema informatico o telematico (615 *ter* c.p.), l'intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (617 *quater* c.p.), l'installazione di apparecchiature predisposte a tal fine (617 *quinquies* c.p.), il danneggiamento di informazioni, dati e programmi informatici (635 *bis* c.p.), il danneggiamento di informazioni, dati e programmi utilizzati da Stato, ente pubblico o di altra utilità (635 *ter* c.p.), il danneggiamento di sistemi informatici o telematici (635 *quater* c.p.), il danneggiamento di analoghi sistemi di pubblica utilità (635 *quinquies* c.p.). La medesima norma al comma 2 contempla due fattispecie di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (615 *quater* c.p.) e della diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema

Non può trascurarsi, tuttavia, come quest'ultimi siano strettamente connessi alla tutela della *privacy*, atteso che il mondo virtuale rappresenta una delle principali fonti di rischio di trattamento illecito dei dati personali.

Difatti, molti dei reati informatici inseriti nel codice penale indirettamente appaiono anche volti a tutelare la *privacy*, in quanto nel proteggere l'integrità di un sistema informatico e i dati ivi contenuti, tutelano anche la riservatezza.

Parte della dottrina definisce i reati in parola "*reati privacy impropri*", ovvero fattispecie plurioffensive, volte a tutelare il bene *privacy* in modo indiretto, come se il legislatore, attraverso la tutela dell'integrità di un sistema informatico, miri anche a proteggere i dati personali ivi contenuti[28].

In un'ottica *a contrario,* altra parte della dottrina[29] colloca accanto ai reati informatici "in *senso stretto*" – connotati dalla previsione, nella fattispecie legale, di specifici elementi di tipizzazione, contenenti un esplicito riferimento alle nuove tecnologie dell'informazione o della comunicazione – i reati informatici in senso ampio o meglio i "*reati cibernetici*" ovvero tutte quelle fattispecie la cui commissione si realizzi o possa realizzarsi in rete. Emblematici, in tal senso, sarebbero proprio i reati in materia di *privacy* di cui al D.Lgs. n. 196/2003.

Il legame tra informatica e *privacy*, emerge anche avendo riguardo al concetto di trattamento illecito dei dati personali, definito all'art. 4, n. 12, Regolamento 679/2016/UE come «*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*». I casi di *data breach* elencati appaiono sovrapponibili ai reati informatici, atteso che i concetti di diffusione, distruzione o l'accesso non autorizzato ai dati personali richiamano le condotte oggetto di alcuni delitti informatici quali, esemplificativamente, il danneggiamento di informazioni o dati o anche la distruzione di un sistema informatico che contiene dati personali (art. 615 *quinques* c.p.) o la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti di cui all'art. 615 *bis*, co. 3, c.p.

Sussiste, in definitiva, una connessione, da un punto di vista logico o cronologico, tra i reati in materia di trattamento dei dati personali e quelli informatici idonei a punire comportamenti prodromici o strumentali a violazioni della *privacy*.

## 4. "La prevenzione del rischio *privacy* tramite il modello di *compliance* 231".

La sopra delineata connessione tra reati *privacy* e delitti informatici consente di affermare che i *cyber crimes* creano un ponte tra il modello 231 e la disciplina sulla *privacy*, in quanto nella costruzione del modello organizzativo, volto a prevenire, tra gli altri, i reati in materia informatica, occorre avere riguardo anche alla tutela dei dati personali.

Per altro verso, il sistema di organizzazione, gestione e controllo in tema di *privacy* rileva anche sulla prevenzione dei reati informatici.

Ciò conduce a domandarsi se alla *privacy* sia applicabile il modello organizzativo di cui al D.Lgs. n. 231/2001. A ben vedere i due modelli presentano diversi punti di contatto che saranno analizzati nel prosieguo.

### 4.1. "*Il* risk based approach".

Con specifico riferimento ai reati informatici, in particolare, il modello organizzativo 231 si fonda sulla preventiva valutazione – di solito compendiata in un documento denominato Target of Evaluation (ToE) - di ciò che deve essere protetto, e, quindi, sull'individuazione dei

informatico o telematico (art. 615 *quinquies* c.p.).

[28] Luberto, (2008), p. 900. L'Autore suggerisce altresì un'ulteriore scissione tra i reati *privacy* impropri non informatici e informatici; infatti, gli artt. 614, 615 e 615-*bis* c.p. sono posti a tutela di un concetto di riservatezza connessa alla tutela del domicilio degli individui, sottolineandone l'aspetto prettamente materialistico. Molti altri reati sono, invece, posti a tutela di beni giuridici, fra cui la riservatezza, intrinsecamente collegati con ambiti prevalentemente informatici.

[29] Patrono, (1985), pp. 557 ss.

sistemi informatici e telematici presenti in azienda. Il modello, quindi, al suo interno, conterrà la prevenzione di tutte le fattispecie di reato che abbiano origine dall'esterno della rete aziendale e, inoltre, tutti i possibili reati che possono essere compiuti dagli utenti interni della rete stessa.

Il modello organizzativo deve, poi, prevedere una parte speciale per disciplinare l'uso del sistema informatico all'interno dell'azienda, che garantisca la trasparenza delle decisioni aziendali e dei flussi informatici di dati, tramite un criterio di tracciabilità delle decisioni e delle operazioni, per impedire o almeno facilmente rintracciare l'individuazione delle condotte di illecito utilizzo delle strutture informatiche aziendali[30].

In tale ottica sarà di assoluta importanza la nomina di un amministratore di sistema e di un responsabile delle credenziali di accesso, che si occupi di tutte le attività di gestione controllo e monitoraggio delle procedure informatiche, come il controllo degli accessi e della sicurezza.

Similmente, l'obiettivo di prevenzione e responsabilizzazione contenuto nel GDPR potrebbe essere realizzato attuando uno specifico modello organizzativo di prevenzione, del tutto simile a quello predisposto ai sensi del D.Lgs. n. 231/2001. L'elemento di novità, che è stato introdotto con il Regolamento 2016/679, è il cosiddetto *Data Protection Impact Assesment* (DPIA)[31].

Il GDPR, infatti, al fine di dare attuazione ai sopra richiamati principi di *privacy by design* e *privacy by default* e nell'ottica di un approccio preventivo alla tutela dei dati personali, all'art. 35 impone una valutazione di impatto sulla protezione dei dati, al fine di determinare l'esistenza e la gravità di rischi nel trattamento.

Si impone, quindi, al titolare e al responsabile del trattamento di effettuare uno *screening* aziendale, per comprendere che tipo di dati personali vengono trattati e quali infrastrutture tecnologiche vengono utilizzate, in modo da identificare eventuali vulnerabilità e fragilità dei sistemi. Si tratta di una vera e propria mappatura dei rischi legati al trattamento dei dati personali che ha lo scopo di ottenere la piena consapevolezza dei rischi cui l'impresa è esposta così da agevolare il processo di protezione.

Le società, inoltre, dovranno adeguatamente diversificare i processi e le funzioni inerenti la *privacy* e formare adeguatamente tutti i propri dipendenti.

## 4.2. "Data Protection Officer *e Organismo di Vigilanza: un legame complesso".*

Ulteriore possibile punto di contatto tra la disciplina in materia di *privacy* e i modelli 231 è la previsione di strumenti di controllo e sorveglianza sulla *compliance*. In particolare, il D.Lgs. n. 231/2001 individua nell'Organismo di Vigilanza il soggetto deputato a sorvegliare sull'adeguatezza del modello e sulla sua attuazione e aggiornamento.

Si tratta di un organismo collegiale, dotato di imparzialità e indipendenza e di autonomi poteri di controllo e iniziativa, i cui compiti, ai sensi dell'art. 6, lett. b), D.Lgs. n. 231/2001 sono vigilare sul funzionamento e l'osservanza del Modello di Organizzazione, Gestione e Controllo e di curare il suo aggiornamento[32].

Similmente, il GDPR, prevede, e in alcuni casi impone, la nomina di un *Data Protection Officer* (DPO), che, al pari dell'ODV, deve possedere specifiche caratteristiche di professionalità, imparzialità e indipendenza. Il DPO può essere un soggetto interno all'azienda, ossia un dipendente del Titolare o del Responsabile del trattamento, oppure un soggetto esterno che assolve i propri compiti sulla base di un contratto di servizi[33].

L'art. 39 del GDPR affida al DPO, tra gli altri compiti, quello di sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la

[30] Saranno, quindi, esplicitati i sistemi di controllo messi in opera al fine di monitorare l'attività dei dipendenti e approfonditi aspetti quali il documentare ed impedire comportamenti illeciti come l'uso di *password* non autorizzate, detenzione o installazione di *software* non esplicitamente previsti dall'azienda, escludere la ovvia detenzione di *virus*, *spyware* di ogni genere e dispositivi atti all'interruzione di servizi o alle intercettazioni in ambito aziendale.
[31] Pisapia, (2018), pp. 105 ss.; Cadoppi, *et al.*, (2019), pp. 1019 ss.
[32] Montalenti, (2014), pp. 7-30; Paonessa, (2014), pp. 440-448; Consulich, (2015), pp. 425-467; Giuffré, (2016), pp. 233-243; Colombo, *et. al.*, (2016), pp. 844-851; Montalenti, (2017), pp. 963-995.
[33] D'Agostino, (2017), pp. 2 ss.; Frillici, Ghini, (2017), pp. 115 ss.

formazione del personale, che partecipa ai trattamenti e alle connesse attività di controllo. Devono, infatti, essere previsti controlli periodici del mantenimento dell'adeguatezza delle misure adottate anche in previsione del fatto che tecnologia, tecnica e tipologie di trattamento sono in continuo, vorticoso sviluppo.

In entrambi i casi, sia l'OdV che il DPO nella loro attività di controllo e monitoraggio segnalano eventuali violazioni, lasciando la decisione circa le misure da intraprendere alla persona giuridica, che deve auto-valutare la situazione e decidere per il meglio, nel solco della regola di autoresponsabilità e *accountability*.

Risulta evidente, quindi, come le due figure risultino in parte coincidenti, seppure non completamente sovrapponibili, per come si dirà in seguito.

A ben vedere la disciplina in materia di privacy incide sul ruolo dell'OdV anche sotto altri aspetti. In particolare, il dibattito dottrinale alla luce dell'entrata in vigore del GDPR e del D.Lgs. n. 101/2018, si è focalizzato sulla posizione dell'organismo di vigilanza rispetto agli obblighi in materia di privacy[34].

Ciò, poiché, detto organismo, nello svolgimento delle sue attività "*entra in contatto con una pluralità di dati personali, quali, in particolare, dati sensibili e dati giudiziari: ciò impone, dunque, di procedere all'individuazione dei pertinenti profili [soggettivi] connessi con il trattamento dei dati personali*"[35].

In dettaglio, l'OdV tratta dati personali provenienti dai flussi informativi, di cui all'art. 6, co. 2, lett. d), D.lgs. 231/2001 e dalle proprie attività di controllo e vigilanza.

Ulteriori dati potrebbero anche derivare dalle segnalazioni sulle violazioni del modello che l'organismo riceve in attuazione della disciplina sul *Whistleblowing*, di cui si dirà in seguito.

È evidente, quindi, come sia di estrema rilevanza stabilire quale posizione soggettiva l'OdV ricopra rispetto ai dati personali trattati e, quindi, quali siano gli obblighi in materia di *privacy* che lo stesso deve rispettare.

In *primis* occorre chiarire che l'OdV - laddove non sia monosoggettivo ma, come auspicato anche dalla Linee Guida in materia e dalla dottrina[36], sia un organismo collegiale - debba essere inteso come un *unicum*.

Difatti, come già sancito dall'art. 28 del D.lgs. 196/2003, in caso di soggetti complessi le qualifiche soggettive *privacy* devono essere riferite a "*l'entità nel suo complesso, considerando come responsabile del trattamento la società o l'organismo in quanto tali piuttosto che una specifica persona al loro interno*"[37]. Gli obblighi in materia di *privacy*, in definitiva, gravano sull'OdV inteso come entità e non sui singoli membri, interni o esterni, che lo compongono.

Punto nodale resta lo stabilire se l'organismo in parola possa essere qualificato come titolare del trattamento dei dati personali o come mero responsabile, laddove il primo viene definito dall'art. 4, n. 7, GDPR come "*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 di dati personali*", mentre il secondo, ai sensi dell'art. 4, n. 8, GDPR è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*".

Parte della dottrina qualifica l'OdV come titolare del trattamento, ritenendo che dagli autonomi poteri di iniziativa e controllo, attribuiti all'organismo dall'art. 6, D.Lgs. n. 231/2001, ne derivino anche i poteri di determinare le finalità e i mezzi del trattamento propri del titolare[38].

Tale approccio non trova l'accoglimento di altra parte della dottrina che, in un'ottica funzionalista, fondata sull'attività e i poteri effettivamente attribuiti al titolare del trattamento, evidenzia come il compito di vigilare non possa essere confuso con l'autonomia nella determinazione delle finalità della vigilanza e, quindi, dei trattamenti strumentali ad essa[39].

Tale dottrina evidenzia come le finalità del trattamento dei dati di interesse dell'OdV non sono determinate dall'organismo stesso bensì: "*a) predeterminate, in generale, dal d.lgs. 231/2001 ("vigilanza sul funzionamento e l'osservanza dei modelli" per "prevenire reati della specie di quello*

[34] Sul tema si veda il *Position Paper* sulla posizione soggettiva dell'ODV a fini privacy, elaborato dall'AODV nel marzo 2019, in *www.aodv231.it*.
[35] Perinu, (2019), 2 ss.
[36] *ex multis*, Galletti, (2006), pp. 126 ss.; Montalenti, (2009), pp. 643 ss.
[37] Bolognini *et. al.*, (2016), pp. 124 ss.
[38] Perugini, (2017), pp. 2 ss.
[39] *Position Paper* sulla posizione soggettiva dell'ODV a fini privacy, elaborato dall'AODV nel marzo 2019, in *www.aodv231.it.*

*verificatosi"); b) e declinate, in particolare, dal modello di organizzazione, gestione e controllo, che è "adottato [dal]l'organo dirigente" e non dall'OdV (art. 6, comma 1, lett. a), d.lgs. 231/2001); c) lo stesso OdV è istituito da "l'organo dirigente" (art. 6, comma 1, lett. b), d.lgs. 231/2001) che "dovrà disciplinare gli aspetti principali relativi al funzionamento dell'OdV"*[40].

Peraltro, anche con riferimento ai mezzi che l'organismo utilizza per il trattamento, si è evidenziato come questi vengano determinati negli aspetti fondamentali dall'organo dirigente nell'ambito della disciplina del funzionamento dell'OdV.

Infine, occorre considerare che "*il rispetto delle norme al cui controllo [gli OdV] sono preposti è innanzitutto un obbligo gravante sulla società oggetto del controllo*"[41], sicché l'organismo si limita a trattare dati personali già appartenenti all'ente vigilato.

Esclusa la configurabilità dell'OdV come titolare del trattamento dei dati personali, parte della dottrina esclude anche che la qualifica di responsabile possa essere attribuibile all'organismo. Ciò alla luce delle modifiche intervenute con il GDPR e il D.lgs. n. 101/2018, che hanno escluso la possibilità che il responsabile del trattamento sia un soggetto interno all'ente. Difatti, secondo la nuova disciplina, requisito essenziale per essere riconosciuto quale responsabile è "*essere una persona giuridica distinta dal titolare*"[42], che, nel caso di specie, sarebbe l'ente vigilato dall'OdV[43].

Nel caso dell'OdV una siffatta distinzione non sarebbe configurabile, atteso che lo stesso ai sensi dell'art. 6, D.lgs. n. 231/2001, è un organismo dell'ente, interno allo stesso[44]. Peraltro, i requisiti di indipendenza e autonomia che connotano l'OdV sarebbero incompatibili con il ruolo di responsabile del trattamento, il quale agisce secondo le indicazioni fornite dal titolare, creandosi un conflitto di interessi tra controllante (l'OdV) e controllato (l'ente)[45].

In definitiva la tendenza dominante è quella di ritenere assorbito l'inquadramento soggettivo dell'OdV ai fini della *privacy* da quello dell'ente vigilato del quale l'organismo costituisce una parte[46].

Ciò, peraltro, non esclude che l'ente vigilato, in qualità di Titolare, possa prescrivere all'OdV, nell'ottica dell'attuazione del principio di *accountability*, il rispetto di particolari misure tecniche e organizzative adeguate a garantire che il trattamento sia effettuato conformemente al GDPR, purché non interferenti con gli autonomi poteri di iniziativa e di controllo spettanti all'organismo[47].

## 4.3. *"La disciplina del* Wisthleblowing*".*

Infine, sia il D.Lgs. n. 231/2001 sia il GDPR si occupano di *Whistleblowing*.

Per quanto concerne la responsabilità amministrativa da reato, la legge 30 novembre 2017, n. 179, recante "*Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato*" ha, tra l'altro, modificato l'art. 6, D.Lgs. n. 231/2001, al fine di prevedere una puntuale tutela per tutti quei dipendenti e/o collaboratori di società, che abbiano segnalato illeciti di cui siano venuti a conoscenza nell'ambito delle proprie mansioni lavorative[48].

In particolare, sono stati introdotti i nuovi commi 2 *bis*, 2 *ter* e 2 *quater* nella citata disposizione, la quale, nella formulazione attuale, dispone che i modelli organizzativi devono prevedere al loro interno una pluralità di "canali" diversi, rispetto a quello comune della *governance* prestabilito in base al diritto societario applicabile secondo la struttura prescelta, che consentano di presen-

[40] *Position Paper* sulla posizione soggettiva dell'ODV a fini privacy, elaborato dall'AODV nel marzo 2019, in *www.aodv231.it.*
[41] Perugini, (2017), pp. 2 ss.
[42] Opinion 1/2010 del Art. 29 *Data Protection Working Party*
[43] Tale soluzione non convince parte della dottrina che osserva come nei casi in cui l'OdV sia composto solo da membri esterni o abbia una composizione mista non può rivestire una posizione equiparabile a quella dell'ente ma dovrebbe essere nominato responsabile del trattamento, con obblighi di autonomi di verifica e controllo. Sul punto, Barbarossa (2019), pp. 2 ss.
[44] Santoriello, (2015), pp. 109 ss.; Pisani, (2008), pp. 155 ss.; Sfameni, (2007); Rordorf, (2001), 1297 ss.; Bartolomucci, (2002), pp. 10 ss.;
[45] Perugini, (2017), pp. 2 ss. L'OdV non potrebbe neppure rivestire la qualifica di autorizzato al trattamento riferita esclusivamente a persone fisiche, mentre l'OdV normalmente come detto è un organismo collegiale da considerare come tale anche ai fini della qualificazione *privacy*.
[46] *Position Paper* sulla posizione soggettiva dell'ODV a fini privacy, elaborato dall'AODV nel marzo 2019, in *www.aodv231.it.*
[47] Perugini, (2017), pp. 2 ss.
[48] Coceani, (2018), pp. 293-302; Frignani e Grosso, (2004), p. 387; Frignani, (2018), pp. 3 ss.; Ferrante, (2018). Pp.145-172; D'Urgolo, (2018), pp. 2 ss.

tare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del D.Lgs. n. 231/2001 o di violazioni del modello di organizzazione e gestione dell'ente[49]. La nuova disciplina impone, altresì, il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione e l'introduzione nel sistema disciplinare di sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

È previsto, altresì, che l'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni possa essere denunciata all'Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo. In ultimo, l'art. 6, co. 2 *quater*, D.Lgs. n. 231/2001 dispone la nullità del licenziamento ritorsivo o discriminatorio del soggetto segnalante, così come di qualsiasi altra misura ritorsiva. Nel caso di controversie legate all'irrogazione di sanzioni disciplinari o all'adozione di ulteriori misure organizzative con effetti negativi sulle condizioni di lavoro del segnalante, il datore di lavoro ha l'onere di dimostrare che esse sono fondate su ragioni estranee alla segnalazione stessa[50].

In applicazione di detta disciplina si ritiene che il Modello Organizzativo debba indicare chiaramente a quale soggetto o organo debbano essere indirizzate le segnalazioni oggetto delle nuove disposizioni. Tale soggetto potrebbe certamente essere l'Organismo di Vigilanza in virtù della sua autonomia e indipendenza rispetto ai vertici dell'ente[51].

Sembra evidente che la disciplina del *whistleblowing* debba integrarsi con la disciplina in materia di *privacy*.

In dettaglio, il D.Lgs. n. 101/2018 ha modificato il D.Lgs. n. 196/2003, prevedendo all'art. 2 *undecies*, co. 1, lett. f), la possibilità di limitare l'esercizio dei diritti d'accesso dell'interessato nel caso in cui ne possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità del dipendente, che segnala, ai sensi della legge n. 179/2017, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio[52]. La medesima norma prevede, altresì, che, nei casi in parola, l'esercizio dei diritti dell'interessato può essere limitato, ritardato o eventualmente eluso per mezzo di una comunicazione motivata, senza che questa possa in alcun modo compromettere la finalità della limitazione, nei tempi e nei limiti in cui questo rappresenti una misura proporzionata e necessaria[53].

Si noti che tanto il D.Lgs. n. 231/2001 quanto il Codice *privacy* tutelano la riservatezza dell'identità del segnalante e non il suo anonimato, richiedendo che l'identità del soggetto che segnala sia comunque nota. Come chiarito dall'Autorità Nazionale Anticorruzione, difatti, il denunciante può godere di una tutela adeguata soltanto se si rende riconoscibile[54]. Ciò non esclude che i modelli organizzativi possano contemplare anche canali per effettuare segnalazioni in forma anonima. Tale ipotesi sembra, tuttavia, rendere più complessa la verifica della fondatezza della denuncia, con il rischio di alimentare denunce infondate, che hanno poco a che fare con la tutela dell'integrità dell'ente[55].

Sul tema rilevante pare anche l'intervento della legislazione europea, attuato in data 16 aprile 2019 con la "*Risoluzione legislativa del Parlamento europeo sulla proposta di direttiva del Parlamento europeo e del Consiglio riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione*"[56]. Si tratta di un'innovazione legislativa rilevante poiché fissa *standard* minimi di protezione allo scopo di superare le diversità di trattamento esistenti fra i vari Paesi

[49] L'art. 6, co. 2 bis, D.Lgs. n. 231/2001, in dettaglio, dispone che debbano essere previsti : «*a) uno o più canali che consentano ai soggetti indicati nell'articolo 5, comma 1, lettere a) e b), di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione; b) almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante; c) il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione; d) nel sistema disciplinare adottato ai sensi del comma 2, lettera e), sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate*».
[50] Sul tema si vedano le Linee Guida di Confindustria sulla disciplina del *whistlebolwing*, in *www.confindustria.it*
[51] Linee Guida di Confindustria sulla disciplina del *whistlebolwing*, in *www.confindustria.it*
[52] Bolognino, (2018), pp. 9 ss.
[53] Fedi, (2018), pp. 1087 ss.
[54] Determinazione ANAC n. 6 del 28 aprile 2015, "*Linee Guida in materia di tutela del dipendente pubblico che segnala illeciti*", in *www.anticorruzione.it*
[55] Linee Guida di Confindustria sulla disciplina del *whistlebolwing*, in *www.confindustria.it*
[56] Testo consultabile in *www.eurlex.it*

europei, armonizzando la disciplina.

La Direttiva estende l'obbligo di offrire canali di ricezione delle segnalazioni sicuri a tutte le aziende con più di 50 dipendenti sia pubbliche che private e conferma l'obbligo di svolgere indagini interne, portando dunque le aziende ad assumere un comportamento più proattivo nella prevenzione e gestione degli illeciti commessi all'interno dell'ente.

Per garantire la sicurezza dei potenziali informatori e la riservatezza delle informazioni divulgate, le nuove norme consentiranno di comunicare le segnalazioni direttamente alle autorità nazionali competenti, nonché agli organi e le agenzie competenti dell'UE. Pertanto, tali canali di comunicazione dovranno essere creati sia dagli enti sia dalle autorità nazionali.

In più, fornisce una protezione legale a un ampio ventaglio di soggetti, non solo dipendenti ma anche consulenti, fornitori, stagisti e volontari.

Tale intervento legislativo certamente condurrà il legislatore italiano a introdurre nuove norme di adeguamento alla normativa europea, con conseguenti modificazioni sia in materia di *privacy* che in tema di *compliance ex* D.Lgs. n. 231/2001.

## 5. "Verso un nuovo modello organizzativo *privacy* integrato?"

I delineati elementi di somiglianza non devono condurre a ritenere che il modello organizzativo 231 possa essere applicato *tout court* alla disciplina in materia di *privacy,* che presenta delle particolarità. L'approccio *risk based* è sicuramente il medesimo, tuttavia, sembrano potersi ravvisare delle differenze rispetto all'oggetto e alla finalità dello stesso.

La valutazione del rischio *ex* D.lgs. 231/01, da un lato mira a rintracciare, analizzare e valutare i rischi di commissione del reato, che possono fisiologicamente annidarsi nella gestione dei processi aziendali, dall'altro lato, risulta funzionale a garantire l'integrazione e l'attuazione di misure di controllo, che consentano di pervenire ad un'organizzazione aziendale tale da prevenire la commissione di reati.

Per converso la valutazione del rischio *ex* GDPR mira a rintracciare, analizzare e valutare il rischio di trattamento illecito dei dati personali, al fine di conformarsi ad un obbligo legislativo e, contestualmente, di proteggere e tutelare l'interessato al trattamento.

Peraltro, l'esenzione di responsabilità a favore della persona giuridica di cui agli artt. 6 e 7, D.Lgs. n. 231/2001, in relazione all'esatta costruzione e applicazione del modello organizzativo, non è prevista nel GDPR, nell'ambito del quale l'adozione di un modello di *compliance* efficiente è solo un elemento di valutazione della responsabilità del titolare del trattamento. Difatti, anche l'adozione di eventuali codici di condotta certificati, pure previsti, non ha funzione scriminante, ma è semplicemente sintomo di adeguatezza delle misure adottate al GDPR.

Con riferimento, poi, alle figure del DPO e dell'OdV queste, come anticipato, non sono sovrapponibili, avendo funzioni differenti. L'OdV sorveglia il modello organizzativo "dall'esterno" senza entrare nello stesso, il DPO, invece, riveste anche una funzione consultiva, che determina una sua maggiore ingerenza nella *compliance* in materia di *privacy*. Inoltre, le valutazioni operate dal DPO hanno un riferimento positivo quale il Codice *privacy* e il GDPR, a differenza dell'OdV, che ha a riferimento il modello organizzativo e la sua adeguatezza preventiva.

Può osservarsi, tra l'altro, come le uniche condotte di reato rilevanti nell'ambito della costruzione di un modello organizzativo, ai sensi del D.Lgs. n. 231/2001, siano quelle finalizzate a portare un interesse o un vantaggio per la persona giuridica.

Difatti, prevenire il rischio di trattamento illecito dei dati *ex* D.Lgs. 231/01, a stretto rigore, significa prevenire il trattamento illecito commesso nell'interesse o a vantaggio della persona giuridica, non essendo rilevanti quelle condotte poste in essere nell'interesse o a vantaggio di terzi o addirittura dannose per l'ente.

Diversamente, il modello organizzativo *privacy* dovrebbe essere volto a prevenire tutte le ipotesi di violazione della normativa in materia, anche quelle che determinerebbero un danno per la società. Pertanto, aver implementato ed attuato un idoneo e adeguato sistema dei controlli ai sensi del D.Lgs. n. 231/2001 può non esser sufficiente per poter vantare un idoneo e adeguato sistema di protezione dei dati personali trattati.

Dalle considerazioni sopra svolte, risulta evidente come sia veramente auspicabile un intervento normativo di armonizzazione e coordinamento del coacervo di norme che disciplinano la *cyber security* di dati, sistemi e reti e i modelli di prevenzione degli illeciti nelle aziende. In

particolare, vista la forte esigenza di prevenzione nell'ambito della tutela dei dati personali in ambito societario e atteso che la tutela di cui all'art. 24 *bis*, D.Lgs. n. 231/2001 risulta debole e inidonea a ricomprendere tutte le possibili condotte lesive della *privacy,* sarebbe certamente auspicabile un intervento legislativo volto a introdurre i reati relativi al trattamento dei dati personali nell'ambito delle fattispecie presupposto di cui al D.Lgs. n. 231/2001. Il legislatore dovrebbe procedere a un'opera di coordinamento tra il modello 231 e il modello organizzativo delineato dal GDPR, evitando duplicazioni organizzative e sanzionatorie e semplificando l'attività di adeguamento delle imprese, che oggi vanno incontro a inutili appesantimenti nella gestione societaria. Ciò consentirebbe di rafforzare e rendere più efficiente la tutela dati personali trattati nel panorama aziendale e della riservatezza informatica in generale, affrontando il problema direttamente e non in modo trasversale.

In mancanza di un intervento legislativo organico, l'obiettivo verso cui tendere è l'implementazione di un sistema di controlli idoneo ed adeguato a prevenire il rischio di commissione di reati "connessi" al trattamento di dati personali, ivi inclusi i reati informatici, e, al contempo, idoneo a proteggere gli stessi dati personali dagli specifici rischi contemplati dal GDPR. Ciò che sicuramente ha preminente importanza è non creare un sistema di controlli interno ridondante e/o, addirittura, incoerente: reciprocità e relazione, ove possibili, non potranno che accrescere l'efficacia del sistema dei controlli interni aziendali.

Tale obiettivo si potrebbe realizzare con la costruzione e l'adozione di un modello organizzativo integrato, soprattutto con riferimento ai delitti informatici, che garantisca un coordinamento e collegamento tra la disciplina di cui al D.lgs. n. 231/2001 e la normativa in materia di *privacy*, tenendo conto delle peculiarità di quest'ultima.

Ciò al fine di evitare una duplicazione di procedure e di coordinare le figure di controllo, ovvero il DPO e l'OdV, che potrebbero cooperare nell'aggiornamento del modello integrato per le materie inerenti al trattamento e la protezione dei dati e i reati informatici. In particolare, il DPO, quale figura di controllo di secondo livello, dovrebbe informare periodicamente l'Organismo di Vigilanza circa i trattamenti in essere e sulla prevenzione di reati, segnalando eventuali violazioni.

L'Organismo di Vigilanza dovrebbe, invece, collaborare con il DPO, al fine di aggiornare il Modello per le materie inerenti al trattamento e la protezione dei dati e per avere informazioni sulla *privacy*, sia a livello di adempimenti normativi, sia a livello, più tecnico, di predisposizione delle sicurezze per il corretto trattamento.

Tale modello integrato potrebbe rendere più effettiva la compliance in un'ottica principalmente preventiva, con l'obiettivo di incrementare la tutela dei dati personali nell'ambito delle realtà d'impresa e di responsabilizzare maggiormente non solo i singoli, ma soprattutto le persone giuridiche.

Ciò fermo restando che si potrà giungere ad una tutela effettiva dei dati personali in rete solo tramite la diffusione di una cultura della protezione dei dati personale, fondata sulla comprensione del fatto che la *privacy* non è un costo per le società, sempre più digitali e interconnesse, ma una risorsa essenziale da proteggere.

Quella della protezione dei dati è ormai divenuta una frontiera su cui si gioca una parte rilevante del nostro futuro come singoli e come collettività. Pertanto, per le persone giuridiche «*il passo più importante che resta da fare, raccogliendo una delle sfide più importanti che il legame tra tecnologica, diritti e prevenzione pone alle nostre generazioni, è quello del riconoscimento universale del diritto alla protezione dei dati personali, quale primo presupposto di libertà nel XXI secolo*»[57].

## Bibliografia

Balducci Romano, Fabio, (2015), "La protezione dei dati personali nell'Unione europea tra libertà di circolazione e diritti fondamentali dell'uomo", *Rivista italiana di diritto pubblico comunitario*, 6, pp. 1619-1659;

Bartolomucci, Sandro (2002), "Responsabilità amministrativa dell'ente: l'adozione di modelli organizzativi", *Diritto e pratica societaria*, 17, pp. 10-25;

[57] Soro, (2018), p. 166

Bellisario, Elena (2017), "Rischi di sostenibilità e obblighi di "disclosure": il d. lgs. n. 254/16 di attuazione della dir. 2014/95/UE", *Le Nuove leggi civili commentate*, 1, pp. 19-46;

Beltrani, Sergio, (2008), Reati informatici e d.lgs. 231/2001 alla luce della legge di attuazione della Convenzione di Budapest, *La responsabilità amministrativa delle società e degli enti*, 2008, 4, pp. 24 ss.

Bolognini, Luca, Pelino, Enrico, Bistolfi, Camilla, (2016), *Il Regolamento privacy europeo*, (Milano, Giuffrè).

Bonfanti, Angelica, (2018), "Corporate social responsibility and corporate accountability: the Italian private international law perspective", *Annuario di diritto comparato e di studi legislativi*, pp. 169-192;

Cadoppi, Alberto, Canestrari, Stefano, Manna, Adelmo, (2019), *Cybercrime*, (Milano, Ipsoa);

Castellaneta, Marina (2018), "L'incidenza del regolamento GDPR sul quadro normativo esistente", *Notariato*, 3, pp. 259-265;

Cavallari, Giulia (2018), La sicurezza del trattamento: analisi dell'articolo 32 GDPR, *www.iusinitinere.it*;

Coceani, Michele, (2018), "Whistleblowing" nel settore privato e sicurezza sul lavoro", *ISL: igiene e sicurezza del lavoro*, 5 pp. 293-302;

Colombo, Cristina, Maniccia, Alessia, Tescione, Vincenzo, (2016), "L'organismo di vigilanza ex d.l.vo n. 231/01. Requisiti, funzioni e profili problematici", *Rivista penale*, 10, pp. 844-851;

Consulich, Federico (2015), "Vigilantes puniri possunt". I destini dei componenti dell'organismo di vigilanza tra doveri impeditivi e cautele relazionali, *Rivista trimestrale di diritto penale dell'economia*, 3, pp. 425-467;

Corasaniti, Giuseppe, Corrias Lucente, Giovanna, (2009), *Cybercrime, responsabilità degli enti, prova digitale*, (Padova, Cedam);

Costantini, Federico, (2018), "Il Regolamento (UE) 679/2016 sulla protezione dei dati personali", *Il Lavoro nella giurisprudenza*, 6, pp. 545-555;

Cuffaro, Vincenzo, (2018), "Quel che resta di un codice: il D.Lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del codice della privacy al regolamento sulla protezione dei dati Commento a d.lg. 10 agosto 2018, n. 101", *Corriere giuridico*, 10, pp. 1181-1185;

D'Agostino, Luca, (2019), "La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D.Lgs. 10 agosto 2018, n. 101", *Archivio penale*, 1-58;

Del Prete, Chiara, Ricci, Daniela, (2017), "Comunicazione di informazioni di carattere non finanziario e di informazioni sulla diversità. D.Lgs. n. 254/2016: introduzione alla disciplina e problematiche applicative", *Rivista dei dottori commercialisti*, 4, pp. 509-518.

D'Onofrio, Tommaso, Macculi, Carlo, (2018), "La rivoluzione GDPR", *Corriere tributario*, 23, pp. 1838-1841;

D'Urgolo, Giandomenico, (2018), "La tutela del pubblico dipendente (e non solo) che segnala illeciti (c.d. "whistleblower")", *GiustAmm.it*, 3, pp. 1-7;

Fedi, Andrea, (2018), "Diritti dell'impresa e protezione dei dati personali", *Le Società*, 10, pp. 1087-1100;

Ferrante, Vincenzo, (2018), "Novità per il settore pubblico e privato in tema di "whistleblowing", *Il lavoro nel diritto*, 2, pp. 145-172;

Frignani, Aldo, (2018), "Whistleblowing": finalmente una legge generale "ad hoc". Luci ed ombre", *Nuovo notiziario giuridico* pp. 1-20;

Frignani, Aldo, Grosso, Patrizia, (2004), L'organismo di controllo, sua composizione e problematiche, Monesi, Carlo, (eds.), *Modelli organizzativi ex d.lgs. 231/2001 (Etica d'impresa e punibilità degli enti)*, (Giuffrè, Milano), pp. 387;

Frillici, Alessandro, Ghini, Patrizia, (2017), La figura del DPO, Rivista 231, pp. 115 ss.;

Fronticelli Baldelli, Enrico (2018), "In vigore il Decreto in materia di Privacy", *Corriere tributario*, 40, pp. 3109-3114;

Galdieri, Paolo, (2012), "Il trattamento illecito del dato nei "social network", in *Giurisprudenza di merito,* 2012, 12, pp. 2699 ss.;

Galletti, Danilo, (2006), "I modelli organizzativi nel d.lgs. n. 231/2001: le implicazioni per la corporate governance", *Giurisprudenza Commentata*, 126-146;

Italiano", *Rivista trimestrale di diritto penale dell'economia,* 1, pp. 185 ss.;

La Manuzzi, Marta, (2017), Diritto penale e trattamento dei dati personali. I reati previsti dal Codice della privacy e la responsabilità amministrativa degli enti alla luce del regolamento 2016/679/UE, *JusOnli-ne,* 1, pp. 218-265;

Luberto, Mario, (2008), "I reati informatici contro il diritto alla privacy. La tutela fornita dal D.lgs 196 del 2003 e dal codice penale", *Giurisprudenza di merito,* 3, pp. 898 ss.;

Manna, Adelmo, (1993*),* "La protezione personale dei dati personali nell'ordinamento

Montalenti, Paolo (2014), "Modello "231" e organismo di vigilanza nel sistema dei controlli societari: un quadro d'insieme", *Il Nuovo Diritto delle Società*, 2, pp. 7-30;

Montalenti, Paolo (2017), "Prevenzione dei reati tributari (c.d. "Cooperative Compliance"), Modello 231, sistemi di controllo e "governance" societaria: profili generali e ipotesi di riforma", in *Il Nuovo Diritto delle Società*, 9, pp. 963-995;

Montalenti, Paolo, (2009), Organismo di vigilanza e sistema dei controlli, *Giurisprudenza Commentata*, I, 643- 660;

Paonessa, Caterina (2014), "Il ruolo dell'organismo di vigilanza nell'implementazione dei modelli organizzativi e gestionali nella realtà aziendale", *La Giustizia penale*, 7, pp. 440-448;

Patrono, Paolo, (1985), "Privacy e vita privata", Enciclopedia del Diritto, XXXV, pp. 557 ss.;

Perinu, Paola (2019), La privacy e la vigilanza sul modello 231. Quale ruolo per l'Organismo di Vigilanza?, *www.AOdV231.it,* pp. 1-6;

Perugini, Maria Roberta (2017), "Organismi di vigilanza e controllo e ruoli privacy: valutazioni generali e prime considerazioni sui trattamenti del DPO", in *https://europrivacy.info.it/2017/01/09*;

Picotti, Lorenzo, (2004), "Reati informatici, riservatezza, identità digitale", *www.aidp.it*, pp. 1-18;

Piraino, Fabrizio (2017), "Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato", *Nuove leggi civile commentate*, 2017, pp. 369-409;

Pisani, Nicola, (2008), I requisiti di autonomia ed indipendenza dell'organismo di vigilanza istituito ai sensi del d.lgs. 231/2001, *La responsabilità amministrativa delle società e degli enti*, 1, pp. 155 ss;

Pisapia, Alice (2018), *La tutela per il trattamento e la protezione dei dati personali,* (Torino, Giappichelli);

Pistorelli, Luca (2013), Relazione Ufficio del Massimario Cassazione, n. III/01/2013 del 22 agosto 2013, p. 7;

Pizzetti, Franco, (2010), "La tutela della riservatezza nella società contemporanea", *Percorsi costituzionali*, I, pp. 62 ss.

*Position Paper* sulla posizione soggettiva dell'ODV a fini privacy, elaborato dall'AODV nel marzo 2019, in *www.aodv231.it.*

Rimini, Emanuele, (2018), "I valori della solidarietà sociale nelle dichiarazioni non finanziarie", *Analisi giuridica dell'economia*, 1, pp. 187-199;

Rodotà, Stefano, (2010), "Una costituzione per internet?", *Politica del diritto*, 3, pp. 337-351;

Rordorf, Renato, (2001), I criteri di attribuzione della responsabilità. I modelli organizzativi e gestionali idonei a prevenire reati, *Le società*, 11, pp. 1297 ss.;

Rossi Dal Pozzo, Francesco, (2016), "La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal safe harbour al privacy shield)", *Rivista di diritto internazionale,* pp. 690 ss.

Santoriello, Ciro, (2015), Attività dell'organismo di vigilanza e obbligo di segretezza in capo ai suoi componenti, *La responsabilità amministrativa delle società e degli enti*, 4, pp. 109 ss.

Sarzana, Carlo, (2008), "La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa", *Diritto penale e processo,* 12, pp. 1572 ss

Senigaglia, Roberto, (2017), "Reg. Ue 2016679 e diritto all'oblio nella comunicazione telematica - Identità, informazione e trasparenza nell'ordine della dignità personale", *Nuove leggi civili*, 2017, pp. 1023 ss.

Sfameni, Paolo, (2007), "Responsabilità da reato degli enti e nuovo diritto azionario: appunti in tema didoveri degli amministratori ed organismo di vigilanza", *Rivista delle società*, 1, 2007, 183.

Soro, Antonello, (2018), "Persona, diritti e Innovazione", Relazione Garante privacy, pp. 1-16 ss.

Tampieri, Maura, (2017), Il diritto all'oblio e la tutela dei dati personali, *Responsabilità Civile e Previdenza*, 3, pp. 101 – 137;

Torre, Valeria, (2004), La gestione del rischio nella disciplina del trattamento dei dati personali, in Picotti Lorenzo (eds.), Il diritto penale dell'informatica nell'epoca di internet, (Padova, Cedam), pp. 237-277.


# Diritto Penale Contemporaneo

## RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL

A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

http://dpc-rivista-trimestrale.criminaljusticenetwork.eu